Logo, company name

Description automatically generated

**STANDARD WDROŻEŃ PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ**

**OPRACOWANIE NA POTRZEBY SEKTORA UBEZPIECZENIOWEGO**

**Warszawa 2022**

# Autorzy standardu

|  |  |  |  |
| --- | --- | --- | --- |
| **Podmioty reprezentowane** | **Imię** | **Nazwisko** | **Rola** |
| **Accenture Sp. z o.o.góźd** | Daniel | Rudnicki | **Koordynacja prac grupy roboczej** |
| Michał | Truskolas | **Koordynacja prac grupy roboczej** |
| Julia | Lang | **Koordynacja prac grupy roboczej** |
| **Aegon TUNŻ S.A.** | Zbigniew | Śliwa | **Uczestnik grupy roboczej** |
| Jan | Kurczewski |  |
| **Agro Ubezpieczenia - TUW** | Dawid | Banasiak | **Uczestnik grupy roboczej** |
| Marcin | Piwko | **Uczestnik grupy roboczej** |
| **Aviva TUnŻ S.A.;**  **Aviva TUO S.A.** | [Paweł](mailto:pawel.kuzmicz@aviva.com) | Kuźmicz | **Uczestnik grupy roboczej** |
| [Rafał](mailto:rafal.salyga@aviva.com) | Sałyga | **Uczestnik grupy roboczej** |
| Sebastian | Pluta | **Uczestnik grupy roboczej** |
| Marek | Kowalski | **Uczestnik grupy roboczej** |
| **AXA Ubezpieczenia TUiR S.A.;**  **AXA ŻYCIE TU S.A.** | Jolanta | Gasiewicz | **Uczestnik grupy roboczej** |
| Marcin | Sęp | **Uczestnik grupy roboczej** |
| Adam | Żelazko | **Uczestnik grupy roboczej** |
| Agnieszka | Czumer | **Uczestnik grupy roboczej** |
| **COMPENSA S.A.;**  **COMPENSA ŻYCIE S.A.** | Marcin | Grabowski | **Uczestnik grupy roboczej** |
| **TU Euler Hermes S.A.** | Mateusz | Kaczmarski | **Uczestnik grupy roboczej** |
| **EUROPA S.A.;**  **EUROPA ŻYCIE S.A.** | Tomasz | Bujała | **Uczestnik grupy roboczej** |
| Marcin | Fedor | **Śpiewak** |
| Anna | Januchta-Baranczyk | **Uczestnik grupy roboczej** |
| Bartosz | Sacewicz | **Uczestnik grupy roboczej** |
| Dorota | Pokorska | **Uczestnik grupy roboczej** |
| Igor | Pełdiak | **Uczestnik grupy roboczej** |
| Konrad | Mazurek | **Uczestnik grupy roboczej** |
| Paweł | Bzdyk | **Uczestnik grupy roboczej** |
| **GENERALI TU S.A.;**  **GENERALI ŻYCIE TU S.A.** | Marcin | Nosek | **Uczestnik grupy roboczej** |
| Waldemar | Lenda | **Uczestnik grupy roboczej** |
| Katarzyna | Wieczorek | **Uczestnik grupy roboczej** |
| Iwona | Wcisło | **Uczestnik grupy roboczej** |
| Michał | Pyszycki | **Uczestnik grupy roboczej** |
| **InterRisk TU S.A. VIG** | Krzysztof | Góźdź | **Uczestnik grupy roboczej** |
| **LINK 4 TU S.A.** | Małgorzata | Jaworska | **Uczestnik grupy roboczej** |
| Michał | Więckowski | **Uczestnik grupy roboczej** |
| **Maruta Wachta sp. j.** | Marcin | Maruta | **Koordynator prawny** |
| Michał | Kulesza | **Koordynator prawny** |
| Marcin | Białkowski | **Koordynator prawny** |
| **Nationale-Nederlanden TU SA; Nationale-Nederlanden TUnŻ S.A.** | Marcin | Szydłowski | **Uczestnik grupy roboczej** |
| Andrzej | Miron | **Uczestnik grupy roboczej** |
| Paweł | Kaczmarek | **Uczestnik grupy roboczej** |
| Ewa | Kłosek | **Uczestnik grupy roboczej** |
| **Open Life TU Życie S.A.** | Paweł | Smater | **Funkcja doradcza** |
| Piotr | Majchrzak | **Funkcja doradcza** |
| **PIIT** | Dariusz | Śpiewak | **Funkcja doradcza** |
| **PKO TU S.A.;**  **PKO Życie S.A.** | Jarosław | Wachowicz | **Uczestnik grupy roboczej** |
| Tomasz | Arabski | **Uczestnik grupy roboczej** |
| **Polska Izba Ubezpieczeń** | Mariusz | Kuna | **Koordynacja prac grupy roboczej** |
| Agnieszka | Durska | **Koordynacja prac grupy roboczej** |
| Anna | Kwiatkowska | **Koordynacja prac grupy roboczej** |
| Paweł | Sawicki | **Koordynacja prac grupy roboczej** |
| **Polski Gaz TUW** | Justyna | Wasińska | **Uczestnik grupy roboczej** |
| **PZU S.A.;**  **PZU ŻYCIE S.A.** | Aleksandra | Podhajska | **Uczestnik grupy roboczej** |
| Rafał | Jeż | **Uczestnik grupy roboczej** |
| **STU ERGO Hestia SA;**  **STUnŻ ERGO Hestia SA** | Jarosław | Łojewski | **Uczestnik grupy roboczej** |
| Damian | Jagusz | **Uczestnik grupy roboczej** |
| Anna | Klein-Kaska | **Uczestnik grupy roboczej** |
| Marcin | Usarzewicz | **Uczestnik grupy roboczej** |
| **The Prudential Assurance Company Ltd. Oddział w Polsce** | Marcin | Sagała | **Uczestnik grupy roboczej** |
| Katarzyna | Mierzejska | **Uczestnik grupy roboczej** |
| **Towarzystwo Ubezpieczeń Wzajemnych "TUW"** | Jerzy | Tarabuła | **Uczestnik grupy roboczej** |
| Anna | Pogorzelska | **Uczestnik grupy roboczej** |
| **Traple Konarski Podrecki i Wspólnicy Sp.j** | Jan | Byrski | **Koordynator prawny** |
| Michał | Synowiec | **Koordynator prawny** |
| Henryk | Hoser | **Koordynator prawny** |
| Xawery | Konarski | **Koordynator prawny** |
| **TUIR WARTA S.A.;**  **TUnŻ WARTA S.A.** | Kinga | Królikowska | **Funkcja doradcza** |
| Monika | Muszyńska | **Funkcja doradcza** |
| Maciej | Pilarski | **Funkcja doradcza** |
| Aleksandra | Płoszajska | **Funkcja doradcza** |
| Krzysztof | Subartowicz | **Uczestnik grupy roboczej** |
| Daria | Pałuba | **Uczestnik grupy roboczej** |
| **TUW PZUW** | Jakub | Papuga | **Uczestnik grupy roboczej** |
| **UNIQA S.A.;**  **UNIQA ŻYCIE S.A.** | Jacek | Koziróg | **Uczestnik grupy roboczej** |
| Maciej | Bramson | **Uczestnik grupy roboczej** |
| **Unum Życie TUiR S.A.** | Robert | Gromadzki | **Uczestnik grupy roboczej** |
| **Vienna Life TUnŻ S.A. VIG** | Paweł | Kwasiborski | **Uczestnik grupy roboczej** |
| Michał | Oko | **Uczestnik grupy roboczej** |
| Ewa | Lepiarczyk | **Uczestnik grupy roboczej** |
| **VIG Polska Sp. z o.o.** | Marek | Chmurzyński | **Uczestnik grupy roboczej** |
| Arkadiusz | Lewandowski | **Uczestnik grupy roboczej** |
| Krzysztof | Masłowski | **Uczestnik grupy roboczej** |
| Jarosław | Strzyga | **Uczestnik grupy roboczej** |

