STANDARD WDROŻEŃ PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ

OPRACOWANIE NA POTRZEBY
SEKTORA UBEZPIECZENIOWEGO

PIU
Polska Izba Ubezpieczeń

accenture

WARSZAWA **2021**

accenture

MARUTA

Traple Konarski Podrecki & Wspólnicy
TKP

Autorzy Standardu

Podmioty reprezentowane	Rola	
Accenture Sp. z o.o.	Koordynacja prac grupy roboczej	Daniel Rudnicki Michał Truskolas Julia Lang
Aviva TUnŻ S.A.; Aviva TUO S.A.	Uczestnicy grupy roboczej	Paweł Kuźmicz Rafał Sałyga Sebastian Pluta Marek Kowalski
AXA Ubezpieczenia TUiR S.A.; AXA ŻYCIE TU S.A.	Uczestnicy grupy roboczej	Jolanta Gasiewicz Marcin Sęp Adam Żelazko Agnieszka Czumer
COMPENSA S.A.; COMPENSA ŻYCIE S.A.	Uczestnik grupy roboczej	Marcin Grabowski
TU Euler Hermes S.A.	Uczestnik grupy roboczej	Mateusz Kaczmarski
EUROPA S.A.; EUROPA ŻYCIE S.A.	Uczestnicy grupy roboczej	Tomasz Bujała, Anna Januchta-Barańczyk Bartosz Sacewicz Dorota Pokorska Igor Pełdiak Konrad Mazurek Paweł Bzdyk
GENERALI TU S.A.; GENERALI ŻYCIE TU S.A.	Uczestnicy grupy roboczej	Marcin Nosek Waldemar Lenda Katarzyna Wieczorek Iwona Wcisło Michał Pyszycki
InterRisk TU S.A. VIG	Uczestnik grupy roboczej	Krzysztof Góźdź
LINK 4 TU S.A.	Uczestnicy grupy roboczej	Małgorzata Jaworska Michał Więckowski
Maruta Wachta sp. j.	Koordynatorzy prawni	Marcin Maruta Michał Kulesza Marcin Białkowski
Nationale-Nederlanden TU SA; Nationale-Nederlanden TUnŻ S.A.	Uczestnicy grupy roboczej	Marcin Szydłowski Andrzej Miron Paweł Kaczmarek Ewa Kłosek
Open Life TU Życie S.A.	Funkcja doradcza	Paweł Smater Piotr Majchrzak

Podmioty reprezentowane	Rola	
PIIT	Funkcja doradcza	Dariusz Śpiewak
PKO TU S.A.; PKO Życie S.A.	Uczestnicy grupy roboczej	Jarosław Wachowicz Tomasz Arabski
Polska Izba Informatyki i Telekomunikacji	Uczestnicy grupy roboczej	Michał Jaworski Marcin Kaczmarczyk Michał Kaczorowski Bartosz Ptak Lech Szczuka
Polska Izba Ubezpieczeń	Koordynacja prac grupy roboczej	Mariusz Kuna Agnieszka Durska Anna Kwiatkowska Paweł Sawicki
PZU S.A.; PZU ŻYCIE S.A.	Uczestnicy grupy roboczej	Aleksandra Podhajska Rafał Jeż
STU ERGO Hestia SA; STUnŻ ERGO Hestia SA	Uczestnicy grupy roboczej	Jarosław Łojewski Damian Jagusz Marcin Usarzewicz
The Prudential Assurance Company Ltd. Oddział w Polsce	Uczestnicy grupy roboczej	Marcin Sagała Katarzyna Mierzejska
Towarzystwo Ubezpieczeń Wzajemnych „TUW”	Uczestnicy grupy roboczej	Jerzy Tarabuła Anna Pogorzelska
Traple Konarski Podrecki i Wspólnicy Sp.j	Koordynatorzy prawni	Jan Byrski Michał Synowiec Henryk Hoser Xawery Konarski
TUIR WARTA S.A.; TUnŻ WARTA S.A.	Funkcja doradcza	Kinga Królikowska Monika Muszyńska Maciej Pilarski Aleksandra Płoszajska
TUW PZUW	Uczestnik grupy roboczej	Jakub Papuga
UNIQA S.A.; UNIQA ŻYCIE S.A.	Uczestnicy grupy roboczej	Jacek Koziróg Maciej Bramson
Unum Życie TUiR S.A.	Uczestnik grupy roboczej	Dawid Banasiak
Vienna Life TUnŻ S.A. VIG	Uczestnicy grupy roboczej	Paweł Kwasiborski Michał Oko Ewa Lepiarczyk
VIG Polska Sp. z o.o.	Uczestnicy grupy roboczej	Marek Chmurzyński Jarosław Strzyga

Standard został skonsultowany w ramach grupy podmiotów opiniujących Polskiej Izby Informatyki i Telekomunikacji.

1. WSTĘP

Wychodząc naprzeciw oczekiwaniom rynku ubezpieczeniowego w Polsce w zakresie możliwości wdrażania rozwiązań opartych o usługi chmury obliczeniowej w podmiotach objętych nadzorem ubezpieczeniowym, powołaliśmy przy Polskiej Izbie Ubezpieczeń przeznaczoną temu tematowi grupę roboczą.

Sektor ubezpieczeniowy w Polsce umocowany jest w ramach ustaw, rozporządzeń, jak również rekomendacji i wytycznych nadzoru finansowego regulujących jego działalność. Adaptacja najnowszych rozwiązań technologicznych w ubezpieczeniach w ramach tych regulacji nie jest zadaniem łatwym. Zainteresowanie sektora ubezpieczeniowego, przy jednocześnie niewielkiej praktyce zakładów ubezpieczeń w zakresie wykorzystania usług chmurowych, skłoniło autorów niniejszego opracowania do zaproponowania zakładom ubezpieczeń stworzenia wspólnej inicjatywy, w celu opracowania standardu wdrożenia rozwiązań informatycznych opartych o chmurę obliczeniową w zakładach ubezpieczeń zgodnie z obowiązującymi regulacjami.

W październiku 2017 r. Urząd Komisji Nadzoru Finansowego opublikował komunikat dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej, który z jednej strony wprost dopuszczał korzystanie z usług chmurowych, lecz z drugiej wywoływał na rynku ubezpieczeniowym efekt mrożący dla ich wdrożeń.

W dniu 24 stycznia 2020 r. Urząd Komisji Nadzoru Finansowego opublikował komunikat (wydany w dniu 23 stycznia 2020 r.), który wyjaśnia wiele kwestii budzących wcześniej wątpliwości zakładów ubezpieczeń. Przy aktywnym udziale zakładów ubezpieczeń chcieliśmy wykorzystać doświadczenia, płynące z dotychczasowych wdrożeń oraz przeanalizować postanowienia komunikatu i w szerokim gronie zakładów ubezpieczeń wypracować wspólnie standard, stanowiący zbiór praktyk i rozwiązań umożliwiających zakładom ubezpieczeń łatwe przejście przez proces adaptacji do chmury, zarówno całej organizacji, jak i w zakresie jedynie wybranych rozwiązań oferowanych przez dostawców usług chmurowych.

Sam komunikat, zgodnie z jego brzmieniem, stanowi uzupełnienie i uszczegółowienie wybranych zaleceń w zakresie outsourcingu, opisanych między innymi w Wytycznych KNF z dnia 16 grudnia 2014 r. dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji oraz Ustawie o działalności ubezpieczeniowej i reasekuracyjnej i Ustawie o dystrybucji ubezpieczeń. Regulacje te muszą być brane pod uwagę przy określaniu możliwości, a następnie przy faktycznym wdrożeniu rozwiązań opartych o chmurę obliczeniową. Komunikat prezentuje podejście krajowe (model referencyjny), co oznacza, że wytyczne, zalecenia lub inne dokumenty prezentujące stanowisko Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EIOPA), które odnoszą się do przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej, w tym Wytyczne EIOPA, nie mają zastosowania do polskich zakładów ubezpieczeń oraz oddziałów zagranicznych zakładów ubezpieczeń prowadzących działalność na terytorium Rzeczypospolitej Polskiej.

Niniejszy Standard prezentuje, jakie zadania, procedury, procesy i analizy zakład ubezpieczeń powinien przeprowadzić i udokumentować pod kątem przygotowania organizacji do działania w sferze usług chmurowych w odniesieniu do poszczególnych zapisów wybranych regulacji.

Niniejszy dokument powstał przy wsparciu Związku Banków Polskich i w oparciu o „Standard wdrożeń przetwarzania informacji w chmurze obliczeniowej", tzw. Standard PolishCloud przygotowany wspólnie przez banki i dostawców technologii w ramach prac ZBP.

2. ZAŁOŻENIA

1. Niniejszy Standard odnosi się do wymogów dotyczących korzystania z rozwiązań chmurowych przez podmioty objęte nadzorem ubezpieczeniowym w rozumieniu Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (tj. Dz. U. z 2020 r. poz. 180, ze zmianami). Standard nie odnosi się zatem do wymogów dotyczących rozwiązań chmurowych dla podmiotów objętych innym nadzorem wskazanym w tej ustawie.
2. Standard analizuje wymogi komunikatu, a co za tym idzie, przedstawia wymogi Urzędu Komisji Nadzoru Finansowego w przypadku przetwarzania w podmiotach objętych nadzorem ubezpieczeniowym informacji w chmurze obliczeniowej publicznej lub chmurze obliczeniowej hybrydowej.

3. TERMINOLOGIA STOSOWANA W STANDARDZIE. OBJAŚNIENIE WYBRANYCH DEFINICJI KOMUNIKATU

Chmura obliczeniowa	ma znaczenie nadane w komunikacie terminowi „chmura obliczeniowa". Na potrzeby Standardu, przez chmurę obliczeniową rozumiemy chmurę obliczeniową publiczną oraz chmurę obliczeniową hybrydową. Określając, czy wykorzystywana jest chmura obliczeniowa, można wziąć pod uwagę w szczególności: – skalowalność dostarczanych usług – możliwość dynamicznego i automatycznego alokowania zasobów obliczeniowych w oparciu o bieżące zapotrzebowanie, – konfigurowalność – możliwość samodzielnej zmiany parametrów indywidualnych usług chmury obliczeniowej, w tym powoływanie nowych oraz usuwanie istniejących usług, – mierzalność – model rozliczania za konkretnie wykorzystywane zasoby obliczeniowe.
Chmura obliczeniowa hybrydowa	ma znaczenie nadane w komunikacie terminowi „chmura obliczeniowa hybrydowa"
Chmura obliczeniowa prywatna	ma znaczenie nadane w komunikacie terminowi „chmura obliczeniowa prywatna"
Chmura obliczeniowa publiczna	ma znaczenie nadane w komunikacie terminowi „chmura obliczeniowa publiczna"
Chmura obliczeniowa społecznościowa	ma znaczenie nadane w komunikacie terminowi „chmura obliczeniowa społecznościowa"
CPD	ma znaczenie nadane w komunikacie terminowi „CPD"
Dostawca usług chmury obliczeniowej	ma znaczenie nadane w komunikacie terminowi „dostawca usług chmury obliczeniowej"
Dostawca	przez dostawcę należy rozumieć dostawcę usług chmury obliczeniowej lub innego dostawcę Zakładu Ubezpieczeń (np. dostawcę usług IT), który korzysta z usług dostawcy usług chmury obliczeniowej w zakresie, w jakim podmiot ten wykonuje na rzecz Zakładu Ubezpieczeń proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez Zakład Ubezpieczeń oraz: 1. przetwarzanie informacji w chmurze obliczeniowej publicznej lub hybrydowej ma charakter outsourcingu szczególnego, lub 2. przetwarzanie w chmurze obliczeniowej publicznej lub hybrydowej dotyczy informacji prawnie chronionych (outsourcing chmury obliczeniowej inny niż szczególny). Zakład Ubezpieczeń stosuje komunikat w relacjach z multiagentami oraz agentami wyłącznymi w zakresie, w jakim podmioty te wykonują na rzecz Zakładu Ubezpieczeń proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez Zakład Ubezpieczeń oraz: 1. przetwarzanie informacji w chmurze obliczeniowej publicznej lub hybrydowej ma charakter outsourcingu szczególnego, lub

	2. przetwarzanie w chmurze obliczeniowej publicznej lub hybrydowej dotyczy informacji prawnie chronionych (outsourcing chmury obliczeniowej inny niż szczególny). Podmioty te, jako podmioty nadzorowane, stosują komunikat, gdy korzystają z chmury obliczeniowej publicznej lub hybrydowej, a przetwarzanie informacji, w ramach tych chmur obliczeniowych, ma charakter outsourcingu szczególnego lub dotyczy informacji prawnie chronionych. Za dostawcę, w rozumieniu Standardu nie uważa się: • ubezpieczającego, który zawarł umowę ubezpieczenia z Zakładem Ubezpieczeń, w tym ubezpieczającego w ubezpieczeniu grupowym, • brokera ubezpieczeniowego, reasekuratora, którzy jako Podmioty nadzorowane, niezależnie od Zakładu Ubezpieczeń, są zobowiązani samodzielnie wykonywać obowiązki wynikające z komunikatu.
EOG	oznacza Europejski Obszar Gospodarczy
Informacja prawnie chroniona	przez informacje prawnie chronione należy rozumieć informacje objęte tajemnicami sektora finansowego, o których mowa w ustawach wskazanych w komunikacie. Ze względu na profil działalności Zakładów Ubezpieczeń zastosowanie mają przepisy: • UDUR (Tajemnica ubezpieczeniowa, oraz inne tajemnice wskazane w tej ustawie, w tym w art. 36 UDUR w zakresie obowiązku zachowania w tajemnicy informacji o przekazaniu danych Policji); • UDU (tajemnice dotyczące pośredników ubezpieczeniowych, o których mowa w art. 22 ust. 5 pkt 3 UDU i w art. 32 ust. 3 pkt 1 UDU) w zakresie obowiązków agenta ubezpieczeniowego i obowiązków brokera ubezpieczeniowego dotyczących zachowania w tajemnicy informacji uzyskanych w związku z wykonywaniem czynności w zakresie dystrybucji ubezpieczeń). Wskazać przy tym należy, że Informacjami prawnie chronionymi mogą być także informacje podlegające ochronie na gruncie innych ustaw niż wskazane powyżej, np. w przypadku wykonywania przez Zakład Ubezpieczeń czynności bankowych w oparciu o art. 4 ust. 11 pkt 1 UDUR. Przez Informacje prawnie chronione nie należy rozumieć danych osobowych, o ile dane te nie są jednocześnie objęte tajemnicą sektora finansowego.
Kodeks cywilny	oznacza ustawę z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tj. Dz. U. z 2020 r. poz. 1740, ze zmianami)
Komunikat	oznacza komunikat Urzędu Komisji Nadzoru Finansowego z dnia 23 stycznia 2020 r., dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej
Model usługi chmury obliczeniowej	wariant dostarczania usługi przez dostawcę, w szczególności SaaS, PaaS, IaaS

