

========== PROJEKT ========== listopada 2019 r.

Komunikat Urzędu Komisji Nadzoru Finansowego

dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej

o charakterze publicznym lub hybrydowym

1. **Definicje**
2. Używane pojęcia przyjęto wyłącznie na potrzeby niniejszego komunikatu, uwzględniając specyfikę przetwarzania informacji w chmurze obliczeniowej:
3. **podmiot nadzorowany** – podmiot podlegający nadzorowi nad rynkiem finansowym zgodnie z ustawą z 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, art. 1 ust. 2 pkt. 1) – 8);
4. **informacja prawnie chroniona** – informacja związana z tajemnicami sektora finansowego wymienionymi w ustawach:
	1. sektor bankowy:
		1. ustawa z 29 sierpnia 1997 r. Prawo bankowe, art. 104;
	2. sektor kapitałowy:
		1. ustawa z 29 lipca 2005 r. o obrocie instrumentami finansowymi, art. 3 ust. 52, art. 147, art. 153;
		2. ustawa z 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi, art. 280;
		3. ustawa z 26 października 2000 r. o giełdach towarowych, art. 2 ust. 10, art. 53;
	3. sektor ubezpieczeniowy:
		1. ustawa z 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, art. 35 ust. 1;
		2. ustawa z 15 grudnia 2017 r. o dystrybucji ubezpieczeń, art. 22 ust. 5 pkt 3), art. 32 ust. 3 pkt. 1);
	4. sektor kapitałowego systemu emerytalnego:
		1. ustawa z 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych, art. 49;
		2. ustawa z 4 października 2018 r. o pracowniczych planach kapitałowych, art. 3 ust. 3;
	5. sektor usług płatniczych:
		1. ustawa z 19 sierpnia 2011 r. o usługach płatniczych, art. 11;
	6. sektor kas spółdzielczych:
		1. ustawa z 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, art. 9e;
5. **chmura obliczeniowa** – model przetwarzania informacji oparty na użytkowaniu przez podmiot nadzorowany usług dostarczonych przez dostawcę usług chmury obliczeniowej, zawierający zarówno infrastrukturę jak i (w stosownych przypadkach) wymagane oprogramowanie.

Przetwarzanie w chmurze obliczeniowej jest definiowane przez National Institute of Standards and Technology jako model świadczenia usług zapewniający niezależny od lokalizacji, dogodny dostęp sieciowy „na żądanie” do współdzielonej puli konfigurowalnych zasobów obliczeniowych (np. serwerów, pamięci masowych, aplikacji lub usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale dostawcy usług[[1]](#footnote-2).

Niniejszy komunikat odnosi się do chmury obliczeniowej publicznej i hybrydowej, niezależnie od modelu świadczenia usługi[[2]](#footnote-3);

1. **chmura obliczeniowa publiczna** – chmura obliczeniowa dostępna do użytku publicznego, będąca w posiadaniu i/lub bezpośrednio zarządzana przez dostawcę usług chmurowych;
2. **chmura obliczeniowa hybrydowa** – chmura obliczeniowa składająca się z dwóch lub więcej odrębnych chmur obliczeniowych, zarządzanych przez odrębnych dostawców usług chmury obliczeniowej. Może składać się z kilku chmur obliczeniowych publicznych lub w kombinacji z infrastrukturą chmury obliczeniowej będącą w posiadaniu i/lub bezpośrednim zarządzaniu podmiotu nadzorowanego. Chmura hybrydowa zapewnia zgodność technologiczną i prawną przetwarzania informacji między wszystkimi chmurami obliczeniowymi, które ją tworzą;
3. **outsourcing chmury obliczeniowej** (dalej: **outsourcing**) – oznacza umowę w dowolnej formie zawartą między podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej, na mocy której dostawca usług chmury obliczeniowej dostarcza podmiotowi nadzorowanemu usługę chmury obliczeniowej, która służy do wsparcia realizacji procesu, usługi lub zadania, które podmiot nadzorowany realizowałby samodzielnie, gdyby usługa chmury obliczeniowej była niedostępna;
4. **outsourcing szczególny chmury obliczeniowej** (dalej: **outsourcing szczególny**) – oznacza outsourcing chmury obliczeniowej, w ramach którego podmiot nadzorowany powierza dostawcy usług chmury obliczeniowej wykonanie za pomocą usługi chmury obliczeniowej:
5. czynności istotnych lub ważnych dla działalności podmiotu nadzorowanego i/lub
6. podstawowych lub istotnych funkcji operacyjnych podmiotu nadzorowanego.