**Standard został skonsultowany w ramach grupy podmiotów opiniujących:**

# Spis treści

[Autorzy standardu 2](#_Toc57385096)

[1 Wstęp 4](#_Toc57385098)

[2 Założenia 4](#_Toc57385099)

3 [Terminologia stosowana w Standardzie. Objaśnienie wybranych definicji Komunikatu 5](#_Toc57385100)

[4 Organizacja dokumentu 9](#_Toc57385102)

[5 Wymogi Komunikatu UKNF 10](#_Toc57385103)

[5.1 Wytyczne stosowania 10](#_Toc57385104)

[5.2 Wytyczne do klasyfikacji i oceny informacji 12](#_Toc57385105)

[5.3 Wytyczne do szacowania ryzyka 13](#_Toc57385106)

[5.4 Minimalne wymagania dla przetwarzania informacji w Chmurze obliczeniowej 18](#_Toc57385107)

[5.5 Zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w Chmurze obliczeniowej 33](#_Toc57385108)

[6 Załączniki 34](#_Toc57385109)

[6.1 Załącznik nr 1 – Przykład szablonu klasyfikacji informacji 34](#_Toc57385110)

[6.2 Załącznik nr 2 – Przykład szablonu szacowania ryzyka 34](#_Toc57385111)

[6.3 Załącznik nr 3 – Przykładowy plan przetwarzania informacji w Chmurze obliczeniowej 34](#_Toc57385112)

[6.4 Załącznik nr 4 - Przykładowy szablon scenariusza wyjścia z chmury 34](#_Toc57385113)

[6.5 Załącznik nr 5 - Przykład - Wyjście z chmury - główne zagadnienia 34](#_Toc57385114)

6.6 [Załącznik nr 6 - ISO 27001 34](#_Toc57385115)

[6.7 Załącznik nr 7 - Przykładowe kroki wdrożenia usługi przetwarzania informacji w Chmurze obliczeniowej publicznej lub hybrydowej w Zakładzie Ubezpieczeń 34](#_Toc57385117)

[6.8 Załącznik nr 8 - Przykład - Proces wdrożenia 34](#_Toc57385118)

[6.9 Załącznik nr 9 - Przykład - Opis metodyki uzyskania szacowania ryzyka i zgodności z Komunikatem UKNF ...................... 34](#_Toc57385120)

[6.10 Załącznik nr 10 - Przykładowe wypełnienie informacji do UKNF o rozpoczęciu korzystania z Chmury obliczeniowej przez Zakład Ubezpieczeń 34](#_Toc57385121)

# 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.

Komunikat nie jest źródłem prawa. Stanowi zbiór wytycznych organu nadzoru w obszarze przetwarzania informacji w chmurze obliczeniowej. Celem jest ustanowienie jednolitego standardu we wszystkich sektorach rynku finansowego. Jednocześnie Komunikat nie jest podstawą do nałożenia na podmiot nadzorowany dodatkowych obowiązków niż te przewidziane przepisami prawa powszechnie obowiązującego.

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.**

# 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. KNF w Komunikacie wyłącza stosowanie wytycznych EBA, EIOPA, ESMA odnoszących się do przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej. Komunikat z dnia 23 stycznia 2020 r. wprowadził w tym zakresie podejście krajowe, które uwzględnia specyfikę rynku finansowego w Polsce oraz istniejące regulacje. EBA, EIOPA, ESMA zostały poinformowane o niestosowaniu wytycznych EBA, EIOPA, ESMA dotyczących outsourcingu w zakresie dostawców usług w chmurze. Należy przy tym podkreślić, że podejście krajowe wyrażone w Komunikacie i wytyczne EBA, ESMA, EIOPA są w dużej mierze ze sobą zbieżne.
4. W celu zachowania spójności – stosowania tych samych wytycznych względem wszystkich podmiotów nadzorowanych - adresatami Komunikatu są podmioty nadzorowane z całego rynku finansowego (z sektora rynku kapitałowego, bankowego i ubezpieczeniowego)
5. Stosowanie Komunikatu dotyczy podmiotów nadzorowanych przez KNF. Obszarem stosowania jest Rzeczpospolita Polska (RP).
6. Podmiot mający siedzibę w innym państwie UE (spoza RP), w związku z korzystaniem z usług chmury obliczeniowej, może być zobowiązany stosować wytyczne ESAs (EBA, EIOPA, ESMA) lub wytyczne państwa swojej siedziby.
7. Sytuacja równoczesnego stosowania wytycznych ESAs oraz Komunikatu może dotyczyć podmiotu z siedzibą spoza RP a prowadzącego działalność w RP. Oddział takiego podmiotu w RP będzie objęty Komunikatem.