Outsourcing szczególny chmury obliczeniowej lub outsourcing szczególny	oznacza outsourcing chmury obliczeniowej, w ramach którego Podmiot nadzorowany powierza dostawcy usług chmury obliczeniowej wykonanie za pomocą usługi chmury obliczeniowej czynności lub funkcji Podmiotu nadzorowanego, których brak lub przerwa w realizacji spowodowana awarią lub naruszeniem zasad bezpieczeństwa usługi chmury obliczeniowej, w ocenie Podmiotu nadzorowanego: • wpływałaby w sposób istotny na ciągłość wypełniania przez Podmiot nadzorowany warunków stanowiących podstawę uprawnienia prowadzenia działalności nadzorowanej lub jej wykonywania lub • zagrażałaby w sposób istotny wynikom finansowym Podmiotu nadzorowanego, niezawodności lub ciągłości wykonywania działalności nadzorowanej. Przetwarzanie Informacji prawnie chronionych nie stanowi warunku koniecznego dla występowania Outsourcingu szczególnego chmury obliczeniowej. Jako przykład istotnego wpływu na ciągłość wypełniania przez Podmiot nadzorowany warunków stanowiących podstawę uprawnienia prowadzenia działalności nadzorowanej lub jej wykonywania, który nie musi wiązać się z przetwarzaniem Informacji prawnie chronionych, można wskazać wykorzystywanie usług chmury obliczeniowej dla potrzeb realizacji niektórych obowiązków raportowych spoczywających na Zakładzie Ubezpieczeń, w tym określonych w art. 336-337 UDUR. Natomiast w zakresie dotyczącym zagrożenia w sposób istotny wynikom finansowym podmiotu nadzorowanego, niezawodności lub ciągłości wykonywania działalności nadzorowanej, które nie musi być powiązane z przetwarzaniem Informacji prawnie chronionych, przykładem może być wykorzystywanie usług chmury obliczeniowej do przetwarzania danych z istotnego systemu wspierającego działalność Zakładu Ubezpieczeń.
Poddostawca	podmiot, który świadczy usługi dla dostawcy usług chmury obliczeniowej, służące dostarczaniu usługi chmury obliczeniowej dla Podmiotu nadzorowanego i posiada albo może posiadać identyfikowany dostęp do informacji przetwarzanych przez Podmiot nadzorowany. Poddostawcą w rozumieniu Standardu nie będzie podmiot, który nie posiada, ani nie może posiadać dostępu do kluczy szyfrujących umożliwiających dostęp do informacji przetwarzanych przez Podmiot nadzorowany oraz nie identyfikuje Podmiotu nadzorowanego w ramach świadczonych usług.
Podmiot nadzorowany	podmiot podlegający nadzorowi nad rynkiem finansowym, w szczególności Zakład Ubezpieczeń, zakład reasekuracji, agent ubezpieczeniowy oraz broker ubezpieczeniowy

RODO	oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
Standard	niniejsze opracowanie
Tajemnica ubezpieczeniowa	oznacza „informację dotyczącą poszczególnych umów ubezpieczenia", zgodnie z art. 35 ust. 1 UDUR
UDU	oznacza ustawę z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń (tj. Dz. U. z 2019 r. poz. 1881 ze zm.)
UDUR	oznacza ustawę z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (tj. Dz. U. z 2020 r. poz. 895)
UKNF	Urząd Komisji Nadzoru Finansowego
Usługa chmury obliczeniowej	ma znaczenie nadane w komunikacie terminowi „usługa chmury obliczeniowej"
Wytyczne EIOPA	wytyczne Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych z dnia 6 lutego 2020 r. dotyczące outsourcingu do dostawców usług chmury obliczeniowej
Wytyczne IT	wytyczne Komisji Nadzoru Finansowego z dnia 16 grudnia 2014 r. dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w Zakładach Ubezpieczeń i zakładach reasekuracji
Zakład Ubezpieczeń	podmiot objęty nadzorem ubezpieczeniowym będący krajowym lub zagranicznym Zakładem Ubezpieczeń w rozumieniu UDUR, jak również oddziałem zagranicznego Zakładu Ubezpieczeń
Zasada proporcjonalności	zgodnie z art. 29 ust. 3 dyrektywy 2009/138/WE, celem Zasady proporcjonalności jest stosowanie określonych wymogów, w tym także tych związanych z outsourcingiem do dostawców usług chmury obliczeniowej, w sposób proporcjonalny do natury, skali i złożoności ryzyka właściwego dla działalności Zakładu Ubezpieczeń lub zakładu reasekuracji. Zakłady Ubezpieczeń, w myśl Zasady proporcjonalności, powinny uwzględniać złożoność czynności lub funkcji zlecanych na zasadzie outsourcingu, ryzyko wynikające z umowy outsourcingu oraz potencjalny wpływ outsourcingu na ciągłość wykonywanej działalności, mając jednocześnie na uwadze zapewnienie realizacji określonego w komunikacie celu.

Pojęcia inaczej nie zdefiniowane w treści Standardu mają znaczenie takie jak w komunikacie.

4. ORGANIZACJA DOKUMENTU

1. Standard został podzielony na rozdziały poświęcone regulacjom mającym wpływ na sposób implementacji usług chmury obliczeniowej w sektorze ubezpieczeniowym.
2. W Rozdziale 5 opisane zostały rekomendacje i regulacje prawne wraz z odpowiednimi ustandaryzowanymi działaniami, jakie w ocenie Autorów należy podjąć celem wdrożenia usługi chmury obliczeniowej zgodnie z daną regulacją.
3. Każdy z podrozdziałów w Rozdziale 5 został opracowany poprzez (o ile ma zastosowanie):
    1) zacytowanie w nagłówku rozdziału danego punktu regulacji,
    2) podsumowanie opisu wymagań wynikających z regulacji,
    3) wskazanie wymagań (produktów) po stronie Zakładu Ubezpieczeń,
    4) wskazanie wymagań (produktów) po stronie dostawcy usług chmury obliczeniowej oraz
    5) wskazanie szablonów lub przykładów dokumentów.

5. WYMOGI KOMUNIKATU UKNF

5.1. 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. Komunikat ma zastosowanie w dwóch przypadkach:
   1) przetwarzania informacji prawnie chronionych w ramach outsourcingu chmury obliczeniowej (tzw. zwykłego outsourcingu), lub
   2) Outsourcingu szczególnego chmury obliczeniowej.
2. W każdym innym przypadku komunikat może być stosowany, jeśli Zakład Ubezpieczeń (również w porozumieniu z dostawcą usług chmury obliczeniowej) tak postanowi.
3. 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.
4. Przed powierzeniem przetwarzania informacji w chmurze obliczeniowej publicznej lub chmurze obliczeniowej hybrydowej Zakład Ubezpieczeń dokonuje:
   1) wstępnej klasyfikacji i oceny informacji planowanych do powierzenia celem zidentyfikowania, czy będą to Informacje prawnie chronione,
   2) oceny, czy powierzenie przetwarzania informacji stanowi Outsourcing szczególny.
5. Wymagania określone w komunikacie powinny być spełnione przez Zakład Ubezpieczeń przed rozpoczęciem przetwarzania informacji w usłudze chmury obliczeniowej.

6. Stosowanie komunikatu powinno odbywać się w sposób zgodny z Zasadą proporcjonalności.
7. Zasada proporcjonalności powinna znaleźć swoje doprecyzowanie na etapie szacowania ryzyka związanego z planowaniem czynności powierzenia przetwarzania informacji w usłudze chmury obliczeniowej.
8. Zakład Ubezpieczeń nie ma obowiązku stosowania komunikatu w odniesieniu do relacji z podmiotem niebędącym dostawcą, nawet jeśli podmiot ten w ramach swojej działalności korzysta z usług chmury obliczeniowej.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Dokument potwierdzający wstępną klasyfikację i ocenę informacji planowanych do powierzenia celem zidentyfikowania, czy będą to Informacje prawnie chronione w ramach outsourcingu chmury obliczeniowej (tzw. zwykłego outsourcingu) lub czy występuje Outsourcing szczególny chmury obliczeniowej.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUGI CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. Załącznik 7. – Przykładowe kroki wdrożenia usługi przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej w Zakładzie Ubezpieczeń
2. Załącznik 8. – Przykład – Proces wdrożenia

5.2. 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. Zakład Ubezpieczeń klasyfikuje informacje w udokumentowany sposób, zgodnie z metodyką opisaną w niniejszym Standardzie lub inną przyjętą w Zakładzie Ubezpieczeń, w tym w szczególności zapewnia, że:
   1) klasyfikacja informacji uwzględnia podział na kategorie informacji;
   2) klasyfikacja informacji uwzględnia co najmniej podział na informacje prawnie chronione oraz pozostałe informacje;
   3) klasyfikacja informacji uwzględnia podstawowe atrybuty bezpieczeństwa, tj. poufność, integralność i dostępność.
2. Zakład Ubezpieczeń na bieżąco monitoruje zmiany dotyczące wymogów prawnych oraz regulacyjnych w zakresie, który wymagałby ponownej klasyfikacji przetwarzanych informacji.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Opisany proces klasyfikacji i oceny informacji przetwarzanych w chmurze obliczeniowej uwzględniający wytyczne opisane w rozdziale V komunikatu – Wytyczne do klasyfikacji i oceny informacji (ust. 1 pkt 1-3 oraz ust. 3 pkt 1-3).
2. Udokumentowane zasady klasyfikacji informacji.
3. Udokumentowane wyniki klasyfikacji informacji, które powinny zostać uwzględnione w planie przetwarzania informacji w chmurze obliczeniowej.
4. Udokumentowane okresowe przeglądy klasyfikacji informacji (nie rzadziej niż raz w roku) wraz z potwierdzeniem aktualności stosowanej klasyfikacji i oceny informacji.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUGI CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. Załącznik 1. – Przykład szablonu klasyfikacji informacji

5.3. 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. Szacowanie ryzyka jest prowadzone w sposób ciągły, z uwzględnieniem praktycznej implementacji zasady PDCA („plan – do – check – act").

2. Podmiot nadzorowany uwzględnia w procesie szacowania ryzyka, w kontekście wyników przeprowadzonej klasyfikacji i oceny przetwarzanych informacji w chmurze obliczeniowej, co najmniej:
    1) ogólne zagrożenia dla stosowania chmury obliczeniowej:
        a) rozproszenie geograficzne przetwarzanych informacji, w szczególności w kontekście zapewnienia zgodności procesu przetwarzania informacji z przepisami prawa, regulacjami wewnętrznymi, zobowiązaniami umownymi oraz deklaracjami i innymi uregulowaniami;
        b) możliwość utraty zgodności postępowania podmiotu nadzorowanego z przepisami prawa (w tym wydanych licencji lub zezwoleń) poprzez korzystanie z usług chmury obliczeniowej w sposób niezamierzony albo inny niż zamierzony;
        c) dostęp do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) dostawcy usług chmury obliczeniowej;
        d) dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się fizycznie przetwarzanie (lokalizacja centrum przetwarzania danych), w szczególności odniesienie do katalogu sytuacji (lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu nadzorowanego, zarówno przez organy administracji krajowej, jak i międzynarodowej;
        e) brak zgodności technologicznej pomiędzy usługami różnych dostawców chmury obliczeniowej powodujące przywiązanie do jednego dostawcy usług chmury obliczeniowej poprzez ograniczenie albo brak możliwości przenoszenia (korzystania z identycznych) usług lub przetwarzanych informacji (vendor lock-in);
        f) awarie mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej;
        g) podatność interfejsów zarządzających usługami, które są udostępniane przez dostawców usług chmury obliczeniowej;
        h) ograniczona możliwość wpływania na zakres, kształt i zmiany usług, w tym w szczególności na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług przetwarzania;
        i) ograniczona możliwość kontrolowania dostawcy usług chmury obliczeniowej oraz jego poddostawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej;
        j) podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy dostawcę usług chmury obliczeniowej a podmiot nadzorowany;
    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. 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. Zakład Ubezpieczeń dokonuje szacowania ryzyka w udokumentowany sposób oraz zgodnie z metodyką opisaną w niniejszym Standardzie lub inną przyjętą w Zakładzie Ubezpieczeń.
2. Zakład Ubezpieczeń powinien nie rzadziej niż raz w roku zweryfikować czynniki mające istotny wpływ na szacowanie ryzyka (w tym wymogi prawne, regulacyjne, organizacyjne oraz techniczne) i w przypadku zaistnienia takich czynników dokonać ponownego szacowania ryzyka.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Udokumentowany proces szacowania ryzyka pod kątem dopuszczalności przetwarzania informacji w chmurze obliczeniowej wraz z opisanym procesem okresowej weryfikacji oraz aktualizacji wyników szacowania ryzyka (nie rzadziej niż raz w roku lub w przypadku istotnych okoliczności mających wpływ na poziom ryzyka).
2. Dokument zawierający wyniki szacowania ryzyka dla każdej usługi w chmurze obliczeniowej uwzględniający strategię postępowania z ryzykiem (akceptacja, redukcja, przeniesienie lub unikanie) oraz plan postępowania z ryzykiem wraz z terminami i przypisanymi osobami odpowiedzialnymi za wdrożenie środków zaradczych.
3. Dokument potwierdzający formalne zatwierdzenie wyników szacowania ryzyka.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUGI CHMURY OBLICZENIOWEJ

1. Udokumentowanie spełnienia 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 chmury obliczeniowej;
   2) lokalizacji CPD, obszaru przetwarzania danych (lokalizacji, z których personel dostawcy usług chmury obliczeniowej uzyskuje dostęp do danych Zakładu Ubezpieczeń). Dopuszczalne jest wskazanie co najmniej państwa i regionu;
   3) sposobu kontroli i monitorowania dostępu do przetwarzanych informacji przez personel dostawcy usług chmury obliczeniowej i jego podwykonawców, 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 Zakład Ubezpieczeń;
11) monitorowania środowiska przetwarzania informacji w usłudze chmury obliczeniowej wraz z zasadami zarządzania logami;
12) możliwości integracji z innymi, wskazanymi przez Zakład Ubezpieczeń, technologiami;
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) treści zawartych umów na korzystnie 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 6. do standardu (analizę ISO 27001).
3. Poinformowanie Zakładu Ubezpieczeń o stosowanych zabezpieczeniach.
4. Jeżeli to możliwe i uzasadnione, udokumentowanie posiadanych certyfikatów lub ich odpowiedników, tj:
   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 2. – Przykład szablonu szacowania ryzyka
2. Załącznik 6. – ISO 27001
3. Załącznik 9. – Przykład – Opis metodyki uzyskania szacowania ryzyka i zgodności z komunikatem UKNF

5.4. MINIMALNE WYMAGANIA DLA PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ

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. Zakład Ubezpieczeń 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 oszacowania ryzyka. Utrzymanie i systematyczne podnoszenie kompetencji (kwalifikacji, wiedzy i umiejętności) powinno być częścią dobrych praktyk Zakładu Ubezpieczeń. 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, Zakład Ubezpieczeń powinien określić kompetencje w organizacji podczas wdrożenia lub przy utrzymaniu rozwiązań chmurowych.