Powierzenie dostawcy usług chmury obliczeniowej określonej czynności i/lub funkcji ma charakter outsourcingu szczególnego, jeżeli:

1. awaria świadczonej usługi i/lub naruszenie zasad bezpieczeństwa mogą mieć potencjalny wpływ na podmiot nadzorowany, jego:
	1. działalność gospodarczą, reputację lub rentowność;
	2. zdolność do zarządzania ryzykiem i zgodność z obowiązującymi przepisami ustawowymi i wykonawczymi;

lub

1. obejmują informacje o kliencie i – w przypadku nieuprawnionego dostępu lub ujawnienia, lub utraty, lub kradzieży informacji o kliencie – mogą generować znaczące ryzyka dla klientów podmiotu nadzorowanego;
2. **udokumentowany proces** – zbiór powiązanych ze sobą, systematycznie realizowanych czynności, które są stosowane i wystarczająco szczegółowo dla podmiotu nadzorowanego opisane w dokumentach zewnętrznych lub wewnętrznych, wyniki tych czynności są zapisywane, a zapisy przechowywane w sposób pozwalający na obiektywne udowodnienie wykonania czynności zgodnie z wymaganiami;
3. **ważność informacji** – istotność informacji dla prowadzenia działalności podmiotu nadzorowanego;
4. **wartość informacji** – konsekwencja materializacji ryzyka polegającego na nieuprawnionym ujawnieniu, zmianie lub zniszczeniu informacji;
5. **szyfrowanie „at rest”** – szyfrowanie informacji „w spoczynku” (np. przechowywanie kopii zapasowych, przechowywanie informacji w bazie danych);
6. **szyfrowanie „in transit”** – szyfrowanie w trakcie transmisji informacji (np. podczas przesyłania informacji z/do chmury obliczeniowej);
7. **łańcuch outsourcingowy** – relacja polegająca na powierzeniu przez dostawcę usług chmury obliczeniowej części czynności (związanych z dostarczaniem usługi chmury obliczeniowej dla podmiotu nadzorowanego) swojemu poddostawcy;
8. **poddostawca** – podmiot i/lub osoba, która świadczy usługi dla dostawcy usług chmury obliczeniowej;
9. **RTO** – Recovery Time Objective. Czas od momentu awarii systemu teleinformatycznego do momentu przywrócenia jego normalnego działania;
10. **RPO** – Recovery Point Objective. Maksymalny czas pomiędzy wykonaniem kopii zapasowej informacji a momentem wystąpienia awarii systemu teleinformatycznego. Oznacza również potencjalną możliwość utraty wyników przetwarzania informacji przez wskazany czas;
11. **SLA** – Service Level Agreement. Umowa o gwarantowanym poziomie świadczenia usługi teleinformatycznej;
12. **HSM** – Hardware Security Module. Urządzenie do przechowywania i zarządzania kluczami kryptograficznymi;
13. **tenant** – organizacja posiadająca i zarządzająca usługami i/lub instancjami środowisk teleinformatycznych w chmurze obliczeniowej. Najważniejszą właściwością tenantu jest jego domyślna separacja (konfiguracji oraz przetwarzanych informacji) od innych tenantów. Każdy pomiot nadzorowany może posiadać wiele tenantów u tego samego dostawcy usług chmury obliczeniowej, jednak wszystkie wymagania związane z separacją tenantów muszą być zachowane;
14. **MFA** – Multi Factor Authentication. Metoda wieloskładnikowego uwierzytelniania;
15. **CPD** – centrum przetwarzania danych;
16. **SIEM** – Security Information and Event Management. System do zarządzania informacją i zdarzeniami bezpieczeństwa.
17. **Wprowadzenie**
18. Postęp technologiczny w obszarze technologii chmury obliczeniowej o charakterze publicznym lub hybrydowym (dalej: chmura lub chmura obliczeniowa) wywołuje wątpliwości ze strony podmiotów nadzorowanych w zakresie możliwości stosowania tej technologii oraz – w przypadku dopuszczalności takiego rozwiązania – zasady dokonywania outsourcingu, w szczególności podczas przetwarzania informacji prawnie chronionych.
19. Urząd Komisji Nadzoru Finansowego (dalej: UKNF) dostrzega brak standaryzacji w podejściu do korzystania z usług przetwarzania w chmurze obliczeniowej w odniesieniu do tych samych kategorii informacji przez podmioty nadzorowane sektora finansowego, co może prowadzić do istotnych różnic w ocenie ryzyka technologicznego, a tym samym powodować zwiększenie ryzyka sektorowego.
20. Usługa przetwarzania informacji w chmurze obliczeniowej ma charakter powierzenia czynności przetwarzania i – zależnie od kategorii przetwarzanych informacji oraz faktycznie realizowanych czynności przetwarzania – może być traktowana jako outsourcing lub outsourcing szczególny. Niniejszy komunikat nie wyłącza przepisów bezwzględnie obowiązujących w tym zakresie, natomiast celem jest zaprezentowanie, jak nadzór rozumie te przepisy.
21. Niniejszy komunikat jest uzupełnieniem i uszczegółowieniem wybranych zaleceń w zakresie outsourcingu opisanych w:
22. rekomendacji D;
23. rekomendacji D-SKOK;
24. wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych;
25. wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji;
26. wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych;
27. wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w podmiotach infrastruktury rynku kapitałowego;
28. wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych.