# 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. * podmiotu realizującego usługi na rzecz dostawcy chmurowego, który nie posiada albo nie może posiadać identyfikowanego dostępu do informacji przetwarzanych przez podmiot nadzorowany. |
| **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, z późniejszymi 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.

# 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**

# Wymogi Komunikatu UKNF

## Wytyczne stosowania

#### TREŚĆ KOMUNIKATU UKNF

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Wytyczne stosowania** 2. 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).   1. 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. 2. Nadzór podkreśla, że opisane w niniejszym komunikacje wymagania powinny być stosowane przez podmioty nadzorowane przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej. 3. 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. |  1. W przypadku kwalifikowania czynności lub informacji do więcej niż jednej kategorii według powyższej matrycy, należy przyjąć do stosowania wymaganie bardziej rygorystyczne. 2. 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. 3. 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. 4. Komunikat nie dotyczy przetwarzania informacji w Chmurze obliczeniowej prywatnej. |

#### OPIS WYMAGAŃ

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.

W każdym innym przypadku Komunikat może być stosowany, jeśli Zakład Ubezpieczeń (również w porozumieniu z Dostawcą usług chmury obliczeniowej) tak postanowi.

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.

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.
3. Wymagania określone w Komunikacie powinny być spełnione przez Zakład Ubezpieczeń przed rozpoczęciem przetwarzania informacji w Usłudze chmury obliczeniowej.
4. Stosowanie Komunikatu powinno odbywać się w sposób zgodny z Zasadą proporcjonalności.
5. Zasada proporcjonalności powinna znaleźć swoje doprecyzowanie na etapie szacowania ryzyka związanego z planowaniem czynności powierzenia przetwarzania informacji w Usłudze chmury obliczeniowej.
6. 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 nr 7 - Przykładowe kroki wdrożenia usługi przetwarzania informacji w Chmurze obliczeniowej publicznej lub hybrydowej w Zakładzie Ubezpieczeń
2. Załącznik nr 8 - Przykład - Proces wdrożenia

## Wytyczne do klasyfikacji i oceny informacji

#### TREŚĆ KOMUNIKATU UKNF

|  |
| --- |
| 1. **Wytyczne do klasyfikacji i oceny informacji** 2. 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. 3. 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. 4. 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. 5. 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. 6. 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 nr 1 – Przykład szablonu klasyfikacji informacji

## Wytyczne do szacowania ryzyka

#### TREŚĆ KOMUNIKATU UKNF

|  |
| --- |
| 1. **Wytyczne do szacowania ryzyka** 2. 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 [[1]](#footnote-2). Szacowanie ryzyka jest prowadzone w sposób ciągły, z uwzględnieniem praktycznej implementacji zasady PDCA („plan – do – check – act”). 3. 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:       1. rozproszenie geograficzne przetwarzanych informacji, w szczególności w kontekście zapewnienia zgodności procesu przetwarzania informacji z przepisami prawa, regulacjami wewnętrznymi, zobowiązaniami umownymi oraz deklaracjami i innymi uregulowaniami;       2. 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;       3. dostęp do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) dostawcy usług chmury obliczeniowej;       4. 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;       5. 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);       6. awarie mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej;       7. podatność interfejsów zarządzających usługami, które są udostępniane przez dostawców usług chmury obliczeniowej;       8. 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;       9. 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;       10. podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy dostawcę usług chmury obliczeniowej a podmiot nadzorowany;    2. specyficzne zagrożenia dla stosowanych konkretnych (nazwanych) usług chmury obliczeniowej:       1. 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);       2. możliwości jednostronnej zmiany warunków technicznych korzystania z usługi (w szczególności jej parametrów lub zasad konfiguracji);       3. stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług, bez ich należytej weryfikacji i oceny adekwatności dla potrzeb podmiotu nadzorowanego;       4. stosowane mechanizmy uwierzytelniania oraz ich słabości;    3. specyficzne zagrożenia związane z zasobami podmiotu nadzorowanego:       1. wymagane i posiadane zasoby, w tym zasoby ludzkie o ustalonych kompetencjach;       2. 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:       1. szyfrowanie informacji nie zmniejsza ważności informacji, nie zmienia też jej klasyfikacji i oceny;       2. szyfrowanie informacji oraz właściwe zarządzanie kluczami szyfrującymi zapobiega ujawnieniu informacji;       3. 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;       4. informacje przetwarzane w chmurze obliczeniowej powinny być szyfrowane zawsze, gdy to jest technologicznie możliwe i – w ocenie podmiotu nadzorowanego – ekonomicznie zasadne;       5. 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;       6. 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:       1. 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:          1. tworzenie łańcucha outsourcingowego w zakresie działalności nadzorowanej jest dopuszczalne wyłącznie w granicach przewidzianych przepisami prawa;          2. 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;       2. 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:          1. 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          2. 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:       1. 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;       2. 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:       1. 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:          1. postanowień umowy;          2. wszystkich wymogów prawa polskiego ciążących na podmiocie nadzorowanym;          3. wytycznych organu nadzoru, w tym również w zakresie niniejszego komunikatu;       2. 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. 4. 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. 5. 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:       1. identyfikacji nowych zagrożeń;       2. zmian w wykorzystywanej usłudze chmury obliczeniowej lub trybie i zakresie jej wykorzystywania;       3. 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. 6. 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. 7. Wyniki szacowania ryzyka powinny zostać formalnie zatwierdzone oraz podlegać okresowej weryfikacji i aktualizacji[[2]](#footnote-3). Zatwierdzenie powinno obejmować decyzję podmiotu nadzorowanego dotyczącą:    1. usług chmury obliczeniowej, z których podmiot nadzorowany będzie korzystał;    2. rodzaju i zakresu przetwarzanych w ramach tych usług informacji. |