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. Zakład Ubezpieczeń w ramach utrzymania produkcyjnych systemów przetwarzających informacje w chmurze obliczeniowej powinien posiadać aktywne wsparcie dostawców usług chmury obliczeniowej wraz z warunkami tego wsparcia.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Udokumentowany proces zapewniający posiadanie przez Zakład Ubezpieczeń kompetencji wewnętrznych lub zewnętrznych niezbędnych do wdrożenia, utrzymania, rozwoju usług chmury obliczeniowej.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUG CHMURY OBLICZENIOWEJ

1. Udokumentowane kompetencje.
2. Udokumentowane wsparcie personelu dostawcy usług chmury obliczeniowej na rzecz Zakładu Ubezpieczeń.

SZABLONY

N/D

4. Umowa z dostawcą usług chmury obliczeniowej

1. Podmiot nadzorowany posiada sformalizowaną umowę (oraz inne dokumenty, w tym oświadczenia, regulaminy, warunki korzystania z usług, także w wersji elektronicznej) z dostawcą usług chmury obliczeniowej, która – tam, gdzie to zasadne w odniesieniu do używanych usług i zakresu przetwarzanych informacji – zawiera lub wskazuje źródła informacji, obejmujące:
   a) klarowny podział odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji, z uwzględnieniem modelu świadczenia usług, ciągłości działania usług (z uwzględnieniem parametrów RTO i RPO tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;
   b) klarowną definicję i wskazanie lokalizacji przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;
   c) prawo właściwe dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów);
   d) potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;
   e) własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu (wygaśnięciu, rozwiązaniu), także w sposób nieplanowany;
   f) gwarancje, rękojmie, ubezpieczenia (polisy ubezpieczeniowe dostawcy usług chmury obliczeniowej), kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej oraz zasad postępowania w takich sytuacjach, o ile ma to zastosowanie;
   g) określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie), zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;
   h) klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) dostawcy usług chmury obliczeniowej oraz warunki nadawania praw dostępu do informacji przetwarzanych przez podmiot nadzorowany;
   i) klarowne wskazanie zasad, zgodnie z którymi zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań poddostawców dostawcy usług chmury obliczeniowej są transparentne i jasno

identyfikowane przez podmiot nadzorowany;

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

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

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

m) prawo podmiotu nadzorowanego do przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji, w tym prawo do przeprowadzenia audytu drugiej lub trzeciej 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.

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. Zakład Ubezpieczeń jest zobowiązany do zawarcia, sformalizowanej umowy z dostawcą usług chmury obliczeniowej. 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 Zakładzie Ubezpieczeń;
3) wytycznych organu nadzoru, w tym również w zakresie komunikatu.

2. W przypadku poddania umowy prawu państwa trzeciego Zakład Ubezpieczeń powinien posiadać pisemną opinię prawną, m.in. opracowaną przez wyspecjalizowany, niezależny od dostawcy usług chmury obliczeniowej podmiot, która może zostać przygotowana na zlecenie dostawcy usług chmury obliczeniowej, potwierdzającą, że zgodnie z wybranym prawem właściwym umowy, wszystkie postanowienia umowy pomiędzy Zakładem Ubezpieczeniem a dostawcą usług chmury obliczeniowej spełniają wymagania prawa oraz wymagania komunikatu, obowiązujące Zakład Ubezpieczeń.
3. Umowa z dostawcą usług chmury obliczeniowej powinna zawierać elementy wymienione w punkcie 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 puntem 4.2 komunikatu, Zakład Ubezpieczeń może korzystać z ramowych umów udostępnianych przez dostawców usług chmury obliczeniowej, przy założeniu braku uszczerbku dla wymagań prawa oraz z uwzględnieniem postanowień komunikatu.
4. Umowa z dostawcą usług chmury obliczeniowej powinna określać zasady rozwiązywania umowy, w tym zasady i terminy zwrotu lub usunięcia przetwarzanych informacji. Umowa powinna w szczególności określać sposób przekazania danych do Zakładu Ubezpieczeń w przypadku wycofania się Zakładu Ubezpieczeń z chmury obliczeniowej lub migracji do innej chmury obliczeniowej.
5. Umowa z dostawcą usług chmury obliczeniowej powinna określać sposób usunięcia danych z infrastruktury dostawcy usług chmury obliczeniowej.
6. W trakcie trwania umowy z dostawcą usług chmury obliczeniowej, jak i po jej zakończeniu Zakład Ubezpieczeń powinien zapewnić sobie pełną i wyłączną kontrolę nad danymi i informacjami uzyskanymi w wyniku przetwarzania danych dostarczonych przez Zakład Ubezpieczeń, np. profilami behawioralnymi (informacje). Zakład Ubezpieczeń powinien zapewnić w umowie trwałe i bezpieczne usunięcie informacji przez dostawcę usług chmury obliczeniowej z infrastruktury Dostawcy i podmiotów z nim współpracujących.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Umowa z dostawcą usług chmury obliczeniowej wraz niezbędnymi dokumentami (oświadczenia, regulaminy, warunki korzystania z usług, itp.).

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUG CHMURY OBLICZENIOWEJ

1. Zawarcie umowy z Zakładem Ubezpieczeń uwzględniającej wymagania komunikatu i bezwzględnie obowiązujących przepisów prawa.

SZABLONY

N/D

5. Plan przetwarzania informacji w chmurze obliczeniowej

1. Podmiot nadzorowany na podstawie wyników szacowania ryzyka opracowuje udokumentowany plan przetwarzania informacji w chmurze obliczeniowej, który zawiera co najmniej:
   a) rodzaj (opis) przetwarzanych informacji oraz informację, jeżeli stosowane, o ich pseudonimizacji lub anonimizacji;
   b) sposób szyfrowania informacji oraz miejsce (lub sposób) zarządzania kluczami szyfrującymi;
   c) informację o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany;
   d) datę zawarcia umowy z dostawcą usług chmury obliczeniowej i referencje do tej umowy (numer, okres

obowiązywania, datę przedłużenia lub zmiany, daty rozpoczęcia korzystania z usług), a w przypadku, gdy umowa nie jest jeszcze zawarta – przewidywaną datę jej zawarcia;

e) prawo właściwe, któremu podlega umowa;

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

OPIS WYMAGAŃ

2. Zakład Ubezpieczeń w ramach bieżącego i planowanego przetwarzania informacji (uruchomienia inicjatywy) w chmurze obliczeniowej powinien posiadać udokumentowany plan przetwarzania informacji w chmurze obliczeniowej. Plan ten w szczególności powinien zawierać (najlepiej w postaci szczegółowej dokumentacji):
    1) opis zadania realizowanego za pomocą usługi chmury obliczeniowej;
    2) mechanizmy zabezpieczenia informacji (pseudonimizacja, anonimizacja), mechanizmy szyfrowania informacji, w tym zasady zarządzania i przechowywania kluczy szyfrujących, oraz opis kontroli dostępu do informacji.
3. Plan przetwarzania w oparciu o wewnętrzną klasyfikację danych powinien precyzyjnie określić, jakie dane (informacje) Zakład Ubezpieczeń, w ramach konkretnej inicjatywy, przetwarza w chmurze obliczeniowej.
4. Zgodnie z pkt. 2 „Opisu Wymagań" dot. pkt. VI Komunikatu – Wytyczne do szacowania ryzyka, plan powinien być przeglądany w ustalonych cyklach bądź przy wystąpieniu większych zmian w zakresie lub sposobie przetwarzania informacji w chmurze obliczeniowej.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Plan przetwarzania informacji, np. w formie wypełnionego szablonu przedstawionego w Załączniku 3. do Standardu).

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. Załącznik 3. – Przykładowy plan przetwarzania informacji w chmurze obliczeniowej

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 Zakład Ubezpieczeń, o ile jest to zasadne, powinien przeprowadzić i udokumentować fazę testów usługi chmury obliczeniowej. Testy powinny być przeprowadzone na danych testowych; przeprowadzone testy powinny być adekwatne do oszacowanego ryzyka, skali, krytyczności danych i procesu uruchomionego w, lub w oparciu o chmurę obliczeniową (zgodnie ust. VI komunikatu – Wytyczne do szacowania ryzyka). W oparciu o wyniki szacowania ryzyka, decyzją wewnętrzną Zakład Ubezpieczeń może zdecydować o braku konieczności realizacji testów.
2. Adekwatnie do modelu usługi chmury obliczeniowej, należy przygotować scenariusze testowe.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Formalne wyniki testów.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

N/D

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. Zakład Ubezpieczeń posiada plan wycofania się z usługi chmury obliczeniowej zarówno w sytuacji zmiany strategii, jak i w sytuacji awaryjnej.
2. Plan powinien być adekwatny do oszacowanego ryzyka, skali, krytyczności danych i procesu uruchomionego w chmurze obliczeniowej lub w oparciu o chmurę obliczeniową. Plan może bazować na danych technologicznych rozwiązania, które są ogólnie dostępne. Zakład Ubezpieczeń powinien zidentyfikować, z jakich procesów i aplikacji korzysta, w tym:
    1) zbadać, w szczególności z uwzględnieniem VI.2.1.e i h komunikatu, które z tych procesów i aplikacji mają istotny wpływ na działalność Zakładu Ubezpieczeń (tzn. ich brak działania lub działanie nieprawidłowe istotnie wpłynie na funkcjonowanie Zakładu Ubezpieczeń z perspektywy skutków ekonomicznych, skutków dla reputacji Zakładu Ubezpieczeń, skutków dla klientów Zakładu Ubezpieczeń oraz wymogów nadzorczych związanych z prowadzoną przez niego działalnością), oraz które procesy i aplikacje mogą zostać przeniesione do innych dostawców usługi chmury obliczeniowej lub do infrastruktury „on-premise";
    2) dokonać kwalifikacji, czy dany proces i aplikacja ma istotne znaczenie. Zakład Ubezpieczeń dokona klasyfikacji w oparciu o szacowanie ryzyka. Szacowanie ryzyka może być przeprowadzane samodzielnie przez Zakład Ubezpieczeń lub w oparciu o standardy opracowane w ramach zrzeszeń branżowych lub innych powszechnie przyjętych. Plan powinien zapewnić, że w sytuacji awaryjnej nie dojdzie do uszczerbku dla zachowania zgodności działania Zakładu Ubezpieczeń z wymaganiami prawa i innych regulacji, w tym związanych z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.
3. Plan wycofania się z usługi może zakładać powrót do środowiska „on-premise", migrację do innego dostawcy lub inne uzasadnione biznesowo scenariusze.
4. Plan powinien być przetestowany, przy czym zakres i podejście do testów powinny wynikać z analizy ryzyka (zgodnie z pkt VI komunikatu – Wytyczne do szacowania ryzyka) w oparciu o obowiązujące w Zakładzie Ubezpieczeń metodyki.
5. Testy planu wycofania:
    - powinny obejmować procesy i aplikacje, które mają istotny wpływ na działalność Zakładu Ubezpieczeń, a nie dostawcę usług chmury obliczeniowej. Testowanie nie powinno być ograniczone do teoretycznych ćwiczeń symulujących podjęcie adekwatnych kroków w przypadku wystąpienia określonych zdarzeń (przeprowadzenia gry sztabowej);
    - powinny być realizowane w terminach i w oparciu o obowiązujące w Zakładzie Ubezpieczeń metodyki, w szczególności poprzez rzeczywiste wykonanie działań awaryjnych w stosunku do procesów i aplikacji, które mają istotny wpływ na działalność Zakładu Ubezpieczeń. Zalecane testowanie planu wycofania nie rzadziej niż raz w roku;
    - powinny odbywać się rotacyjnie w oparciu o różne procesy i aplikacje. Rotacyjne testowanie powinno dotyczyć procesów i aplikacji, które mają istotny wpływ na działalność Zakła-

du Ubezpieczeń. Dodatkowe założenia testowania planu wycofania:

- Zakład Ubezpieczeń może przeprowadzać testy w oparciu o listę procesów i aplikacji mających istotny wpływ na działalność Zakładu Ubezpieczeń (Zestawienie).
- Zestawienie powinno być aktualizowane co najmniej raz w roku, natomiast monitorowanie wykorzystywanych procesów i aplikacji powinno odbywać się w sposób ciągły.
- Zakład Ubezpieczeń opracowuje i utrzymuje Zestawienie. Zestawienie może stanowić podstawę do wyboru testowanego procesu.

6. Plan powinien być przeglądany i aktualizowany w określonym przez wewnętrzne procedury Zakładu Ubezpieczeń okresie czasu.
7. Plan powinien zawierać kryteria podjęcia decyzji o uruchomieniu planu wycofania się z usługi chmury obliczeniowej. Uruchomienie planu może nastąpić m.in. w przypadku:
    - nieakceptowalnej zmiany warunków świadczenia usługi przez dostawcę;
    - wypowiedzenia umowy przez dostawcę;
    - wewnętrznej decyzji biznesowej o zaprzestaniu korzystania z usługi lub zmiany strategii korzystania z usług zewnętrznych dostawców;
    - decyzji administracyjnej nakazującej Zakładowi Ubezpieczeń rozwiązanie umowy z dostawcą.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

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

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. Załącznik 4. – Przykładowy szablon scenariusza wyjścia z chmury
2. Załącznik 5. – Przykład – Wyjście z chmury – główne zagadnienia

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. Zakład Ubezpieczeń powinien rozważyć scenariusz uwzględniający potencjalną możliwość utraty kontroli nad przetwarzanymi informacjami u danego dostawcy usług chmury obliczeniowej oraz możliwość przerwania ciągłości działania usługi chmury obliczeniowej.
2. Zakład Ubezpieczeń może polegać na planach ciągłości działania po stronie dostawcy usług chmury obliczeniowej. Dobrą praktyką jest pełnienie przez Zakład Ubezpieczeń nadzoru nad działaniami dostawcy usług chmury obliczeniowej w tym zakresie, tj. regularnej weryfikacji adekwatności planu oraz analizy przedstawianych wyników testów planu ciągłości działania i planów awaryjnych (np. poprzez weryfikacje wewnętrznego zespołu Zakładu Ubezpieczeń, wyników niezależnych audytów, certyfikacje, etc.), czego możliwość należy zagwarantować na etapie podpisywania umowy z dostawcą usług chmury obliczeniowej.
3. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej dostawców usług chmury

obliczeniowej, Zakład Ubezpieczeń powinien regularnie weryfikować możliwość realizacji tego scenariusza, zwłaszcza po zmianach technologicznych 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 Zakładu Ubezpieczeń, dopuszcza się brak opracowywania planu ciągłości działania.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

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 w Zakładzie Ubezpieczeń (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 podpunktu powyżej, w szczególności dotycząca weryfikacji możliwości realizacji scenariusza po zmianach technologicznych u jednego z dostawców usług chmury obliczeniowej.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUG CHMURY OBLICZENIOWEJ

N/D

SZABLONY

N/D

6. Wymagania dla dostawców usług chmury obliczeniowej[1]

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.
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.