Podmioty nadzorowane, których nie dotyczą powyższe rekomendacje i wytyczne, powinny stosować postanowienia niniejszego komunikatu wprost.

1. Niniejszy komunikat jest podejściem krajowym do outsourcingu przetwarzania informacji w chmurze obliczeniowej dla sektora finansowego (model referencyjny). Tym samym:
2. komunikat UKNF z 23 października 2017 r. dotyczący „korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej” zostaje zastąpiony w całości przez niniejszy komunikat;
3. wytyczne, zalecenia lub inne dokumenty prezentujące stanowisko Europejskiego Urzędu Nadzoru Bankowego, Europejskiego Urzędu Nadzoru nad Ubezpieczeniami i Pracowniczymi Programami Emerytalnymi bądź Europejskiego Urzędu Nadzoru nad Rynkami i Papierami Wartościowymi, które odnoszą się lub mogłyby odnosić się w przyszłości do przetwarzania informacji w chmurze obliczeniowej nie mają zastosowania do podmiotów nadzorowanych w tym zakresie.
4. Powszechne korzystanie z usług chmury obliczeniowej przez podmioty nadzorowane może powodować ryzyko koncentracji przetwarzania informacji prawnie chronionych znacznej części sektora finansowego fizycznie w tych samych obiektach (centrach przetwarzania danych) i/lub w ramach współpracy podmiotów nadzorowanych z ograniczoną liczbą dostawców usług chmury obliczeniowej. Dodatkowo przetwarzanie informacji prawnie chronionych w chmurze obliczeniowej generuje identyczne ryzyka związane z ochroną przetwarzanych informacji, niezależnie od charakteru i ważności lub istotności procesu outsourcingowego. Z uwagi na te ryzyka nadzór oczekuje, że podmioty nadzorowane będą informowały UKNF o zamiarze wdrożenia outsourcingu szczególnego w chmurze obliczeniowej i/lub w celu przetwarzania informacji prawnie chronionych, na zasadach określonych w niniejszym komunikacie.
5. **Model referencyjny**
6. W celu wsparcia podmiotów nadzorowanych oraz unikania wątpliwości interpretacyjnych UKNF definiuje model referencyjny stosowania usług chmury obliczeniowej, na który składają się opisane w niniejszym komunikacie:
7. wytyczne stosowania;
8. wytyczne do klasyfikacji i oceny informacji;
9. wytyczne do szacowania ryzyka;
10. minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej;
11. zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej.
12. **Wytyczne stosowania**
13. 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:
14. przetwarzane informacje należą do informacji prawnie chronionych zgodnie z niniejszym komunikatem i/lub
15. przetwarzanie informacji ma charakter outsourcingu szczególnego zgodnie z niniejszym komunikatem.
16. Nadrzędnym zadaniem podmiotu nadzorowanego przy przetwarzaniu 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 informacji w chmurze obliczeniowej. 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.
17. Nadzór podkreśla, że opisane w niniejszym komunikacje wymagania powinny być stosowane przez podmioty nadzorowane przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej.
18. W celu właściwego stosowania postanowień niniejszego komunikatu podmiot nadzorowany powinien określić dla każdej planowanej do wykorzystania lub wykorzystywanej usługi chmury obliczeniowej:
19. czy przetwarzane są informacje prawnie chronione oraz
20. czy czynność przetwarzania może być definiowana jako outsourcing szczególny.