#### OPIS WYMAGAŃ

1. 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:
2. niezbędnych kompetencji personelu Dostawcy usług chmury obliczeniowej do planowanych lub prowadzonych działań przetwarzania informacji z wykorzystaniem Usług chmury obliczeniowej;
3. 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;
4. sposobu kontroli i monitorowania dostępu do przetwarzanych informacji przez personel Dostawcy usług chmury obliczeniowej i jego poddostawców, w tym w szczególności dostępów uprzywilejowanych (kont administratorów, współadministratorów, serwisowych);
5. mechanizmów kontroli dostępu do usługi dla użytkowników, w szczególności MFA lub ograniczenia dostępu z urządzeń prywatnych;
6. opisu mechanizmów izolacji zasobów używanych do świadczenia Usług chmury obliczeniowej, wraz z informacją o potencjalnych skutkach awarii mechanizmów izolacji;
7. dokumentacji interfejsów zarządzających Usługami chmury obliczeniowej, informacji o zabezpieczeniach interfejsów i ew. o ich podatnościach;
8. dokumentacji wykonywanych przeglądów, audytów lub kontroli, w tym testów bezpieczeństwa (częstotliwości, metodyki, zakresu, wyników, monitorowania statusów);
9. zasad uzgadniania wprowadzania zmian przez Dostawcę usług chmury obliczeniowej;
10. 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;
11. podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy Dostawcę usług chmury obliczeniowej a Zakład Ubezpieczeń;
12. monitorowania środowiska przetwarzania informacji w Usłudze chmury obliczeniowej wraz z zasadami zarządzania logami;
13. możliwości integracji z innymi, wskazanymi przez Zakład Ubezpieczeń, technologiami;
14. stosu technologicznego w zakresie zapewnienia bezpieczeństwa środowiska, danych (informacji) oraz zasobów Chmury obliczeniowej, w szczególności mechanizmów szyfrowania i zarządzania kluczami szyfrującymi;
15. opracowanych i przetestowanych planów ciągłości działania oraz procedur odtworzeniowych, z uwzględnieniem mechanizmów redundancji oraz kopii bezpieczeństwa;
16. zasad zarządzania incydentami bezpieczeństwa;
17. łańcucha outsourcingowego, w tym procesu kontroli;
18. 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.
19. W przypadku analizy rozszerzonej zabezpieczeń można wykorzystać Załącznik nr 6 do standardu (analizę ISO 27001).
20. Poinformowanie Zakładu Ubezpieczeń o stosowanych zabezpieczeniach.
21. 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 nr 2 – Przykład szablonu szacowania ryzyka

1. Załącznik nr 6 – ISO 27001
2. Załącznik nr 9 – Przykład - Opis metodyki uzyskania szacowania ryzyka i zgodności z Komunikatem UKNF

## Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej

#### TREŚĆ KOMUNIKATU UKNF

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

#### Opis wymagań

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).

1. Kompetencje powinny zapewniać bezpieczeństwo, spójność architektoniczną oraz dostarczać odpowiednie wsparcie rozwiązań, a także rozliczalność wykorzystywanych Usług chmury obliczeniowej.
2. 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

### 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:      1. klarowny podział odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji, z uwzględnieniem modelu świadczenia usług, ciągłości działania usług (z uwzględnieniem parametrów RTO i RPO[[3]](#footnote-4) tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;      2. klarowną definicję i wskazanie lokalizacji[[4]](#footnote-5) przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;      3. prawo właściwe dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów);      4. potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;      5. własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu (wygaśnięciu, rozwiązaniu), także w sposób nieplanowany;      6. 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;      7. określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie), zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;      8. klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) dostawcy usług chmury obliczeniowej oraz warunki nadawania praw dostępu do informacji przetwarzanych przez podmiot nadzorowany;      9. 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;      10. źródła autoryzowanych informacji o planowanych zmianach w standardach świadczonych usług chmury obliczeniowej (w tym zmianach o charakterze technicznym);      11. źródła dokumentacji technicznej i deklaracji zgodności (w tym zgodności z obowiązującymi przepisami prawa), wraz z instrukcjami dotyczącymi konfiguracji usług chmury obliczeniowej;      12. zakres dodatkowych informacji i dokumentacji przekazywanych przez dostawcę usług chmury obliczeniowej w związku ze świadczeniem usług chmury obliczeniowej;      13. prawo podmiotu nadzorowanego do przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji, w tym prawo do przeprowadzenia audytu 2-giej lub 3-ciej strony na zlecenie podmiotu nadzorowanego (o ile taka potrzeba wynika z szacowania ryzyka);      14. 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;      15. 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;      16. zasady zmiany treści umowy, w tym parametrów technicznych używanych usług chmury obliczeniowej;      17. zasady rozwiązywania umowy, w tym zasady i terminy zwrotu lub usunięcia przetwarzanych informacji;      18. zasady wsparcia, w tym zakres i okna czasowe (z uwzględnieniem stref czasowych), tryb i sposób zgłaszania problemów z usługami chmury obliczeniowej;      19. 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:   * + 1. 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;     2. 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
7. 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

### 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:      1. rodzaj (opis) przetwarzanych informacji oraz informację, jeżeli stosowane, o ich pseudonimizacji lub anonimizacji;      2. sposób szyfrowania informacji oraz miejsce (lub sposób) zarządzania kluczami szyfrującymi;      3. informację o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany;      4. 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;      5. prawo właściwe, któremu podlega umowa;      6. opis zadania realizowanego za pomocą usługi chmury obliczeniowej wraz z informacją, czy jest to outsourcing szczególny chmury obliczeniowej w rozumieniu niniejszego komunikatu lub czy przetwarzane są informacje prawnie chronione. |

#### Opis wymagań

1. 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 generowania kluczy szyfrujących, oraz opis kontroli dostępu do informacji.
2. Plan przetwarzania w oparciu o wewnętrzną klasyfikację danych powinien precyzyjnie określić jakie dane (informacje) Zakład Ubezpieczeń, w ramach konkretnej inicjatywy, przetwarza w Chmurze obliczeniowej.
3. 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 nr 3 do Standardu).

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

N/D

#### Szablony

1. Załącznik nr 3 - Przykładowy plan przetwarzania informacji w chmurze obliczeniowej

|  |
| --- |
| * 1. 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

|  |
| --- |
| * 1. 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;

1. powinny odbywać się rotacyjnie w oparciu o różne procesy i aplikacje. Rotacyjne testowanie powinno dotyczyć procesów i aplikacji, które mają istotny wpływ na działalność Zakładu 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.