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

(...)

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

OPIS WYMAGAŃ

1. Zakład Ubezpieczeń, w zależności od modelu usługi chmury obliczeniowej oraz od klasyfikacji informacji, podejmuje decyzję dotyczącą konieczności weryfikacji podstawowego lub rozszerzonego katalogu zabezpieczeń stosowanych przez dostawcę usług chmury obliczeniowej.
2. W przypadku wyboru katalogu podstawowego, zabezpieczenia weryfikowane są w oparciu o zakres przedstawiony w pkt. 1 „Opisu wymagań do opracowania po stronie dostawcy" dot. pkt. VI komunikatu – Wytyczne do szacowania ryzyka.
3. W przypadku wyboru katalogu rozszerzonego, zabezpieczenia weryfikowane są w oparciu o wymagania zawarte w Załączniku A standardu ISO 27001, w oparciu o szablon przedstawiony w Załączniku 6 do niniejszego dokumentu.
4. Niezależnie od wybranego katalogu zabezpieczeń, w zależności od modelu usługi chmury obliczeniowej oraz przy zachowaniu Zasady proporcjonalności, Zakład Ubezpieczeń może ograniczyć katalog weryfikowanych zabezpieczeń.
5. W zależności od decyzji Zakładu Ubezpieczeń Dostawca usług chmury obliczeniowej powinien zapewnić zgodność usługi chmury obliczeniowej z normami ISO wymienionym w pkt VII ust. 6.1 i 6.2 komunikatu lub ich odpowiednikami (normami BS, normami PN-ISO, etc.).
6. 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 w/w normami poprzez udokumentowanie realizacji poszczególnych wymagań norm.
7. Dokumentacja związana ze zgodnością oraz wyniki audytów certyfikacyjnych lub dokumentacja zgodności dostarczona przez dostawcę usług chmury obliczeniowej, powinny być przekazane przed zawarciem umowy oraz okresowo udostępniane Zakładowi Ubezpieczeń. Rekomendowane jest zawarcie w umowie z dostawcą usług chmury obliczeniowej postanowień obligujących go do cyklicznego dostarczania odpowiednich dokumentów.
8. Zakład Ubezpieczeń powinien regularnie weryfikować dokumentację związaną ze zgodnością, a w przypadku, gdy w/w dokumentacja wykaże istotne niezgodności, Zakład Ubezpieczeń powinien uzgodnić z dostawcą usług chmury obliczeniowej plan naprawczy oraz monitorować jego realizację.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Udokumentowane wymagania Zakładu Ubezpieczeń w zakresie w/w norm i standardów, w szczególności dokumentacja akceptacji ryzyka w przypadku rezygnacji z wybranych wymagań.
2. Pozyskanie certyfikatu 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.

WYMAGANIA (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 Zakładu Ubezpieczeń lub dokumentacja zgodności z przedmiotowymi normami przygotowana przez dostawcę usług chmury obliczeniowej.

SZABLONY

N/D

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, co nie wyklucza możliwości przetwarzania danych (informacji) przez dostawcę usług chmury obliczeniowej poza EOG.
2. Jeżeli usługa ma być świadczona w CPD na terenie EOG, Zakład Ubezpieczeń korzystający z usług chmury obliczeniowej globalnego dostawcy usług chmury obliczeniowej powinien zdefiniować mechanizmy kontrolne zapewniające, że usługi, które wykorzystuje są świadczone w CPD na terenie EOG.
3. W przypadku gdy CPD zlokalizowane jest na terenie EOG, ale usługa jest również wspierana przez personel mający dostęp do danych (informacji) zlokalizowany poza EOG, wymagane jest zapewnienie zgodności z przepisami w tym zakresie.

WYMAGANIA (produkty) DO OPRACOWANIA

po stronie Zakładu Ubezpieczeń

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.

WYMAGANIA (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).

SZABLONY

N/D

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 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji;

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

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

OPIS WYMAGAŃ

1. Zakład Ubezpieczeń może wymagać od dostawcy usług chmury obliczeniowej przedstawienia mechanizmu kontroli dostępu do danych (informacji) przetwarzanych w usłudze chmury obliczeniowej, w tym dla pracowników (współpracowników) i poddostawców dostawcy usług chmury obliczeniowej.
2. W zależności od modelu usługi chmury obliczeniowej i w miarę możliwości technicznych dostawca usług chmury obliczeniowej nie powinien mieć stałego dostępu do danych (informacji) ani dostępu administracyjnego, serwisowego etc. na poziomie serwerów, baz danych, aplikacji czy urządzeń.
3. Zakład Ubezpieczeń może wymagać od dostawcy usług chmury obliczeniowej przekazania 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).

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

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

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUG CHMURY OBLICZENIOWEJ

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

SZABLONY

N/D

7. Kryptografia

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. Wymagane jest szyfrowanie informacji przetwarzanych w chmurze obliczeniowej. Mechanizmy i zakres wykorzystywania zabezpieczeń kryptograficznych powinny wynikać z analizy ryzyka z zachowaniem Zasady proporcjonalności (zgodnie z pkt 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 Zakładu Ubezpieczeń przez dostawców dokumentacji mechanizmów szyfrowania danych (informacji), a także mechanizmów weryfikacji poprawności konfiguracji i działania w/w mechanizmów;
    3) posiadanie przez Zakład Ubezpieczeń kompetencji w zakresie poprawnej konfiguracji usług chmury obliczeniowej, w tym mechanizmów szyfrowania;
    4) w zależności od modelu usługi chmury obliczeniowej korzystanie przez Strony z zalecanych ustawień podnoszących bezpieczeństwo (tzw. hardening); ustawienia te powinny zostać udokumentowane.

WYMAGANIA (produkty) DO OPRACOWANIA

po stronie Zakładu Ubezpieczeń

1. W zależności od modelu usługi chmury obliczeniowej dokumentacja mechanizmów szyfrowania oraz metody weryfikacji poprawności konfiguracji szyfrowania.
2. W zależności od modelu usługi chmury obliczeniowej potwierdzenie posiadanych kompetencji – patrz pkt VII ust. 3 komunikatu.
3. W zależności od modelu usługi chmury obliczeniowej dokumentacja hardeningu usługi, w szczególności uwzględniająca wykorzystanie mechanizmów szyfrowania.
4. W zależności od modelu usługi chmury obliczeniowej potwierdzenie szyfrowania danych (informacji) w spoczynku i podczas przesyłu (w szczególności informacja przekazana przez dostawcę usług chmury obliczeniowej, dokumentacja techniczna etc.).

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUGI CHMURY OBLICZENIOWEJ

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

SZABLONY

N/D

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.
3. W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM), to HSM mogą być udostępniane przez dostawcę usług chmury obliczeniowej, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS 140-2 Level 2 lub równoważne.
4. Podmiot nadzorowany w udokumentowanym procesie zarządza tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz kontrolą tego procesu.
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

1. W zależności od modelu usługi chmury obliczeniowej lub o ile ma to uzasadnienie w ocenie ryzyka, Zakład Ubezpieczeń powinien zapewnić, że informacje są szyfrowane kluczami generowanymi oraz zarządzanymi przez Zakład Ubezpieczeń. Brak spełnienia tego wymo-

gu powinien zostać poparty stosowną analizą ryzyka (patrz pkt VI.2. ust. 5.a) komunikatu).

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, Zakład Ubezpieczeń powinien zapewnić, że proces wspomniany w pkt. 2 powyżej zapewnia przechowywanie kluczy w infrastrukturze Zakładu Ubezpieczeń, chyba że analiza ryzyka uzasadnia brak takiego mechanizmu.
4. W zależności od wyników analizy ryzyka (pkt VI. Ust. 2.5 komunikatu) możliwe jest stosowanie technologii HSM. HSM może być udostępniony przez dostawcę usług chmury obliczeniowej lub być zarządzany przez Zakład Ubezpieczeń. Bez względu na to, która strona udostępnia HSM, musi on spełniać wymagania FIPS 140-2 Level 2 lub równoważne.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu ubezpieczeń

1. W zależności od modelu usługi chmury obliczeniowej dokumentacja techniczna potwierdzająca, że informacje są szyfrowane kluczami generowanymi/dostarczonymi oraz zarządzanymi przez Zakład Ubezpieczeń.
2. W zależności od modelu usługi chmury obliczeniowej 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. W zależności od modelu usługi chmury obliczeniowej sformalizowany (udokumentowany) proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz przechowywaniem kopii zapasowych kluczy w infrastrukturze Zakładu Ubezpieczeń.
4. W zależności modelu usługi chmury obliczeniowej w przypadku, gdy proces zarządzania kluczami szyfrującymi nie zapewnia przechowywania kopii kluczy w infrastrukturze Zakładu Ubezpieczeń, analiza ryzyka, z której wynika uzasadniony brak takiej potrzeby.
5. Tam gdzie HSM jest wykorzystywany – dokumentacja potwierdzająca spełnienie wymagania FIPS 140-2 Level 2 lub równoważnego.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUGI 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. Tam gdzie HSM jest wykorzystywany – dokumentacja potwierdzająca spełnienie wymagania FIPS 140-2 Level 2 lub równoważnego.

SZABLONY

N/D

8. Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej

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.
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.
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, Zakład Ubezpieczeń 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, ilości logów, stosowanych przez Zakład Ubezpieczeń rozwiązań technicznych, etc. można rozważyć przekazywanie logów z chmury obliczeniowej do systemu klasy SIEM oraz opracowanie reguł korelacji pozwalających na wykrycie incydentu bezpieczeństwa w chmurze obliczeniowej.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

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

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUGI 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 w Zakładzie Ubezpieczeń.

SZABLONY

N/D

4. Wymagania w stosunku do podmiotu nadzorowanego w zakresie zarządzania dostawcami usług mającymi dostęp zdalny do usług chmury obliczeniowej wykorzystywanych przez podmiot nadzorowany:
    a) podmiot nadzorowany zapewnia, że wyłącznie uprawniony personel dostawcy usług ma dostęp do wskazanych systemów teleinformatycznych lub ich wybranych zakresów;
    b) podmiot nadzorowany wymaga używania przez personel dostawcy usług uwierzytelnienia MFA, przy czym rodzaj i zakres uzależniony jest od wyników szacowania ryzyka;
    c) podmiot nadzorowany zapewnia, że dostęp administracyjny lub o charakterze uprzywilejowanym realizowany jest z zaufanych sieci podmiotu nadzorowanego lub dostawcy usług i pod kontrolą (w tym np. poprzez nagrywanie sesji i jej parametrów, a następnie poprzez analizowanie prawidłowości i celowości realizowanych czynności), chyba że z szacowania ryzyka wynika uzasadniony brak takiej potrzeby.

OPIS WYMAGAŃ

1. Zakład Ubezpieczeń powinien zapewnić poprzez mechanizmy kontrolne lub zapisy 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 wyłącznie z przeznaczonych do tego celu i zabezpieczonych stacji roboczych/terminali, zlokalizowanych

w bezpiecznej (zaufanej) lokalizacji sieciowej.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. W zależności od modelu usługi chmury obliczeniowej udokumentowane procedury lub zapisy umowne potwierdzające zasady dostępu do informacji Zakładu Ubezpieczeń przez uprawniony personel dostawcy.
2. W zależności od modelu usługi chmurowej opis mechanizmów uwierzytelnienia.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUG CHMURY OBLICZENIOWEJ

1. W zależności od modelu usługi chmury obliczeniowej używanie przez personel dostawcy, mający dostęp zdalny do systemów wykorzystywanych w usłudze chmury obliczeniowej Zakładu Ubezpieczeń, uwierzytelnienia MFA oraz bezpiecznych stacji w bezpiecznych lokalizacjach sieciowych.
2. W zależności od modelu usługi chmury obliczeniowej oraz w zależności od wyników analizy ryzyka przeprowadzanej przez Zakład Ubezpieczeń mogą być stosowane inne mechanizmy zapewniające monitorowanie dostępu i rozliczalność działań dostawcy, np. nagrywanie sesji i jej parametrów w przypadku dostępu administracyjnego dostawcy lub dostępu personelu Zakładu Ubezpieczeń o charakterze uprzywilejowanym.

SZABLONY

N/D

9. Dokumentowanie działań podmiotu nadzorowanego

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.

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. Punkt VII.9 komunikatu określa wymogi organizacyjne i dokumentacyjne, które Zakład Ubezpieczeń powinien spełniać (np. w wdrożonym charakterze polityk lub innych regulacji), chcąc wdrażać usługi chmury obliczeniowej.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Udokumentowanie schematu organizacji pracowników lub współpracowników Zakładu Ubezpieczeń odpowiedzialnych za bezpieczeństwo, w tym cyberbezpieczeństwo, z uwzględnieniem elementów z pkt 9.1. a) komunikatu.
2. Udokumentowanie architektury sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych Zakładu Ubezpieczeń z sieciami niezaufanymi, w tym architektury wdrażanego rozwiązania w chmurze obliczeniowej z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych.
3. Udokumentowanie zasad klasyfikacji informacji lub systemów pod kątem przetwarzania w chmurze obliczeniowej.
4. Udokumentowane zasady (polityka) stosowanych w organizacji zabezpieczeń technologicznych i rozwiązań organizacyjnych w odniesieniu do rozwiązań w chmurze obliczeniowej.
5. Udokumentowane zasady (polityka) zarządzania ciągłością działania.
6. Dla wdrażanej usługi chmury obliczeniowej, udokumentowane zasady bieżącego zabezpieczania przetwarzanych informacji, jak również dla sytuacji planowanego lub nieplanowanego zakończenia współpracy z dostawcą usługi chmury obliczeniowej.
7. Udokumentowane zasady (polityka) zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi.
8. Udokumentowane zasady (polityka) przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem chmury obliczeniowej (np. coroczny przegląd).
9. Udokumentowane zasady (polityka) raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej.
10. Umowa z dostawcą usługi chmury obliczeniowej wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań.
11. Opis procesów, procedury lub instrukcje, dotyczące obszarów wskazanych w podpunktach i. do vi. pkt 9.1. komunikatu.
12. Udokumentowane zasady zarządzania politykami i dokumentacją w ramach systemu zarządzania organizacją, zapewniające ochronę przed nieuprawnionym dostępem, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUGI CHMURY OBLICZENIOWEJ

N/D

SZABLONY

N/D

5.5. 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 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 1. do niniejszego komunikatu.