|  |  |
| --- | --- |
| Matryca stosowania komunikatu | Outsourcing |
| 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 i/lub informacji do więcej niż jednej kategorii według powyższej matrycy, należy przyjąć jako stosowane wymaganie bardziej rygorystyczne.
2. Niezależnie od powyższego, niniejszego komunikatu nie stosuje się, gdy stosowny szczególny przepis prawa:
3. wyklucza możliwość przetwarzania w chmurze obliczeniowej określonej informacji i/lub wyklucza możliwość wykonywania w chmurze obliczeniowej określonych czynności przetwarzania;
4. nakłada wymóg spełnienia określonych wymagań technicznych i/lub organizacyjnych dotyczących przetwarzania określonych informacji, które wykluczałyby możliwość spełnienia wymagań niniejszego komunikatu.
5. **Wytyczne do klasyfikacji i oceny informacji**
6. Podmiot nadzorowany przeprowadza w udokumentowanym procesie klasyfikację i ocenę informacji pod kątem dopuszczalności ich przetwarzania w chmurze obliczeniowej, w szczególności biorąc pod uwagę:
7. zgodność z wymaganiami prawa oraz specyficznymi dla sektora finansowego i/lub podmiotu nadzorowanego postanowieniami oraz zobowiązaniami kontraktowymi;
8. zakres klasyfikowanych informacji, ich rodzaj i ważność;
9. wartość informacji dla podmiotu nadzorowanego;

w odniesieniu do przetwarzanych przez podmiot nadzorowany:

1. informacji prawnie chronionych w rozumieniu niniejszego komunikatu;
2. informacji, których ochrona wynika z uregulowań prawnych nie uwzględnionych w niniejszym komunikacie;
3. informacji, które nie podlegają ochronie prawnej.
4. Podmiot nadzorowany w procesie klasyfikacji i oceny informacji uwzględnia:
5. skalę prowadzonej działalności;
6. korporacyjne, grupowe lub inne modele i/lub metody oceny i klasyfikacji, które uwzględniają powyższe założenia i są wspólne dla grupy podmiotów, do których zalicza się podmiot nadzorowany;
7. odpowiedzialność podmiotu nadzorowanego za przetwarzane informacje.
8. Podmiot nadzorowany powinien przeprowadzić klasyfikację i ocenę informacji ponownie, gdy:
	1. zamierza przetwarzać nowy rodzaj informacji, a w szczególności o większej ważności;
	2. zamierza wykorzystać nową usługę chmury obliczeniowej lub istniejąca usługa będzie przetwarzała informacje w innym CPD niż dotychczas wykorzystywane;
	3. zmiana prawa, regulacji, regulaminów lub postanowień umów, których stroną jest podmiot nadzorowany, wpływa lub może wpływać na zgodność postępowania podmiotu nadzorowanego w kontekście przetwarzania informacji w chmurze obliczeniowej;
	4. istotnie zwiększa się lub zmniejsza skala działalności podmiotu nadzorowanego i skala przetwarzania informacji w chmurze obliczeniowej;
	5. istotnie zwiększa się wartość przetwarzanych w chmurze obliczeniowej informacji dla podmiotu nadzorowanego.
9. Podmiot nadzorowany powinien regularnie (lecz nie rzadziej niż raz w roku) przeglądać i potwierdzać adekwatność stosowanej klasyfikacji i oceny informacji do bieżących warunków swojego działania.
10. **Wytyczne do szacowania ryzyka**
11. Podmiot nadzorowany prowadzi w udokumentowanym procesie kompleksowe szacowanie ryzyka (identyfikację, analizę oraz ocenę zagrożeń, możliwość ich wystąpienia oraz wpływ tego wystąpienia na podmiot nadzorowany i prowadzoną działalność), zgodnie z wymaganiami aktualnego wydania normy PN-ISO 27005 lub jej odpowiednika w europejskim systemie normalizacji, lub na bazie innego, usystematyzowanego podejścia[[3]](#footnote-4). Szacowanie ryzyka jest prowadzone w sposób ciągły, z uwzględnieniem praktycznej implementacji zasady PDCA („plan – do – check – act”).
12. 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 i/lub zezwoleń) poprzez korzystanie z usług chmury obliczeniowej w sposób niezamierzony lub inny niż zamierzony;
		3. dostęp do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) dostawcy usług chmurowych;
		4. pozaumowny dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się fizycznie przetwarzanie (lokalizacja centrum przetwarzania danych);
		5. brak zgodności pomiędzy usługami różnych dostawców chmury obliczeniowej;
		6. słabość mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej;
		7. podatność interfejsów zarządzających usługami, które są udostępniane przez dostawców usług chmurowych;
		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 podwykonawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej;
		10. podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy dostawcą usług chmury obliczeniowej a podmiotem nadzorowanym;
	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 i/lub publicznie dostępnych parametrów konfiguracyjnych usług, bez ich należytej weryfikacji i 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. brak jest gwarancji dla uznania danego algorytmu szyfrowania za „całkowicie bezpieczny”. Nadzór zaleca używanie algorytmów szyfrowania, które nie są powszechnie uznane za skompromitowane. W przypadku używania algorytmu uznanego za skompromitowany podmiot nadzorowany powinien niezwłocznie podjąć działania w celu zapewnienia bezpieczeństwa przetwarzanych informacji;
		3. informacje przetwarzane w chmurze obliczeniowej powinny być szyfrowane zawsze, gdy to technologicznie możliwe i racjonalnie zasadne;
		4. informacje prawnie chronione muszą być szyfrowane zawsze „at rest” oraz „in transit”;
	6. stanowisko nadzoru w sprawie tworzenia „łańcucha outsourcingowego”, zgodnie z którym:
		1. możliwość tworzenia „łańcucha outsourcingowego” powinna być każdorazowo oceniana przez podmiot nadzorowany z perspektywy przepisów szczególnych prawa dotyczących konkretnie realizowanych czynności przetwarzania informacji w chmurze obliczeniowej;
		2. zakres odpowiedzialności dostawcy usług chmury obliczeniowej wobec podmiotu nadzorowanego nie może ulegać ograniczeniu lub wyłączeniu w zakresie odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego w wyniku niewykonania lub nienależytego wykonania umowy pomiędzy podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej, o ile:
			1. w ramach usługi chmury obliczeniowej przetwarzane są informacje prawnie chronione szyfrowane za pomocą kluczy szyfrujących dostarczonych i/lub zarządzanych przez dostawcę usług chmury obliczeniowej lub
			2. przetwarzanie ma charakter outsourcingu szczególnego;
		3. w łańcuchu outsourcingowym poddostawcą dostawcy usług chmury obliczeniowej jest podmiot, który świadczy faktyczne usługi związane z możliwością identyfikowanego dostępu do przetwarzanych przez podmiot nadzorowany informacji;
	7. 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, 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 udokumentowaną analizę prawną potwierdzającą, że zgodnie z wybranym prawem właściwym umowy wszystkie postanowienia umowy pomiędzy podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej oraz postanowienia niniejszego komunikatu są praktycznie wykonalne;
	8. inne istotne zagrożenia, które podmiot nadzorowany identyfikuje w związku z wykorzystywaniem usług chmury obliczeniowej.