1. Plan powinien być przeglądany i aktualizowany w określonym przez wewnętrzne procedury Zakładu Ubezpieczeń okresie czasu.
2. 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 nr 4 - Przykładowy szablon scenariusza wyjścia z chmury
2. Załącznik nr 5 - Przykład - Wyjście z chmury - główne zagadnienia

|  |
| --- |
| * 1. 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

### Wymagania dla dostawców usług chmury obliczeniowej[[5]](#footnote-6)

|  |
| --- |
| * 1. W zakresie świadczonych usług chmury obliczeniowej i odpowiednio do ich skali dostawca usług chmury obliczeniowej spełnia wymagania zapewnienia zgodności swojego działania z poniższymi normami lub ich odpowiednikami w polskim lub europejskim układzie normalizacji, chyba że podmiot nadzorowany akceptuje (na podstawie wyników szacowania ryzyka) brak konieczności spełnienia tego wymagania albo jego części:      1. PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT;      2. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji;      3. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania;      4. ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej;      5. 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. Spełnienie wymagań może być poświadczone odpowiednimi certyfikatami zgodności wystawionym 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

|  |
| --- |
| * 1. Nadzór rekomenduje, aby CPD zlokalizowane było na terytorium państwa Europejskiego Obszaru Gospodarczego (EOG). Punkt ten stosuje się z zastrzeżeniem, że podmioty nadzorowane, które:      1. 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      2. 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

|  |
| --- |
| * 1. Dostawca usług chmury obliczeniowej zapewnia w swoim postępowaniu udokumentowaną zasadę ochrony przetwarzanych przez podmiot nadzorowany informacji przed nieautoryzowanym dostępem lub użyciem przez swoich pracowników lub poddostawców poprzez co najmniej:      1. domyślną zasadę braku dostępu do przetwarzanych informacji podmiotu nadzorowanego;      2. domyślną zasadę braku konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego lub w innych uruchamianych usługach chmury obliczeniowej;      3. zasadę „minimum koniecznego” dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez podmiot nadzorowany (w tym również usunięcia usterek) oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. Obowiązujące w tym zakresie procedury obsługi mogą być dodatkowo potwierdzone stosownym certyfikatem (np. SOC[[6]](#footnote-7) 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji;      4. udostępnienie wytycznych, wzorcowych konfiguracji, opisów zasad, itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji;      5. domyślne uruchamianie nowego środowiska (lub usługi chmury obliczeniowej) separowanego od innych tenantów, z ustawieniami „secure-by-default”[[7]](#footnote-8). |

#### 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

### 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:      1. 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;      2. 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;      3. używa dedykowanych lub zalecanych przez dostawcę usług chmury obliczeniowej ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług chmury obliczeniowej;      4. 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

|  |
| --- |
| * 1. 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.   2. W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM[[8]](#footnote-9)), to HSM mogą być udostępniane przez dostawcę usług chmury obliczeniowej, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS[[9]](#footnote-10) 140-2 Level 2 lub równoważne.   3. Podmiot nadzorowany w udokumentowanym procesie zarządza tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz kontrolą tego procesu.   4. 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 wymogu powinien zostać poparty stosowną analizą ryzyka (patrz pkt VI.2. ust. 5.a) Komunikatu).
2. W zależności od Modelu usługi chmury obliczeniowej, proces zarządzania generowaniem, dostarczaniem, 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. Generowanie lub zarządzanie kluczami szyfrującymi, które są używane do szyfrowania informacji przetwarzanej w usługach chmury obliczeniowej innego dostawcy usług chmury obliczeniowej, nie jest uznawane za równoznaczne z generowaniem i zarządzaniem kluczami przez podmiot nadzorowany.
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.
5. Oceniając ryzyko podmiot nadzorowany powinien ustalić, czy dostawca chmury obliczeniowej (w tym jego poddostawcy) ma lub może mieć dostęp do danych przetwarzanych w chmurze obliczeniowej, i na jakich warunkach. Informacje te powinny być przechowywane przez okres niezbędny do realizacji umowy i udostępniane podmiotowi.

#### 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 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 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

### 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 USŁUG CHMURY OBLICZENIOWEJ

1. Dokumentacja w zakresie logowania zdarzeń w Chmurze obliczeniowej, a także możliwości integracji mechanizmów logowania w Chmurze obliczeniowej z systemem klasy SIEM, jeżeli są wykorzystywane w Zakładzie Ubezpieczeń.

#### Szablony

N/D

|  |
| --- |
| * 1. Wymagania w stosunku do podmiotu nadzorowanego w zakresie zarządzania dostawcami usług mającymi dostęp zdalny do usług chmury obliczeniowej wykorzystywanych przez podmiot nadzorowany[[10]](#footnote-11):      1. podmiot nadzorowany zapewnia, że wyłącznie uprawniony personel dostawcy usług ma dostęp do wskazanych systemów teleinformatycznych lub ich wybranych zakresów;      2. podmiot nadzorowany wymaga używania przez personel dostawcy usług uwierzytelnienia MFA, przy czym rodzaj i zakres uzależniony jest od wyników szacowania ryzyka;      3. 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

### 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:      1. 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;      2. 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;      3. zasady kategoryzacji informacji lub systemów pod kątem przetwarzania w chmurze obliczeniowej lub odniesienie do obecnie funkcjonujących klasyfikacji, jeżeli mogą być stosowane;      4. zasady stosowanych zabezpieczeń technologicznych i rozwiązań organizacyjnych;      5. zasady zarządzania ciągłością działania;      6. zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z dostawcą usług chmury obliczeniowej;      7. zasady zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi;      8. zasady przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem usług chmury obliczeniowej;      9. zasady raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej;      10. umowy z dostawcami usług chmury obliczeniowej wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań;      11. procesy, procedury lub instrukcje dotyczące:          1. analizy zagrożeń i szacowania ryzyka, w tym źródła pozyskiwania informacji o zagrożeniach specyficznych dla stosowanych usług chmury obliczeniowej oraz sektora finansowego;          2. zarządzania środowiskiem teleinformatycznym (sieciami, systemami, aplikacjami, bazami danych, itp.), z uwzględnieniem usług chmury obliczeniowej, w tym planowanie, rozwój i utrzymywanie;          3. zarządzania logami;          4. zarządzania kluczami szyfrującymi;          5. zarządzania incydentami bezpieczeństwa;          6. 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 wdrożonych 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