OPIS WYMAGAŃ

1. Z zastrzeżeniem ust. 2 i 3, komunikat wymaga poinformowania UKNF o zamiarze przetwarzania informacji w chmurze obliczeniowej (w przypadku umowy zawieranej przez Zakład Ubezpieczeń z dostawcą lub dostawcą usługi chmury obliczeniowej), gdy:
    1) usługi chmury obliczeniowej stanowią Outsourcing szczególny, lub
    2) w chmurze obliczeniowej przetwarzane są Informacje prawnie chronione,
    3) jeżeli podmiot nadzorowany korzysta z usługi chmurowej dostarczonej przez inny Zakład Ubezpieczeń i wykorzystuje ją do wykonywania czynności na rzecz tego podmiotu, to obydwa podmioty dokonują oddzielnych notyfikacji. Przykładowo w relacji Zakład Ubezpieczeń – agent ubezpieczeniowy, jeżeli ten drugi korzysta z usługi chmurowej dostarczanej przez Zakład Ubezpieczeń, to zarówno Zakład (niezależnie od tego, z iloma agentami współpracuje), jak i agent dokonują oddzielnych notyfikacji we własnym zakresie wykorzystywania chmury.
2. W przypadku współpracy Zakładu Ubezpieczeń z innym podmiotem nadzorowanym, nie ma on obowiązku dokonywania oddzielnych notyfikacji uwzględniają-

cych korzystanie z chmury przez Zakład Ubezpieczeń, któremu powierzono przetwarzanie, jeżeli korzystanie z chmury jest jego autonomiczną decyzją. W tym, z uwzględnieniem:

1) w relacji Zakład Ubezpieczeń – agent ubezpieczeniowy, jeżeli ten drugi autonomicznie korzysta z usług chmurowych (niedostarczonych przez Zakład Ubezpieczeń), to Zakład Ubezpieczeń nie ma obowiązku notyfikowania korzystania z chmury i tylko agent ubezpieczeniowy notyfikuje UKNF korzystanie z chmury.
2) każdy Zakład Ubezpieczeń prowadzi ewidencję umów outsourcingu chmurowego. Zalecane jest aby ewidencja, w zakresie usług chmury obliczeniowej, uwzględniała również informacje wymienione w Załączniku 1. do komunikatu. Ewidencja umów outsourcingu chmurowego może nie stanowić ewidencji umów outsourcingu w rozumieniu art. 77 ustawy o działalności ubezpieczeniowej i reasekuracyjnej.

3. W przypadku niespodziewanych okoliczności (sytuacji), które miałyby wpływ na stosowanie komunikatu – Zakład Ubezpieczeń modyfikuje treść składanego oświadczenia zgodnie ze stanem faktycznym i informuje o tym UKNF odrębnym pismem z wyjaśnieniami.
4. Zgłoszenia należy dokonać co najmniej 14 dni przed rozpoczęciem przetwarzania informacji (niezależnie od samej daty zawarcia umowy) w chmurze obliczeniowej. Oznacza to, że nie ma znaczenia samo zawarcie umowy z dostawcą, ale data rozpoczęcia przetwarzania informacji w chmurze obliczeniowej, w tym Informacji prawnie chronionych (bez względu czy w fazie przedprodukcyjnej czy już w fazie produkcyjnej).
5. Uprawnionym do podpisania informacji, o której mowa w pkt VIII komunikatu jest zarówno zarząd Zakładu Ubezpieczeń (zgodnie z reprezentacją w KRS), jak i osoby właściwie przez zarząd umocowane. Decyzja może mieć formę uchwały zarządu.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie Zakładu Ubezpieczeń

1. Wypełniony i podpisany przez odpowiednio umocowane osoby Załącznik 1 komunikatu.

WYMAGANIA (produkty) DO OPRACOWANIA po stronie dostawcy USŁUGI CHMURY OBLICZENIOWEJ

N/D

SZABLONY

1. Załącznik 10. – Przykładowe wypełnienie informacji do UKNF o rozpoczęciu korzystania z chmury obliczeniowej przez Zakład Ubezpieczeń

1. 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.
2. Okresowa weryfikacja i aktualizacja powinna być prowadzona zgodnie z praktyką i zasadami podmiotu nadzorowanego, jednak nie rzadziej niż raz w roku.
3. 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.
4. 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.
5. Wymagania te uwzględnia podmiot nadzorowany w swoim podejściu do stosowania usług chmury obliczeniowej, a w szczególności w procesie szacowania ryzyka.
6. System and Organization Controls.
7. Oznacza domyślną konfigurację usługi chmury obliczeniowej, która uwzględnia wymagania bezpieczeństwa przetwarzania informacji, w szczególności zapobiega przypadkowemu (niezamierzonemu) ujawnieniu przetwarzanej informacji.
8. HSM – Hardware Security Module, urządzenie do przechowywania i zarządzania kluczami kryptograficznymi.
9. Federal Information Processing Standard – publiczne standardy dla agencji cywilnych i rządowych w USA. W tym przypadku międzynarodowy standard bezpieczeństwa dla systemów kryptograficznych.
10. 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.
11. Chyba że szczególny przepis prawa dotyczący działalności podmiotu nadzorowanego przewiduje inny termin przekazania informacji.

ZAŁĄCZNIKI

Załącznik 1. Przykład szablonu klasyfikacji informacji

Załącznik 2. Przykład szablonu szacowania ryzyka

Załącznik 3. Przykładowy plan przetwarzania informacji w chmurze obliczeniowej

Załącznik 4. Przykładowy szablon scenariusza wyjścia z chmury

Załącznik 5. Przykład – Wyjście z chmury – główne zagadnienia

Załącznik 6. ISO 27001

Załącznik 7. Przykładowe kroki wdrożenia usługi przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej w zakładzie ubezpieczeń

Załącznik 8. Przykład – Proces wdrożenia

Załącznik 9. Przykład – opis metodyki uzyskania szacowania ryzyka i zgodności z komunikatem UKNF

Załącznik 10. Przykładowe wypełnienie informacji do UKNF o rozpoczęciu korzystania z chmury obliczeniowej przez zakład ubezpieczeń

Załącznik 1. **Przykład szablonu klasyfikacji informacji**

TABELA 1

Lp.	Nazwa kategorii informacji	Właściciel informacji	Przykłady informacji	Zasoby informatyczne, w których informacje są przetwarzane	Ocena atrybutów bezpieczeństwa			Wartość informacji	Poziom ochrony informacji*
					Poufność	Dostępność	Integralność		
1.									
2.									
3.									

TABELA 2

Atrybut bezpieczeństwa	Stosowane zabezpieczenia	Poziom ochrony informacji*				
		Klasa A	Klasa B	Klasa C	Klasa D	Klasa E
Poufność						
Integralność						
Dostępność						

* Dla każdej kategorii informacji należy określić poziom ochrony stosowanych zabezpieczeń (np. szyfrowanie, multi factor authentication, backupy)

Załącznik 2. **Przykład szablonu szacowania ryzyka**

Lp.	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*	Osoba odpowiedzialna	Termin wdrożenia
1.	Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	Usługa chmury obliczeniowej świadczona jest w lokalizacjach: 1)..... 2).....								
2.	Możliwość utraty zgodności postępowania podmiotu nadzorowanego 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 (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 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)									

Załącznik 2. **Przykład szablonu szacowania ryzyka**

11.	Możliwość korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego (VI.2.2.a)									
12.	Możliwość jednostronnej zmiany warunków technicznych korzystania z usługi (VI.2.2.b)									
13.	Stosowanie domyślnych lub 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)									

* 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 3. **Przykładowy plan przetwarzania informacji w chmurze obliczeniowej**

1. Informacje o realizowanych zadaniach i przetwarzanych informacjach	
Nazwa systemu /aplikacji, której informacje są przetwarzane	
Opis zadania realizowanego za pomocą usługi	
Rodzaj przetwarzanych informacji	
Klasa przetwarzanych informacji[1]	
Typ informacji	
Outsourcing szczególny	
Opis formatu i struktury informacji	
2. Ochrona informacji	
Mechanizmy zabezpieczenia informacji	
Opis mechanizmów zabezpieczenia informacji	
Opis mechanizmów szyfrowania informacji	
Zarządzanie i przechowywanie kluczy szyfrujących	
Opis kontroli dostępu do przetwarzanych informacji	
3. Umowa z dostawcą	
Dostawca	
Nr 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	

Załącznik 4. **Przykładowy szablon scenariusza wyjścia z chmury**

1. Opis usługi	
Identyfikator umowy	
Usługa (przedmiot umowy)	
Dostawca (nazwa/firma przedsiębiorcy)	
Planowana data zakończenia przetwarzania danych w chmurze:	
Okres wypowiedzenia umowy: a) przez Zakład Ubezpieczeń b) przez dostawcę	
2. 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 Zakładu Ubezpieczeń: ☐ Przejęcie działalności przez jednostkę Zakładu Ubezpieczeń Zaprzestanie działalności: ☐ Brak kontynuowania działalności po wygaśnięciu umowy Inne: ☐ ..... ☐ .....
3. Kluczowe działania umożliwiające realizację scenariusza wyjścia	
Przedłużenie relacji	
Realizacja usługi przez inny podmiot	
Realizacja usługi przez Zakład Ubezpieczeń (powrót do Zakładu Ubezpieczeń)	
Zaprzestanie działalności będącej przedmiotem umowy	
Inne	Przykłady:
4. Zaangażowane jednostki Zakładu Ubezpieczeń realizujące scenariusz wyjścia	
Jednostki realizujące scenariusz	
Jednostki wspierające	
Jednostki informowane o wdrożeniu scenariusza	

5. Historia dokumentu

Data utworzenia /przeglądu /zmiany	Zatwierdzający (Dyrektor/Manager Zespołu w jednostce Właściciela Funkcjonalnego)	Komentarz/zakres zmian

Załącznik 5. **Przykład – Wyjście z chmury – główne zagadnienia**

WSTĘP

W zależności od procesu oraz modelu usługi chmury obliczeniowej należy opracować odpowiedni plan wyjścia z usługi chmury obliczeniowej. Poniżej zostały przedstawione zagadnienia, na które w zależności od sytuacji należy zwrócić uwagę przy opracowywaniu planu wyjścia z chmury obliczeniowej. W przypadku procesów wspomagających działalność ubezpieczeniową, których wyłączenie nie będzie miało istotnego wpływu na prowadzoną działalność, poniższe zagadnienia mogą nie mieć zastosowania.

Rozdział I
PLAN WYCOFANIA USŁUGI

1. Scenariusze wycofania

1. Należy określić przewidywane scenariusze wycofania dla usługi np. migracja on premise, zmiana dostawcy usług chmury obliczeniowej, etc.
2. Dopuszczalne jest określenie alternatywnych scenariuszy w zależności od sytuacji – np. nagłe zaprzestanie świadczenia usługi, rezygnacja z usługi po zakończeniu kontraktu, etc.
3. Scenariusze wycofania mogą być testowane m.in. w ramach gry sztabowej.

2. Wpływ zmiany na organizację

1. Należy opisać wpływ zmiany na organizację, tj. zmiany w procesach krytycznych, wpływ na zasoby ludzkie i strukturę organizacyjną, wymagania szkoleniowe, etc.

3. Opis transferu usługi CHMURY OBLICZENIOWEJ oraz danych

1. Przez opis transferu usługi chmury obliczeniowej oraz danych należy rozumieć wysokopoziomowy opis procesu migracji usługi chmury obliczeniowej oraz danych, wymaganych narzędzi etc.
2. Transfer usług chmury obliczeniowej to całokształt działań (w tym czynności prawnych) prowadzących do zwrotu Zakładowi Ubezpieczeń sprzętu Zakładu Ubezpieczeń, oprogramowania Zakładu Ubezpieczeń, całości przetwarzanych na zlecenie Zakładu Ubezpieczeń danych Zakładu Ubezpieczeń oraz w zależności od okoliczności prawnych, przeniesienia na Zakład Ubezpieczeń umów z osobami trzecimi wymaganych do realizacji usług zdefiniowanych w umowie, w sposób gwarantujący nieprzerwaną realizację usług chmury obliczeniowej.

4. Scenariusze testowe wycofania i kryteria akceptacji

1. Zakład Ubezpieczeń powinien opracować scenariusze testowe dla procesów migracji.
2. Zakład Ubezpieczeń wraz z dostawcą usług chmury obliczeniowej jest zobowiązany do wykonywania testów Planu Wyjścia.

5. Backup danych i czasy migracji

1. Należy oszacować czas potrzebny na przygotowanie projektu przełączenia, uruchomienia prac operacyjnych, uzyskaniu odpowiednich zgód i poinformowanie użytkowników usługi chmury obliczeniowej o planowanym przełączeniu.
2. Konieczne jest określenie czasu pobrania danych do migracji od dostawcy usług chmury obliczeniowej. Czas musi uwzględniać zapisy umowne z dostawcą usług chmury obliczeniowej na wyodrębnienie danych i fizyczne ich przekazanie (w tym warunki sieciowe i czas na zamontowanie danych).
3. Konieczne jest określenie czasu dla procesu przełączenia usługi w wymiarze inicjalnym i docelowym migracji danych, a także uruchomieniu usługi na odtworzonych danych. Czas ten nie może naruszać przyjętego RTO i RPO dla usługi.

4. Dla usług o znaczeniu krytycznym dla ciągłości działania Zakładu Ubezpieczeń należy przechowywać backup lokalny danych przekazanych do chmury obliczeniowej celem minimalizacji czasu przełączenia usługi. Zakres backupu i czas retencji danych powinien zostać zdefiniowany z punktu widzenia ryzyka dla ciągłości działania. Backup ma na celu jedynie minimalizację czasu inicjalnego przełączenia najbardziej krytycznych danych. Całkowity czas migracji zakłada pozyskanie wszystkich danych od dostawcy usług chmury obliczeniowej.

6. Harmonogram migracji

1. Należy uwzględnić szacunkowy harmonogram migracji na „on-premise" lub do innej usługi.
2. Zaleca się przygotowanie harmonogramu projektowego uwzględniającego m.in. wymagane zasoby, zadania i kamienie milowe.

7. Role i odpowiedzialności

1. Konieczne jest określenie ról i odpowiedzialności Zakładu Ubezpieczeń i dostawcy usług chmury obliczeniowej w procesie migracji.
2. Należy określić obowiązki dostawcy usług chmury obliczeniowej
3. W razie wypowiedzenia lub rozwiązania umowy, niezależnie od przyczyny, dostawca usług chmury obliczeniowej powinien zapewnić Zakładowi Ubezpieczeń, niezwłocznie po wygaśnięciu lub rozwiązaniu umowy, możliwość transferu Danych Zakładu Ubezpieczeń poprzez:
    1) umożliwienie Zakładowi Ubezpieczeń pobrania Danych Zakładu Ubezpieczeń ze swojej infrastruktury w terminie ustalonym przez Zakład Ubezpieczeń i dostawcę usług chmury obliczeniowej;
    2) wydanie loginów i haseł zgodnie z umową;
    3) zapewnienie właściwej ochrony danych Zakładu Ubezpieczeń znajdujących się w logach systemów współdzielonych;
    4) zwrot sprzętu Zakładu Ubezpieczeń wniesionego do infrastruktury dostawcy usług chmury obliczeniowej, jeśli taka sytuacja miała miejsce;
    5) zwrot dokumentacji w wersji papierowej (o ile taka istniała).
4. Dostawca usług chmury obliczeniowej powinien zapewnić, w zależności od okoliczności prawnych, Zakładowi Ubezpieczeń możliwość ciągłego, nieprzerwanego korzystania z licencji niezbędnych do podtrzymania ciągłości działania usług, w tym zapewnić możliwość przeniesienia na Zakład Ubezpieczeń licencji, o których mowa w punkcie powyżej.
5. Dostawca usług chmury obliczeniowej powinien zostać zobowiązany do:
    1) usunięcia w sposób nieodwracalny danych Zakładu Ubezpieczeń oraz oprogramowania Zakładu Ubezpieczeń z zasobów dostawcy usług chmury obliczeniowej oraz Podwykonawców współpracujących;
    2) usunięcia w sposób nieodwracalny danych Zakładu Ubezpieczeń z zasobów dostawcy usług chmury obliczeniowej oraz Podwykonawców współpracujących, w szczególności mających charakter danych osobowych oraz danych objętych tajemnicą ubezpieczeniową lub zawodową;
    3) współpracy z Zakładem Ubezpieczeń w zakresie transferu danych do Zakładu Ubezpieczeń lub innego podmiotu wskazanego przez Zakład Ubezpieczeń;
    4) zapewnienia współpracy jego Podwykonawców w zakresie realizacji planu wyjścia;
    5) określenia wspólnie z Zakładem Ubezpieczeń: a) szczegółowego harmonogram planu wyjścia, b) szczegółowego zakresu prowadzonych czynności, c) szczegółowego sposobu realizacji planu wyjścia, d) odpowiedzialności Stron, e) środki techniczne niezbędne do realizacji planu wyjścia, jeśli są potrzebne.

8. Wymagania dla wycofywania usługi (sprzęt, etc.)

8.1. Scenariusz 1 migracja „on-premise”

1. Należy zdefiniować parametry środowiska lokalnego w zakresie dostępności, wydajności i pojemności w celu przejęcia usługi chmury obliczeniowej, w której się w niej znajdują.
2. Plan wyjścia powinien w szczególności obejmować także:
    1) wyznaczenie dedykowanych managerów odpowiedzialnych za przeprowadzenie procesu transferu usług chmury obliczeniowej;
    2) przygotowanie, w uzgodniony przez Strony sposób, do transportu całości sprzętu Zakładu Ubezpieczeń, jeżeli taki był elementem świadczenia usług;
    3) wydanie Zakładowi Ubezpieczeń haseł i loginów pozwalających na dalsze korzystanie z danych Zakładu Ubezpieczeń, w tym haseł i loginów do baz danych oraz wszystkich systemów objętych usługami;
    4) przekazanie przez dostawcę usług chmury obliczeniowej wszystkich informacji dotyczących sposobu dostarczania i obsługi świadczonych usług istotnych z punktu widzenia przeniesienia usług i przekazania kompetencji utrzymaniowych innemu podmiotowi;
    5) zapewnienie po stronie dostawcy usług chmury obliczeniowej bezpiecznego połączenia teleinformatycznego platformy, wykorzystywanej do świadczenia usług chmury obliczeniowej, do systemu informatycznego wskazanego przez Zakład Ubezpieczeń, z wykorzystaniem bezpiecznej sieci teleinformatycznej, w celu przeprowadzenia transferu danych Zakładu Ubezpieczeń;
    6) zapewnienie przez Zakład Ubezpieczeń środków technicznych po stronie systemu informatycznego Zakładu Ubezpieczeń umożliwiających zestawienie połączenia teleinformatycznego;
    7) zapewnienie transferu do systemu teleinformatycznego wskazanego przez Zakład Ubezpieczeń całości danych Zakładu Ubezpieczeń, w sposób zapewniający ich pełne bezpieczeństwo oraz integralność i poziom transferu umożliwiający sprawne przeniesienie wszystkich danych Zakładu Ubezpieczeń w czasie uzgodnionym przez Strony, a także wydania wszystkich kopii zapasowych danych Zakładu Ubezpieczeń (o ile były sporządzane zgodnie z umową);
    8) przekazanie przez dostawcę usług chmury obliczeniowej wiedzy specyficznej dla realizowanych usług chmury obliczeniowej, w takim zakresie, w jakim będzie to niezbędne do dalszej realizacji usług przez Zakład Ubezpieczeń lub podmiot trzeci wskazany przez Zakład Ubezpieczeń;
    9) niezwłocznie po zakończeniu świadczenia usług chmury obliczeniowej usunięcie przez dostawcę usług chmury obliczeniowej oraz Podwykonawców dostawcy usług chmury obliczeniowej, w sposób trwały oraz zgodny z najlepszymi praktykami w tym zakresie, całości ewentualnie posiadanych kopii danych Zakładu Ubezpieczeń (po uprzednim transferze takich danych do Zakładu Ubezpieczeń lub podmiotu wskazanego przez Zakład Ubezpieczeń) oraz wszystkich danych i informacji (np. plików konfiguracyjnych specyficznie wykorzystywanych dla danego Zakładu Ubezpieczeń a nie stanowiących części usług dostarczanych przez dostawcę usług chmury obliczeniowej) wykorzystywanych do konfiguracji, obsługi, backupu i archiwizacji systemu lub poszczególnych jego elementów.
3. Wymagania uwzględniają:
    1) odpowiednią ilość serwerów wraz z określeniem ich lokalizacji w centrach danych;
    2) przewidują wolne miejsce w centrach danych wraz z zapewnieniem fizycznej możliwości wpięcia w infrastrukturę;
    3) odpowiednią konfigurację serwerów, zapewniającą odpowiednią wydajność (odpowiednia ilość procesorów, odpowiednia ilość pamięci RAM, odpowiednie połączenia sieciowe, odpowiednie zasoby dyskowe);

4) odpowiednią ilość przestrzeni dyskowej, która jest niezbędna do przejęcia danych przechowywanych w usłudze chmury obliczeniowej. Przestrzeń ta musi zostać przewidziana na okres jednego roku i aktualizowana raz do roku w planie przełączenia.

4. Zdefiniowane środowisko jest dostępne w jednym z poniższych podejść:
    1) fizycznie zakupione i skonfigurowane na potrzeby migracji;
    2) nie zakupione, ale dostępne u producenta w podanej konfiguracji. Taka dostępność potwierdzona jest listem intencyjnym lub umową z dostawcą usług chmury obliczeniowej w której określony jest czas pozyskania i dostarczenia infrastruktury;
    3) posiadana jest infrastruktura wykorzystywana do innych celów, która może zostać w razie uruchomienia planu zwolniona i w okresie przejściowym do zakupu, może zostać użyta celem wykonania przełączenia.

8.2. Scenariusz 2 migracja do innego dostawcy usług CHMURY OBLICZENIOWEJ

1. Alternatywne usługi chmury obliczeniowej wraz z dostawcami usług chmury obliczeniowej, czasem uruchomienia i kosztem.

Usługa alternatywna	Kluczowe funkcjonalności niedostępne w usłudze alternatywnej	Czas uruchomienia usługi / Szacunkowy czas migracji	Koszt

2. Należy określić minimalne wymagania bezpieczeństwa dla wycofania z usługi chmury obliczeniowej, w tym:
    1) wymagania bezpieczeństwa dla docelowego rozwiązania po wycofaniu;
    2) wymagania bezpieczeństwa dla procesu migracji.
3. Na potrzeby opisu procesu migracji danych i przełączenia usługi powinny zostać opracowane instrukcje wykonawcze dla wszystkich ról zdefiniowanych w procesie. Proces powinien uwzględniać poniższe punkty wraz z ich operacyjnym rozwinięciem i technicznym uszczegółowieniem.
    1) formalna decyzja o wycofaniu lub przełączeniu. Określenie zasad wydania takiej decyzji i jej trybu;
    2) poinformowanie użytkowników o uruchomieniu planu przełączenia, wraz z podaniem przewidywanych czasów i skutków dla użytkowników;
    3) pozyskanie i skonfigurowanie infrastruktury;
    4) wyodrębnienie danych od dostawcy usług chmury obliczeniowej i fizyczne ich przekazanie;
    5) zamontowanie danych z backupu w środowisku Zakładu Ubezpieczeń i poinformowanie o inicjalnym uruchomieniu usługi;
    6) zamontowanie danych od dostawcy usług chmury obliczeniowej i poinformowanie o pełnym przełączeniu usługi.
4. Zakład Ubezpieczeń może podjąć decyzję o wyłączeniu realizacji niektórych zobowiązań wynikających z planu wyjścia. W przypadku podjęcia takiej decyzji przez Zakład Ubezpieczeń, Strony dostosowują plan wyjścia do zmian wprowadzonych przez Zakład Ubezpieczeń – w szczególności w związku z rezygnacją z określonych zadań Zakład Ubezpieczeń może żądać skrócenia harmonogramu realizacji planu wyjścia.
5. Strony w czasie realizacji planu wyjścia zapewnią personel techniczny o kompetencjach i wiedzy umożliwiającej realizację uzgodnionego przez Strony planu wyjścia w uzgodnionym terminie.

6. Strony zapewnią dostęp do informacji niezbędnych do wykonania powierzonych zadań w ramach planu wyjścia, w tym szczegóły dotyczące odpowiedniego systemu informatycznego.
7. Strony w trakcie trwania umowy przygotowują szczegółowe plany wyjścia dla poszczególnych usług oraz zobowiązują się do ich częściowego lub całościowego przetestowania w trakcie trwania umowy.
8. Cały proces wyjścia powinien zakończyć się podpisaniem protokołu, w którym jedna strona potwierdza przejęcie sprzętu, licencji, oprogramowania itp., druga strona potwierdza usunięcie danych Zakładu Ubezpieczeń.
9. Strony w trakcie trwania umowy dokonają przybliżonej oceny kosztów planu wyjścia

Rozdział II
PLAN NAGŁEGO ZAPRZESTANIA ŚWIADCZENIA USŁUGI CHMURY OBLICZENIOWEJ

1. W przypadku nagłego i długotrwałego braku dostępu do usługi z powodu problemów po stronie dostawcy usług chmury obliczeniowej (dłuższe niż zakłada SLA) przewidując przywrócenie usługi w określonym czasie, należy wykonać plan znajdujący się w tym punkcie.
2. Wymagania techniczne zbieżne z rozdziałem I, przy założeniu powrotu do wykorzystywanej usługi chmury obliczeniowej:
    1) określenie jakie konta i jakie uprawnienia zostaną użyte do przełączenia;
    2) przełączenie usługi zakłada dostęp tylko do wybranego zakresu danych w trybie nagłym. Należy podać zakres i typ danych jaki będzie dostępny i jak zostanie pozyskany. Przyjmuje się zatem ryzyko nieposiadania dostępu do całości danych i uruchomienia funkcjonalności przesyłania wiadomości bieżących;
    3) udokumentowane instrukcje dla Administratorów Systemów wraz przygotowanymi zgłoszeniami serwisowymi (RFC) dla wszystkich zadań przełączenia;
    4) w przypadku problemów na poziomie krytycznym powiadamiany jest odpowiedni dział w ramach struktury IT Zakładu Ubezpieczeń oraz uruchamiane jest wsparcie dostawcy usług chmury obliczeniowej w ramach wykupionej usługi wsparcia. Równolegle rejestrowany jest problem, którego obsługa realizowana jest w ramach oddzielnego procesu problem managementu Zakładu Ubezpieczeń;
    5) jeżeli Zakład Ubezpieczeń nie ma zdefiniowanego procesu problem management, należy opracować także dedykowaną instrukcję, role i zadania dla koordynatora przełączenia usługi. Instrukcja taka zawiera przede wszystkim zasady poinformowania użytkowników o przełączeniu usługi;
    6) powrót do usługi chmury obliczeniowej jest opisany jako powyżej poprzez instrukcje dla administratorów i rozpisane zadania.

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

ISO27001 – opis kontroli po stronie dostawcy							
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 odstępch 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 nieumyślnej modyfikacji lub nadużycia organów organizacji.	Tak			Samoocena	
A.6.1.3	Kontakty z organami władzy	Zabezpieczenie Należy utrzymywac stosowne kontakty z własciwymi 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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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 zmian 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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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.9.2.2	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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

A.9.2.3	Zarządznie 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	
36959	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 Dosteę 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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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 zewnętrzymi 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, odizolowac 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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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 licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.	Tak			Samoocena	
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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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 nieuprawnionymi 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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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, których dotyczą oraz ponownego szacowania ryzyka.	Tak			Samoocena	
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 bezpieczeństwem informacji	Zabezpieczenie Reakcja na incydenty związane z bezpieczeństwem informacji powinna być zgodna z udokumentowanymi procedurami.	Tak			Samoocena	
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Zabezpieczenie Wiedzę zdobytą 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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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 aktualności i skuteczności w niekorzystnych sytuacjach.	Tak			Samoocena	
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	

Załącznik 6. Przykładowy szablon scenariusza wyjścia z chmury

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	Sprawdzanie zgodności technicznej	Zabezpieczenie Należy regularnie przeglądać systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa informacji i standardami obowiązującymi w organizacji.	Tak			Samoocena	

Załącznik 7. **Przykładowe kroki wdrożenia**

1. WSTĘP

Niniejszy dokument opisuje przykładowe kroki wdrożenia usługi przetwarzania informacji w chmurze obliczeniowej, przy założeniu, że komunikat ma zastosowanie. Opisane w dokumencie kroki mogą mieć częściowe zastosowanie w zależności od procesu oraz modelu usługi chmury obliczeniowej. Proces wdrożenia w przypadku, gdy komunikat nie ma zastosowania, jest poza zakresem niniejszego dokumentu.

Zidentyfikowanie potrzeby biznesowej

1. Na tym etapie identyfikowana i dokumentowana jest potrzeba biznesowa, zgodnie z procesami obowiązującymi w Zakładzie Ubezpieczeń.
2. Otwierany jest projekt, uruchamiany proces zarządzania zmianą lub inna inicjatywa, która pozwala na przypisanie prac i zadań związanych z krokami opisanymi poniżej.
3. Jednostki odpowiedzialne za architekturę, technologię oraz bezpieczeństwo określają zasadność dalszej analizy niniejszej potrzeby pod kątem możliwości realizacji usługi w chmurze obliczeniowej.