## 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[[11]](#footnote-12) przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej (a w przypadku, gdy przetwarzanie to już jest realizowane – nie później niż 1 sierpnia 2020 r.) informuje UKNF o:    1. rodzaju i zakresie informacji planowanych do przetwarzania / przetwarzanych w chmurze obliczeniowej;    2. nazwie dostawcy usług chmury obliczeniowej oraz rodzaju planowanych do używania / używanych usług chmury obliczeniowej;    3. dacie podpisania umowy z dostawcą usług chmury obliczeniowej oraz terminach jej obowiązywania, a w przypadku, gdy umowa nie jest jeszcze zawarta – przewidywaną datę jej zawarcia;    4. lokalizacji (kraj, region albo inne równoważne) centrum przetwarzania danych (CPD) świadczącym usługę chmury obliczeniowej;    5. spełnieniu wymagań opisanych w niniejszym komunikacie;    6. osobach lub stanowiskach do kontaktu w sprawie stosowania chmury obliczeniowej w podmiocie nadzorowanym. 2. Powyższa informacja powinna zostać podpisana przez uprawnionego przedstawiciela podmiotu nadzorowanego oraz dostarczona do UKNF przy wykorzystaniu formularza stanowiącego załącznik nr 1 do niniejszego komunikatu. |

#### Opis wymagań

1. Z zastrzeżeniem 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 uwzględniających korzystanie z chmury  przez Zakład Ubezpieczeń, któremu powierzono przetwarzanie, jeżeli korzystanie z chmury jest jego autonomiczną decyzją. W tym, z uwzględnieniem:
3. 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 chmury.
4. każdy Zakład Ubezpieczeń prowadzi ewidencję umów outsourcingu chmurowego. Zalecane jest aby ewidencja, w zakresie usług chmury obliczeniowej, uwzględniała również informacje wymienione w Załączniku Nr 1 do Komunikatu. Ewidencja umów outsourcingu chmurowego może nie stanowić ewidencji umów outsourcingu w rozumieniu art. 77 ustawy o działalności ubezpieczeniowej i reasekuracyjnej.
5. 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.
6. W przypadku rozszerzenia zakresu lub zmiany rodzaju przetwarzanych danych podmiot nadzorowany zawiadamia UKNF poprzez przesłanie informacji w sprawie przetwarzania informacji w chmurze obliczeniowej.
7. 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). ). Jeśli przetwarzanie informacji w chmurze obliczeniowej pozostaje w związku z outsourcingiem funkcji należących do systemu zarządzania oraz podstawowych lub ważnych czynności, zastosowanie będzie miał termin 30 dni na notyfikację w sprawie przewarzania informacji.
8. Uprawnionym do podpisania informacji, o której mowa 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 Zakład Ubezpieczeń

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

#### WYMAGANIA (produkty) po stronie dostawcy USŁUG CHMURY OBLICZENIOWEJ

N/D

#### Szablony

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

# komunikat a przepisy UDUiR

## Wymogi wynikające z UDUR – regulacje o charakterze ogólnym

1. Z uwagi na kwalifikację zakładów ubezpieczeń jako instytucji zaufania publicznego działalność ubezpieczeniowa poddana została kompleksowej regulacji zarówno na poziomie prawa krajowego, jak i unijnego. Jednym z istotnych elementów regulacji działalności zakładów ubezpieczeń są wymogi odnoszące się do powierzania przez zakłady ubezpieczeń wykonywania określonych czynności podmiotom zewnętrznym, w tym dostawcom usług informatycznych.
2. Bezwzględnie wiążące wymogi prawne dotyczące dokonywania outsourcingu przez zakłady ubezpieczeń wynikają z następujących aktów prawnych:
   1. ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej („UDUR”), która w zakresie regulacji outsourcingu stanowi implementację do polskiego porządku prawnego przepisów dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II);
   2. rozporządzenia delegowanego Komisji (UE) 2015/35 z dnia 10 października 2014 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady 2009/138/WE w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) („Rozporządzenie 2015/35”).
3. Regulacja wynikająca z ww. aktów prawnych ma charakter ogólny i znajduje zastosowanie do szerokiego zakresu umów zawieranych przez zakłady ubezpieczeń z dostawcami zewnętrznymi. Zgodnie z przepisem art. 3 ust. 1 pkt 27 UDUR przez „outsourcing” należy rozumieć „umowę między zakładem ubezpieczeń albo zakładem reasekuracji a dostawcą usług, na podstawie której dostawca usług wykonuje proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez zakład ubezpieczeń lub zakład reasekuracji, a także umowę, na podstawie której dostawca usług powierza wykonanie takiego procesu, usługi lub działania innym podmiotom, za pośrednictwem których wykonuje on dany proces, usługę lub działanie”.
4. O ile niektóre przepisy ww. aktów prawnych ustanawiają konkretne wymogi w przypadku outsourcingu (tj. outsourcingu w rozumieniu art. 3 ust. 1 pkt 27 UDUR), o tyle większość z nich ma zastosowanie wyłącznie do określonego zakresu umów outsourcingowych, tj. umów outsourcingu czynności ubezpieczeniowych, czynności reasekuracyjnych, funkcji należących do systemu zarządzania czy czynności podstawowych lub ważnych.
5. Zakład ubezpieczeń powinien dokonać kwalifikacji każdej zawieranej umowy outsourcingu, jak i umowy o świadczenie usług chmury obliczeniowej, i na tej podstawie zidentyfikować zakres wymogów prawnych, które mają do niej zastosowanie. Kwalifikacja umów o świadczenie usług chmury obliczeniowej powinna uwzględniać zakres procesów realizowanych z wykorzystaniem danej usługi oraz informacji przetwarzanych z wykorzystaniem tej usługi, w czym pomocny może być proces klasyfikacji i oceny informacji przetwarzanych w chmurze przeprowadzony zgodnie z wymogami nadzorczymi, o których piszemy poniżej.