Produkty

1. Opis wymagań biznesowych.
2. Wniosek lub zgłoszenie otwierające projekt, zmianę lub inną inicjatywę.

2. WSTĘPNA OCENA POD KĄTEM MOŻLIWOŚCI REALIZACJI POTRZEBY W USŁUDZE CHMURY OBLICZENIOWEJ

1. Na tym etapie dokonywana jest wstępna ocena („pre-assessment") potrzeby pod kątem realizacji usługi w chmurze obliczeniowej, tj.:
    1) porównanie rozwiązań w usłudze chmury obliczeniowej vs. on-premise – wstępna ocena realizacji wymagań i kosztów, w tym analiza potencjalnych dostawców usług chmury obliczeniowej;
    2) architektura, integracja, docelowa konfiguracja – zgodność z docelową architekturą Zakładu Ubezpieczeń;
    3) wstępne PoC rozwiązania, jeśli planowane jest wykorzystanie całkowicie nowych dla Zakładu Ubezpieczeń technologii;
    4) inwentaryzacja i klasyfikacja informacji, klasyfikacja istotności usługi chmury obliczeniowej – w zależności od wyników podejmowana jest wstępna decyzja pod kątem zastosowania komunikatu;
    5) zbadanie możliwości pozyskania kompetencji dla usługi chmury obliczeniowej i on-premise;
    6) zgodność ze strategią Zakładu Ubezpieczeń;
    7) zgodność z regulacjami wewnętrznymi.

Produkty

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

3. PUNKT DECYZYJNY LUB DECYZJA O DOPUSZCZALNOŚCI WDROŻENIA USŁUGI CHMURY OBLICZENIOWEJ

1. Na tym etapie podejmowana jest decyzja o dalszym procesowaniu potrzeby, która zakłada poniższe scenariusze:
    1) brak możliwości lub uzasadnienia do wykorzystania usługi chmury obliczeniowej;
    2) dopuszczalne wdrożenie usługi chmury obliczeniowej – z zastrzeżeniem spełnienia wymagań komunikatu, w przypadku gdy ma on zastosowanie;
    3) dopuszczalne wdrożenie usługi chmury obliczeniowej – w przypadku, gdy komunikat nie ma zastosowania.
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 Zakładu Ubezpieczeń).

4. OPRACOWANIE WYMAGAŃ DO WDROŻENIA USŁUGI CHMURY OBLICZENIOWEJ ZGODNIE Z KOMUNIKATEM

1. Na tym etapie tworzony jest zestaw wymagań biznesowych, formalnych, bezpieczeństwa lub innych. Wymagania są określane na podstawie wymagań wewnętrznych regulacji Zakładu Ubezpieczeń oraz komunikatu.
2. Przy tworzeniu wymagań można uwzględnić poniższe kwestie:
    1) Czy istnieją na rynku usługi chmury obliczeniowej posiadające referencje w branży finansowej, w szczególności ubezpieczeniowej?
    2) Czy potencjalni oferenci mogą zapewnić CPD na terenie EOG?
    3) Czy możliwe jest zapewnienie odpowiednich kompetencji po stronie Zakładu Ubezpieczeń? Czy są wymagane dodatkowe szkolenia dla pracowników? Jakie są możliwości na rynku? Z jakimi kosztami należy się liczyć?
    4) Czy dostawca usług chmury obliczeniowej potwierdza zgodność przetwarzania danych osobowych ze standardami wewnętrznymi Zakładu Ubezpieczeń i powszechnie obowiązującymi przepisami prawa?
    5) Czy chmura obliczeniowa będzie w stanie zapewnić wymaganą pojemność i wydajność?
    6) Zasady przekazywania informacji odnośnie zdarzeń naruszenia bezpieczeństwa informacji, rozumianego jako poufność, integralność i dostępność przetwarzanych informacji i zasobów, ze szczególnym uwzględnieniem Informacji prawnie chronionych.
    7) Zasady bezpiecznego i trwałego niszczenia informacji w chmurze obliczeniowej.
    8) Monitorowanie parametrów działania usług chmury obliczeniowej, z których miałby korzystać Zakład Ubezpieczeń.
    9) Zasady zakończenia współpracy z dostawcą usług chmury obliczeniowej.
    10) Wykonywanie zobowiązań wynikających z umowy, w ustalonym zakresie i terminie, z zachowaniem należytej staranności, z uwzględnieniem zawodowego charakteru prowadzonej działalności gospodarczej oraz aktualnego stanu wiedzy z dziedziny ubezpieczeń i technologii informatycznych.
3. Wymagania wynikające z komunikatu względem dostawcy usług chmury obliczeniowej zostały wskazane w Zestawieniu wymagań (Wymagania (produkty) do opracowania po stronie dostawcy usługi chmury obliczeniowej), będących częścią Standardu.

Produkty

1. Udokumentowane wymagania do usługi chmury obliczeniowej.

5. OPRACOWANIE I DYSTRYBUCJA ZAPYTANIA OFERTOWEGO

1. Przed uruchomieniem procesowania zapytania, należy zweryfikować, czy istnieją w Zakładzie Ubezpieczeń umowy adresujące wymagania z pkt 4 w zakresie możliwości ich wykorzystania.
2. Na tym etapie dokument zapytania ofertowego jest opracowywany i wysyłany do dostawców usług chmury obliczeniowej. Odpowiedzi na zapytanie powinny zawierać w miarę możliwości informacje o spełnieniu wymagań określonych w pkt 4 powyżej.

Produkty

1. Zapytanie ofertowe.
2. Odpowiedzi na zapytanie.

6. OCENA RYZYKA ZWIĄZANEGO Z USŁUGĄ CHMUROWĄ

1. Na podstawie odpowiedzi dostawców usług chmury obliczeniowej, w szczególności odpowiedzi na wymagania wynikające z komunikatu wskazane w Zestawieniu wymagań, przeprowadzana jest ocena ryzyka dla oferowanych usług chmury obliczeniowej. Zestawienie wymagań określa 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.
2. Oferty, które nie spełniają minimalnych wymagań, powinny zostać odrzucone.
3. Wynik analizy ryzyka, łącznie z wymaganiami funkcjonalnymi, aspektami finansowymi, etc., jest podstawą do podjęcia decyzji o wyborze dostawcy usług chmury obliczeniowej dla danego przedsięwzięcia.

Produkty

1. Wstępna ocena ryzyka (dla ofert, które nie zostały odrzucone).
2. Proponowany plan postępowania ze zidentyfikowanymi rodzajami ryzyka.

7. OCENA OFERT I AKCEPTACJA OFERTY

1. Na tym etapie, obok kwestii biznesowych, dokonywany jest wybór oferty oraz finalna ocena ryzyka dla wybranej oferty.
2. Dokonywane są też uzgodnienia wspólnie z dostawcą usług chmury obliczeniowej co do środków postępowania z ryzykiem i opracowywany jest finalny plan postępowania ze zidentyfikowanymi ryzykami.

Produkty

1. Wybór oferty wraz z uzasadnieniem.
2. Zaktualizowana ocena ryzyka (dla wybranej oferty).
3. Uzgodniony z dostawcą usług chmury obliczeniowej plan postępowania ze zidentyfikowanymi ryzykami.

8. PODPISANIE UMOWY

1. Podpisanie umowy zgodnej z wymaganiami komunikatu. Zaadresowanie zidentyfikowanych rodzajów ryzyka poprzez wprowadzenie postanowień umownych, planów naprawczych, etc.

Produkty

1. Podpisana umowa. Zalecane jest, aby decyzja o wejściu w technologię chmury obliczeniowej była poprzedzona udokumentowaną zgodą Zarządu Zakładu Ubezpieczeń.
2. Aktualizacja statusu planu postępowania ze zidentyfikowanymi rodzajami ryzyka.

9. WDROŻENIE PRZEDPRODUKCYJNE – KONFIGURACJA USŁUGI

1. W ramach wdrożenia realizowane są kluczowe kamienie milowe wynikające z komunikatu, w szczególności:
    1) dokumentacja usługi chmury obliczeniowej;
    2) dostosowanie procedur wewnętrznych Zakładu Ubezpieczeń;
    3) pozyskanie kompetencji;
    4) opracowanie planu przetwarzania informacji w chmurze obliczeniowej;
    5) opracowanie planu wyjścia;
    6) opracowanie planu ciągłości działania (BCP) lub modyfikacja istniejącego;

7) wdrożenie zabezpieczeń i mechanizmów monitorowania (np. integracja ze SIEM, etc.);
8) testy (funkcjonalne, akceptacyjne, bezpieczeństwa, wydajnościowe, etc.).

2. Na tym etapie nie jest jeszcze dokonywana migracja danych produkcyjnych.
3. Po zakończeniu wdrożenia dokonywana jest aktualizacja statusu planów naprawczych i oceny ryzyka w celu potwierdzenia, że zidentyfikowane uprzednio rodzaje ryzyka zostały zaadresowane zgodnie z założeniami.
4. Określany jest też termin migracji danych i uruchomienia produkcyjnego.

Produkty

1. Dokumentacja usługi chmury obliczeniowej i mechanizmów kontrolnych.
2. Aktualizacja statusu planu postępowania ze zidentyfikowanymi ryzykami.
3. Plan przetwarzania informacji w chmurze obliczeniowej.
4. Plan wyjścia z usług chmury obliczeniowej.
5. Zaktualizowane plany BCP.
6. Wyniki testów i ich akceptacja.
7. Plan migracji i wdrożenia produkcyjnego.
8. Zaktualizowana ocena ryzyka (aktualizacja istniejącej), jeżeli ma zastosowanie.
9. Dokumentacja szkoleń lub pozyskania kompetencji dla użytkowników końcowych i innych kluczowych ról.

10. INFORMOWANIE UKNF

1. Poinformowanie UKNF, zgodnie z wymaganiami komunikatu.

Produkty

1. Uzupełniony formularz stanowiący Załącznik nr 1 do komunikatu.

11. 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 zgodnie z komunikatem i regulacjami wewnętrznymi Zakładu Ubezpieczeń.

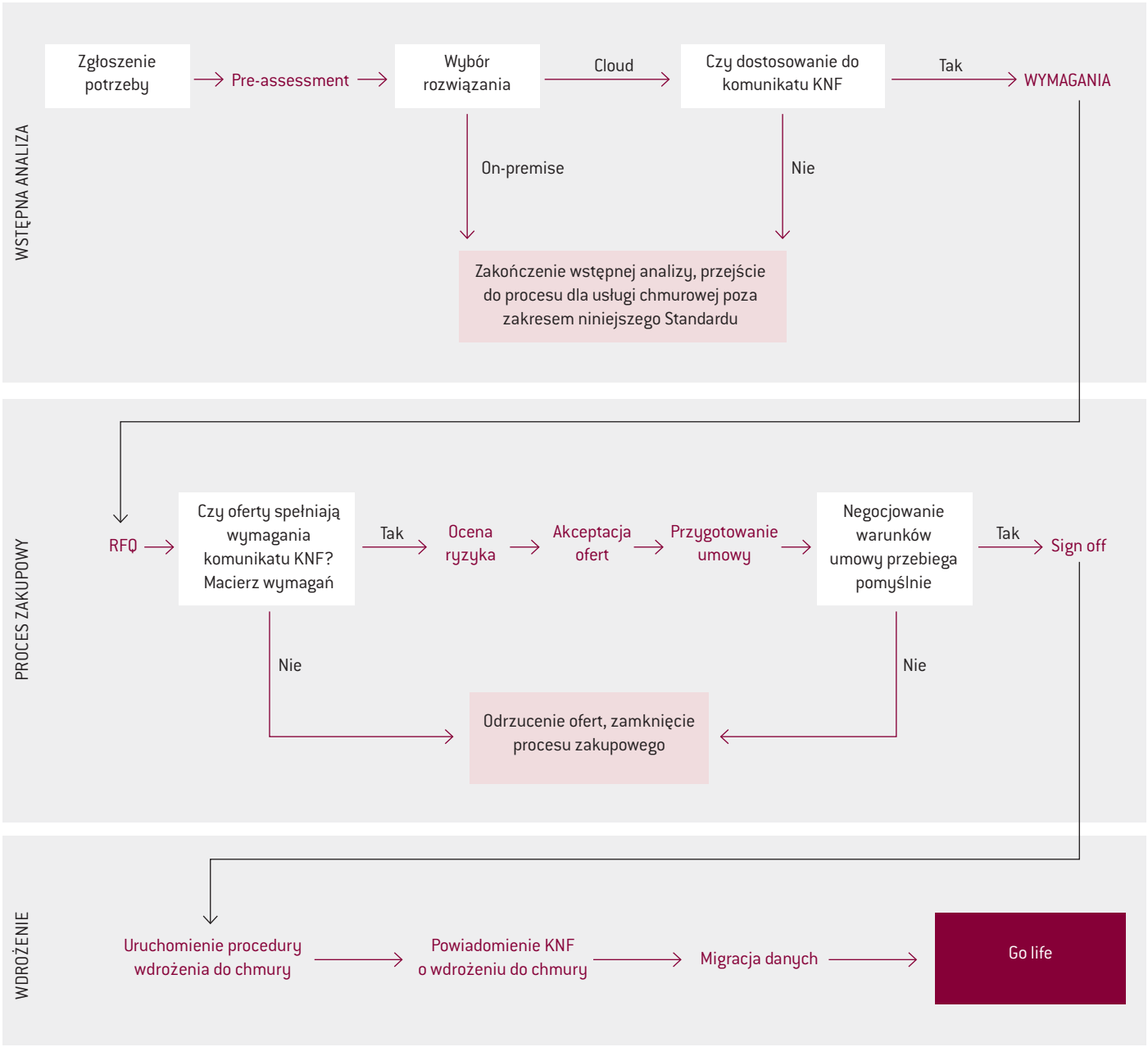
12.URUCHOMIENIE PRODUKCYJNE

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 Zakładu Ubezpieczeń.

Produkty

1. Udokumentowana decyzja o uruchomieniu usługi zgodnie z regulacjami wewnętrznymi Zakładu Ubezpieczeń.
2. Komunikacja wewnętrzna w Zakładzie Ubezpieczeń.

Załącznik 8. **Przykład – Proces wdrożenia**



Załącznik 9. **Przykład – Opis metodyki uzyskania szacowania ryzyka i zgodności z komunikatem UKNF**

PRZETWARZANIE INFORMACJI W CHMURZE OBLICZENIOWEJ ZGODNIE Z KOMUNIKATEM UKNF Z 23 STYCZNIA 2020 – ZAŁOŻENIA METODYKI

1. ZAŁOŻENIA OGÓLNE I ORGANIZACYJNE

1.1. Metodyka ma zastosowanie w każdym wypadku, gdy informacje Zakładu Ubezpieczeń przetwarzane są, w jakimkolwiek zakresie, przy użyciu publicznej lub hybrydowej chmury obliczeniowej bezpośrednio lub za pośrednictwem dostawcy (podwykonawcy), niebędącym dostawcą usługi chmury obliczeniowej, jednak korzystającego z usług chmury obliczeniowej innego podmiotu.

1.2. W przypadku gdy dostawca usługi chmury obliczeniowej korzysta z usług innego dostawcy chmury obliczeniowej, proces należy realizować przy uwzględnieniu obu usług chmurowych.

1.3. Przypisanie ról i odpowiedzialności w procesie należy do Zakładu Ubezpieczeń. Należy zapewnić co najmniej:

1.3.1. udział właściciela merytorycznego procesu co najmniej w zakresie zgromadzenia wymaganych informacji o procesie;

1.3.2. udział przedstawicieli jednostek odpowiedzialnych za bezpieczeństwo, co najmniej w charakterze doradczym (opiniodawczym) na etapie szacowania ryzyka;

1.3.3. udział przedstawicieli IT, co najmniej w charakterze doradczym (opiniodawczym) na etapie szacowania ryzyka technicznego (technologicznego);

1.3.4. udział inspektora ochrony danych lub innej osoby wyznaczonej do nadzoru nad obszarem ochrony danych osobowych, co najmniej w charakterze doradczym (opiniodawczym) na etapie klasyfikacji informacji i szacowania ryzyka w zakresie zgodności z prawem ochrony danych osobowych.

1.4. Należy zapewnić, by decyzja o postępowaniu z ryzykiem była podejmowana przez najwyższe kierownictwo Zakładu Ubezpieczeń lub osoby przez nie upoważnione.

1.5. Należy zapewnić, by w każdym wypadku Zarząd Zakładu Ubezpieczeń posiadał wiedzę o rozpoczęciu korzystania z usług chmury obliczeniowej.

1.6. Wszystkie czynności w ramach realizacji metodyki powinny być dokumentowane w postaci pisemnej lub elektronicznej, w sposób zapewniający identyfikację osoby dokonującej czynności oraz integralność sporządzonej informacji.

2. INWENTARYZACJA (OPIS PROCESU)

2.1. Należy sporządzić opis planowanego procesu, w ramach którego wykorzystywana ma być chmura obliczeniowa, określając możliwie precyzyjnie – co najmniej:

2.1.1. przebieg poszczególnych etapów procesu biznesowego, w ramach którego zakłada się korzystanie z chmury obliczeniowej, w tym określenie, możliwie szczegółowo i precyzyjnie, rodzaju przetwarzanych informacji i ich kategorii;

2.1.2. skalę zakładanego przetwarzania, co najmniej przez wskazanie, czy skala jest mała, średnia czy duża, oraz wskazując przyjęte w tym zakresie kryteria;

2.1.3. zakładaną architekturę rozwiązania, lub co najmniej wskazanie usług, z których Zakład Ubezpieczeń zamierza korzystać oraz zakładanej konfiguracji – o ile te informacje są dostępne.

3. KLASYFIKACJA INFORMACJI

3.1. Celem klasyfikacji informacji jest zapewnienie, że informacje uzyskują ochronę na odpowiednim poziomie,

z perspektywy związanych z nimi wymogami prawnymi oraz ich wagi.

3.2. W praktyce klasyfikacje odnoszą się najczęściej do kryteriów: poufności, integralności i dostępności (zasad dostępu do informacji) z perspektywy skutków finansowych i regulacyjnych dla organizacji. Dobrą praktyką jest określenie ponadto ramowych minimalnych warunków zabezpieczeń obowiązujących w odniesieniu do poszczególnych klas informacji (przykład: Załącznik nr 1, Tabela nr 2).

3.3. Zakład Ubezpieczeń powinien posiadać wdrożoną i stosowaną klasyfikację informacji, w oparciu o przyjęte przez siebie kryteria. Klasyfikacja może opierać się na kryterium określonym przez Zakład Ubezpieczeń, pod warunkiem że odzwierciedlać będzie ona co najmniej podział na informacje prawnie chronione w rozumieniu komunikatu oraz pozostałe informacje.

3.4. Niniejsza metodyka opiera się na następującej klasyfikacji:

3.4.1. Klasa A – informacje publiczne

3.4.2. Klasa B – informacje wewnętrzne

3.4.3. Klasa C – informacje ważne

3.4.4. Klasa D – informacje szczególnie chronione

3.4.5. Klasa E – informacje krytyczne

3.5. Zinwentaryzowane zgodnie z pkt 2 informacje należy przypisać do klas, przed przystąpieniem do procesu oceny informacji.

4. OCENA INFORMACJI

Cel: ustalenie, czy w konkretnym analizowanym przypadku dopuszczalne jest korzystanie przez ZAKŁAD UBEZPIECZEŃ z chmury obliczeniowej

4.1. Ocena dokonywana jest w sposób usystematyzowany, w odniesieniu do konkretnej usługi chmurowej i konkretnego procesu, podlegającego migracji do chmury.

4.2. Ocena powinna obejmować – co najmniej:

4.2.1. analizę występowania ograniczeń regulacyjnych mogących uniemożliwiać lub ograniczać korzystanie z chmury obliczeniowej (np. ograniczenia terytorialne);

4.2.2. analizę występowania ograniczeń kontraktowych, mogących uniemożliwiać lub ograniczać korzystanie z chmury obliczeniowej (np. z uwagi na ograniczenia terytorialne, ograniczenia w zakresie korzystania z podwykonawców, itd.);

4.2.3. analizę występowania ograniczeń wewnątrzorganizacyjnych (np. wewnętrzne procedury ograniczające możliwości korzystania z chmury obliczeniowej dla określonych rodzajów informacji);

4.2.4. ocenę występowania ewentualnych innych okoliczności prawnych lub biznesowych właściwych dla analizowanego przypadku i udokumentowania takich okoliczności;

4.2.5. określenie charakteru analizowanej informacji jako objętej lub nieobjętej tajemnicą (status informacji chronionej w rozumieniu komunikatu);

4.2.6. abstrakcyjną (tj. nieodnoszącą się do konkretnego zagrożenia) ocenę wpływu na bezpieczeństwo informacji w oparciu o przyjęte przez Zakład Ubezpieczeń kryteria; jako minimum ocena powinna odnosić się do skutków potencjalnego zagrożenia dla:

- reputacji,
- finansów,
- ciągłości działania Zakładu Ubezpieczeń oraz
- uprawnienia do prowadzenia działalności regulowanej przez Zakład Ubezpieczeń;

4.2.7. stwierdzenie, w oparciu o dokonaną ocenę, czy proces obejmuje Outsourcing szczególny w rozumieniu komunikatu;

4.2.8. oszacowanie wartości informacji; dokonując oceny należy wziąć pod uwagę co najmniej następujące czynniki:

- potencjalne kary finansowe związane z takim naruszeniem;
- koszty związane z identyfikacją i usuwaniem naruszenia;
- koszty i utracone przychody (utrata klientów, utrata informacji o środkach materialnych i niematerialnych itp.);
- koszty reputacyjne oraz wydatki poniesione na obszar public relations;

4.2.9. rozstrzygnięcie o dopuszczalności (lub niedopuszczalności) korzystania z chmury obliczeniowej oraz ewentualnie warunków takiego korzystania.

4.3. Klasyfikacja i ocena informacji powinna odbywać się cyklicznie, nie rzadziej niż raz na rok oraz za każdym razem:

4.3.1. dla każdej planowanej do wykorzystania lub wykorzystywanej usługi chmury obliczeniowej;

4.3.2. dla każdego nowego rodzaju informacji, który Zakład Ubezpieczeń zamierza przetwarzać w procesie;

4.3.3. po wystąpieniu następujących zdarzeń: zmiana prawa, regulacji, regulaminów lub postanowień umów, które to zmiany mogą wpływać na zgodność postępowania podmiotu nadzorowanego w kontekście przetwarzania informacji w chmurze obliczeniowej;

4.3.4. zwiększenia lub zmniejszania skali przetwarzania informacji w procesie;

4.3.5. w przypadku istotnego zwiększenia się wartości przetwarzanych informacji.

5. SZACOWANIE RYZYKA

Cel: identyfikacja ryzyk i zarządzanie nimi

5.1. Zakres szacowania ryzyka (poziom szczegółowości analizy) powinien być określony zgodnie z zasadą proporcjonalności. W każdym jednak wypadku należy uwzględnić kroki opisane w niniejszym rozdziale.

5.2. Szacowanie ryzyka wymaga identyfikacji zagrożeń związanych z chmurą obliczeniową, w szczególności zagrożeń wynikających z okoliczności wskazanych w rozdziale VI komunikatu. Zagrożenia standardowo dotyczą w szczególności następujących obszarów ryzyka:

5.2.1. lokalizacje przetwarzania (rozproszenie geograficzne);

5.2.2. korzystanie z usług chmury obliczeniowej w sposób inny niż zamierzony;

5.2.3. dostęp do informacji chronionej;

5.2.4. kontrola nad danymi (własność danych);

5.2.5. podatności interfejsów, błędy konfiguracji;

5.2.6. zakres szyfrowania;

5.2.7. kompetencje techniczne;

5.2.8. vendor lock-in;

5.2.9. poddanie umowy prawu obcemu lub obcej jurysdykcji;

5.2.10. ograniczona kontrola nad przebiegiem współpracy z dostawcą;

5.2.11. adhezyjność warunków umowy z dostawcą.

5.3. Identyfikując zagrożenie należy wskazać jego źródło (np. postanowienia umowy, dokumentacja bezpieczeństwa, dostępna publicznie informacja o stwierdzonych podatnościach usługi).

5.4. Określone okoliczności mogą być źródłem zagrożenia z perspektywy prawnej, organizacyjnej lub technicznej lub

każdej z nich równocześnie, co należy uwzględnić identyfikując i analizując zagrożenie.

5.5. Każde zagrożenie powinno zostać ocenione pod kątem wpływu jego wystąpienia na aspekty wskazane w pkt 4.2.6. z uwzględnieniem przyjętych na jego podstawie kryteriów.

5.6. Każde zagrożenie powinno zostać ocenione pod kątem poziomu prawdopodobieństwa jego wystąpienia. Oceniając poziom prawdopodobieństwa, Zakład Ubezpieczeń powinien wziąć pod uwagę co najmniej wiedzę historyczną nt. wystąpienia podobnych zagrożeń, dostępną ekspercką wiedzę w tym zakresie, oraz ustaloną zgodnie z pkt 4.2.8 wartość informacji.

5.7. Poziomowi wpływu oraz poziomowi prawdopodobieństwa przypisuje się wartość liczbową, w celu ustalenia poziomu ryzyka początkowego, uzyskiwanego jako iloczyn tych dwóch wartości.

5.8. Zakład Ubezpieczeń może zidentyfikować interakcje między zagrożeniami (ich wzajemne wzmocnienia) lub przypisać określonym obszarom dodatkową wagę (z uwagi na szczególne okoliczności dotyczące Zakładu Ubezpieczeń). W takim wypadku poziom ryzyka początkowego podlega odpowiedniemu podwyższeniu.

5.9. Dla każdego ryzyka na poziomie innym niż niski, określa się środki zaradcze w postaci planu postępowania z ryzykiem, a następnie – poziom ryzyka szczątkowego. Dla każdego ryzyka szczątkowego określa się plan postępowania z ryzykiem (unikanie, redukcja, przenoszenie, akceptacja).

5.10. Każde ryzyko powinno być monitorowane, a wyniki monitorowania – raportowane zgodnie z zasadami przyjętymi przez Zakład Ubezpieczeń.

5.11. W celu zarządzania ryzykiem, określa się plan postępowania z ryzykiem, przypisując do poszczególnych ryzyk osoby odpowiedzialne za stosowanie środków zaradczych.

5.12. 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

6.1. W celu zapewnienia dostępności dokumentacji na wypadek kontroli organu nadzoru należy zgromadzić:

6.1.1. dokumentację, wymaganą komunikatem lub przepisami prawa tj. np. plan przetwarzania informacji w chmurze, plan ciągłości działania, exit plan itp. oraz

6.1.2. wypełniony szablon szacowania ryzyka wraz z dokumentacją stanowiącą podstawę szacowania ryzyka (np. umowa z dostawcą, zamówione opinie prawne, wewnętrzna dokumentacja potwierdzająca posiadane kompetencje techniczne, dokumentacja środków bezpieczeństwa itd.).

6.2. W zależności od potrzeb, należy zweryfikować kompletność procesu w oparciu o checklistę wymogów określonych w Komunikacie oraz przepisach sektorowych.

7. DECYZJA O ROZPOCZĘCIU KORZYSTANIA Z USŁUGI CHMURY OBLICZENIOWEJ

7.1. Decyzję powinno podjąć najwyższe kierownictwo Zakładu Ubezpieczeń lub osoba przez nie upoważniona.

8. INFORMOWANIE UKNF O KORZYSTANIU Z USŁUGI CHMURY OBLICZENIOWEJ

Załącznik 10. **Przykładowe wypełnienie informacji do UKNF o rozpoczęciu korzystania z chmury obliczeniowej przez zakład ubezpieczeń**

Lokalizacje CPD przetwarzanych informacji (państwo, region):	Zakład Ubezpieczeń S.A., ul. Zgłoszeniowa 1/2, 00-123 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/ przetwarzaniu:

Rodzaj i zakres przetwarzanych informacji:	Informacje o pracownikach Zakładu Ubezpieczeń: dane osobowe pracowników, umowy o prace Informacje o agentach ubezpieczeniowych: dane osobowe agentów, umowy agencyjne Informacje o klientach Zakładu Ubezpieczeń: dane osobowe klientów, umowy ubezpieczenia, nagrania rozmów na infolinii, decyzje w przedmiocie wypłaty sumy odszkodowania, pisma klientów zawierające zgłoszenie wystąpienia szkody
Nazwa i adres dostawcy usług chmury obliczeniowej:	dostawca usług chmury obliczeniowej S.A., ul. Szyfrowana 2/1, 00-321 Warszawa
Nazwa usług chmury obliczeniowej lub ich rodzaj:	storage, serwery wirtualne, sieci i systemy operacyjne
Lokalizacje CPD przetwarzanych informacji (państwo, region):	Warszawa, Dublin (Irlandia), Frankfurt (Niemcy), Holandia, Finlandia
Data podpisania umowy z dostawcą usług chmury obliczeniowej lub przewidywany termin jej zawarcia:	10 października 2020 r. – data zawarcia umowy
Okres, na jaki została zawarta umowa z dostawcą usług chmury obliczeniowej:	5 lat od dnia 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 Działu IT, tel. 111 222 333, adres e-mail: jan.kowalski@zaklad.ubezpieczen.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 listopada 2020 r.	Członek Zarządu ZU	Członek Zarządu/Prokurent ZU
Miejscowość, data	Podpisy osób reprezentujących podmiot nadzorowany	