## Wymogi wynikające z komunikatu – regulacje o charakterze szczegółowym

1. Szereg dodatkowych wymogów w zakresie outsourcingu dokonywanego przez zakłady ubezpieczeń wynika z rekomendacji lub wytycznych organów nadzoru lub innych podmiotów publicznych, które określane są mianem „prawa miękkiego”. Mimo że akty takie nie posiadają charakteru bezwzględnie wiążących przepisów prawa, to ich treść może określać np. oczekiwany przez organy nadzoru sposób realizacji wymogów wynikających z przepisów prawa oraz wskazywać na możliwy sposób korzystania przez organy nadzoru z przysługujących im kompetencji nadzorczych.
2. Spośród aktów prawa miękkiego mających zastosowanie do korzystania przez zakłady ubezpieczeń z usług chmury obliczeniowej wskazać należy przede wszystkim na komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z 23 stycznia 2020 r. („Komunikat UKNF”).
3. Rolą prawa miękkiego, w tym Komunikatu UKNF, jest w szczególności wskazanie kierunków właściwej interpretacji wymagań wynikających z przepisów wiążących bezwzględnie. Z funkcją interpretacyjną wiąże się także wyższy stopień szczegółowości regulacji. Akty prawa miękkiego doprecyzowują ogólne wymogi ustawowe, pozwalając na ich dostosowanie do zmieniającego się otoczenia gospodarczego i potrzeb rynkowych. Naturalnie dotyczy to w szczególności obszaru informatycznego, który jest wyjątkowo podatny na dynamiczne zmiany.
4. Z perspektywy praktycznej Komunikat UKNF stanowi zatem zestaw dyrektyw interpretacyjnych służących wsparciu podmiotów nadzorowanych w zapewnieniu zgodności regulacyjnej i prawidłowym ukształtowaniu przez nie procesów wewnętrznych oraz relacji z dostawcami zewnętrznymi – tak, aby mogły one utrzymać zgodność z obowiązującymi przepisami prawa i oczekiwaniami organu nadzoru.
5. Jednocześnie, z uwagi na swoistą kwalifikację prawną, akty prawa miękkiego nie mogą wyłączać ani ograniczać stosowania przepisów o randze ustawowej. Wprost przesądzono o tym także w treści Komunikatu UKNF. Nadzór wyraźnie podkreśla, że zdefiniowanie w Komunikacie UKNF modelu referencyjnego stosowania chmury obliczeniowej nastąpiło „w celu wsparcia podmiotów nadzorowanych oraz unikania wątpliwości interpretacyjnych” i oczekuje jego traktowania „jako sprecyzowanie istniejących wymagań prawnych oraz bez uszczerbku dla tych wymagań”[[12]](#footnote-13)

## Wpływ komunikatu na wybrane wymogi UDUR

1. Komunikat UKNF powinien być stosowany przez zakład ubezpieczeń w przypadku przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej (w zakresie jej części opartej o chmurę obliczeniową publiczną), jeżeli:
   1. przetwarzane informacje należą do informacji prawnie chronionych w rozumieniu Komunikatu UKNF lub
   2. przetwarzanie informacji ma charakter outsourcingu szczególnego chmury obliczeniowej w rozumieniu Komunikatu UKNF.
2. Obowiązek stosowania Komunikatu UKNF nie ma zatem bezpośredniego związku z kwalifikacją umowy z dostawcą usług chmury obliczeniowej na gruncie obowiązujących przepisów prawa. Innymi słowy – zakład ubezpieczeń powinien zweryfikować, czy wymogi Komunikatu UKNF mają zastosowanie niezależnie od tego, czy konkretna umowa z dostawcą usług chmury obliczeniowej stanowi którykolwiek z rodzajów outsourcingu regulowanych przepisami UDUR (zob. w tym zakresie uwagi w pkt 1.3 i nast. powyżej).
3. Jak wskazywano wyżej, treść Komunikatu UKNF może wpływać na interpretację konkretnych wymogów wynikających z obowiązujących zakład ubezpieczeń przepisów prawa. Komunikat UKNF odnosi się m.in. do kwestii zakresu odpowiedzialności dostawcy usług chmury obliczeniowej w stosunku do zakładu ubezpieczeń. Zgodnie ze stanowiskiem wyrażonym w pkt VI.2.6.b Komunikatu UKNF zakres odpowiedzialności dostawcy (oraz jego poddostawców) wobec zakładu ubezpieczeń może ulegać ograniczeniu albo wyłączeniu w granicach przepisów prawa regulujących działalność zakładów ubezpieczeń. Jednocześnie – niezależnie od wymogów ustawowych – UKNF wyraża krytyczną ocenę wobec wyłączeń lub ograniczeń odpowiedzialności dostawców usług chmury obliczeniowej wobec zakładów ubezpieczeń, 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.
4. Przepisy UDUR nie wprowadzają zakazu ograniczania lub wyłączania odpowiedzialności outsourcera wobec zakładu ubezpieczeń, dlatego powyższe stanowisko nadzoru należy traktować wyłącznie jako zalecenie, które nie jest zabezpieczone sankcją prawną. Z drugiej jednak strony, rekomendowane jest ukształtowanie relacji kontraktowej z dostawcą w taki sposób, aby zakład ubezpieczeń mógł dochodzić pełnego odszkodowania w przypadku wystąpienia takich szkód.
5. Komunikat UKNF ustanawia ponadto dodatkowy obowiązek notyfikacyjny (pkt VIII), zgodnie z którym zakład ubezpieczeń powinien zawiadomić UKNF o przypadkach outsourcingu szczególnego lub przetwarzania informacji prawnie chronionych w terminie 14 dni przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej, chyba że szczególny przepis prawa przewiduje inny termin przekazania informacji.
6. Taki inny termin w konkretnym przypadku może wynikać z art. 75 ust. 2 UDUR, który zobowiązuje zakłady ubezpieczeń do zawiadomienia Komisji Nadzoru Finansowego co najmniej na 30 dni przed wdrożeniem outsourcingu funkcji należących do systemu zarządzania lub outsourcingu podstawowych lub ważnych czynności, a także o istotnej zmianie w takim outsourcingu.
7. Jeżeli zatem dany przypadek korzystania przez zakład ubezpieczeń z usługi chmury obliczeniowej będzie wypełniał zarówno przesłanki stosowania Komunikatu UKNF, jak i uznania go za outsourcing funkcji należących do systemu zarządzania lub czynności podstawowych lub ważnych, o których mowa w art. 75 ust. 2 UDUR, to zakład ubezpieczeń powinien zawiadomić Komisję Nadzoru Finansowego o planowanym przetwarzaniu w terminie wynikającym z art. 75 ust. 2 UDUR, a nie w terminie określonym w pkt VIII.1 Komunikatu UKNF.
8. UKNF zwrócił uwagę na powyższy problem w opublikowanych 18 października odpowiedziach na pytania przedstawicieli podmiotów nadzorowanych. Zgodnie z przekazanymi wyjaśnieniami, „o ile […] przetwarzanie informacji w chmurze obliczeniowej pozostaje w związku z outsourcingiem regulowanym art. 75 ust. 2 [UDUR], zastosowanie będzie miał termin 30 dni na notyfikację w sprawie przetwarzania informacji”[[13]](#footnote-14).
9. W przypadku zawiadomienia dokonywanego zgodnie z art. 75 ust. 2 UDUR Komisja Nadzoru Finansowego wymaga przekazania określonych informacji na specjalnym formularzu, który został przez nią udostępniony zakładom ubezpieczeń. W przypadku zawiadomienia dokonywanego zgodnie z wymogami Komunikatu UKNF należy z kolei posługiwać się formularzem stanowiącym załącznik nr 1 do Komunikatu UKNF (pkt VIII.2). Zakresy informacji objętych poszczególnymi formularzami nie są jednakowe, w związku z czym wydaje się, że zakład ubezpieczeń powinien przekazać w ramach notyfikacji oba formularze.
10. Ponadto Komunikat UKNF odnosi się m.in. do następujących kwestii, które regulowane są przez obowiązujące przepisy sektorowe:
    1. zasady szacowania ryzyka związanego z outsourcingiem,
    2. zasady korzystania z poddostawców w łańcuchach outsourcingowych,
    3. umowne zapewnienie możliwości realizacji czynności kontrolnych wobec dostawcy,
    4. metody zapobiegania ujawnieniu informacji, w tym informacji objętych tajemnicą ubezpieczeniową.

# Załączniki

## Załącznik nr 1 – Przykład szablonu klasyfikacji informacji

## Załącznik nr 2 – Przykład szablonu szacowania ryzyka

## Załącznik nr 3 – Przykładowy plan przetwarzania informacji w chmurze obliczeniowej

## Załącznik nr 4 - Przykładowy szablon scenariusza wyjścia z chmury

## Załącznik nr 5 - Przykład - Wyjście z chmury - główne zagadnienia

## Załącznik nr 6 - ISO 27001

## Załącznik nr 7 - PRZYKŁADOWE Kroki wdrożenia usługi przetwarzania INFORMACJI w chmurze obliczeniowej PUBLICZNEJ LUB HYBRYDOWEJ w ZAKŁADZIEUBEZPIECZEŃ

## Załącznik nr 8 - Przykład - Proces wdrożenia

## ZAŁĄCZNIK NR 9 – PRZYKŁAD - OPIS METODYKI UZYSKANIA SZACOWANIA RYZYKA I ZGODNOŚCI Z KOMUNIKATEM UKNF

## ZAŁĄCZNIK NR 10 - PRZYKŁADOWE WYPEŁNIENIE INFORMACJI DO UKNF O ROZPOCZĘCIU KORZYSTANIA Z CHMURY OBLICZENIOWEJ PRZEZ ZAKŁAD UBEZPIECZEŃ

## ZAŁĄCZNIK NR 11 - przykładowe klauzule umowne

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. [↑](#footnote-ref-2)
2. Okresowa weryfikacja i aktualizacja powinna być prowadzona zgodnie z praktyką i zasadami podmiotu nadzorowanego, jednak nie rzadziej niż raz w roku. [↑](#footnote-ref-3)
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. [↑](#footnote-ref-4)
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. [↑](#footnote-ref-5)
5. Wymagania te uwzględnia podmiot nadzorowany w swoim podejściu do stosowania usług chmury obliczeniowej, a w szczególności w procesie szacowania ryzyka. [↑](#footnote-ref-6)
6. System and Organization Controls. [↑](#footnote-ref-7)
7. Oznacza domyślną konfigurację usługi chmury obliczeniowej, która uwzględnia wymagania bezpieczeństwa przetwarzania informacji, w szczególności zapobiega przypadkowemu (niezamierzonemu) ujawnieniu przetwarzanej informacji. [↑](#footnote-ref-8)
8. HSM – Hardware Security Module, urządzenie do przechowywania i zarządzania kluczami kryptograficznymi [↑](#footnote-ref-9)
9. Federal Information Processing Standard – publiczne standardy dla agencji cywilnych i rządowych w USA. W tym przypadku międzynarodowy standard bezpieczeństwa dla systemów kryptograficznych. [↑](#footnote-ref-10)
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. [↑](#footnote-ref-11)
11. Chyba że szczególny przepis prawa dotyczący działalności podmiotu nadzorowanego przewiduje inny termin przekazania informacji. [↑](#footnote-ref-12)
12. Pkt III.1 oraz IV.1 Komunikatu UKNF. [↑](#footnote-ref-13)
13. Pytania i odpowiedzi (Q&A) w zakresie stosowania Komunikatu UKNF z 23 stycznia 2020 r. dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, odpowiedź UKNF na pytanie: „Jakie terminy notyfikowania w sprawie przetwarzania informacji w chmurze obliczeniowej, inne niż wskazany w pkt VIII.1 Komunikatu termin 14 dni, mogą mieć zastosowanie do zakładów ubezpieczeń i zakładów reasekuracyjnych na gruncie ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej?”, <https://www.knf.gov.pl/dla_rynku/fin_tech/chmura_obliczeniowa/Q&A> (dostęp: 31.01.2022 r.). [↑](#footnote-ref-14)