1. Podmiot nadzorowany w procesie szacowania ryzyka powinien uwzględnić potencjalną możliwość:
2. korzystania ze zweryfikowanych, aktualizowanych źródeł informacji o zagrożeniach specyficznych dla stosowania usług chmury obliczeniowej, w tym również w odniesieniu do konkretnych (nazwanych) usług;
3. korzystania z pomocy ze strony podmiotów i/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;
4. przeanalizowania dostępnych wyników audytów zewnętrznych dostawców usług chmury obliczeniowej w odniesieniu do usług chmury obliczeniowej oraz procesu zarządzania bezpieczeństwem informacji dostawcy usług chmury obliczeniowej, poszerzając zakres analizy o dostępne certyfikaty wydane dostawcy usług chmury obliczeniowej potwierdzające spełnienie wymagań;
5. uprzedniego testowania usług chmury obliczeniowej, także przy wykorzystaniu scenariuszy warunków skrajnych, zarówno w zakresie sposobu działania usługi jak i jej konfiguracji.
6. Podmiot nadzorowany, na podstawie wyników szacowania ryzyka, zarządza tym ryzykiem uwzględniając w szczególności:
7. wymagania przepisów prawa, regulacji wewnętrznych oraz postanowień umownych;
8. stopień złożoności organizacyjnej, podział uprawnień i odpowiedzialności podmiotu nadzorowanego, zawarte porozumienia, oraz analogiczne czynniki występujące w grupie kapitałowej i/lub organizacji grupowej lub o charakterze stowarzyszenia, do których podmiot nadzorowany należy;
9. efektywność stosowanych mechanizmów kontrolnych i monitorujących, zwłaszcza w odniesieniu do:
	* 1. identyfikacji nowych zagrożeń;
		2. zmian w wykorzystywanej usłudze 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;
10. kompetencje techniczne i zdolności organizacyjne podmiotu nadzorowanego, w szczególności w kontekście bezpiecznego eksploatowania środowiska teleinformatycznego w chmurze obliczeniowej oraz realizacji postanowień umownych;
11. zdolność podmiotu nadzorowanego i zgodność z przepisami prawa do transferowania zidentyfikowanego ryzyka lub akceptacji oszacowanego poziomu ryzyka.
12. Wyniki szacowania ryzyka powinny zostać formalnie zatwierdzone przez uprawnionego przedstawiciela podmiotu nadzorowanego oraz podlegać okresowej weryfikacji i aktualizacji[[4]](#footnote-5). Zatwierdzenie powinno obejmować decyzję podmiotu nadzorowanego dotyczącą:
13. usług chmury obliczeniowej, z których podmiot będzie korzystał;
14. rodzaju i zakresu przetwarzanych w ramach tych usług informacji.
15. **Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej**
16. 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.
17. 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.
18. **Zapewnienie kompetencji**
	1. Podmiot nadzorowany zapewnia w udokumentowanym procesie właściwe kompetencje dla planowanych i/lub prowadzonych działań przetwarzania informacji w środowisku chmury obliczeniowej. Kompetencje te zawierają wymagania w odniesieniu do wykształcenia, wyszkolenia, umiejętności i doświadczenia pracowników własnych i/lub zewnętrznych zaangażowanych w proces planowania, realizacji, testowania i utrzymywania środowiska teleinformatycznego w chmurze obliczeniowej oraz zawierania i przeglądania umowy z tym związanej.
	2. Podmiot nadzorowany zapewnia rozumienie konsekwencji stosowania określonej architektury środowiska chmury obliczeniowej, zasad jej konfiguracji, podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji, zależnie od zakresu i rodzaju planowanego i/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 i/lub rozwojem oprogramowania przeznaczonego do używania w środowisku chmury obliczeniowej.
	3. Kompetencje pracowników i/lub współpracowników podmiotu nadzorowanego odpowiedzialnych za bezpieczeństwo oraz planowanie, konfigurację i zarządzanie oraz monitoring środowiska chmurowego powinny być potwierdzone odpowiednią dokumentacją szkoleniową i/lub imiennymi zaświadczeniami w zakresie odpowiednim do używanych usług chmury obliczeniowej, w tym również specyficznych lub specyficznie konfigurowanych dla danego dostawcy usług chmury obliczeniowej. Wymaganie to odnosi się również do kompetencji osób odpowiedzialnych za przegląd i/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.
19. **Umowa z dostawcą usług chmury obliczeniowej**
	1. Podmiot nadzorowany posiada sformalizowaną umowę na piśmie (oraz inne dokumenty, w tym oświadczenia, regulaminy, warunki korzystania z usług) z dostawcą usług chmury obliczeniowej, która – adekwatnie do używanych usług i zakresu przetwarzanych informacji - zawiera co najmniej:
	2. klarowny podział odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji, z uwzględnieniem modelu świadczenia usług, ciągłości działania usług (z uwzględnieniem parametrów RTO i RPO) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;
	3. klarowną definicję i wskazanie lokalizacji[[5]](#footnote-6) przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;
	4. prawo właściwe umowy (w tym zasady rozstrzygania sporów), w szczególności odniesienie do katalogu sytuacji (i/lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu nadzorowanego, zarówno przez organy administracji krajowej/międzynarodowej jak i przez poddostawców dostawcy usług chmury obliczeniowej;
	5. zapewnienie, że świadczenie usługi będzie realizowane zgodnie z wymaganiami prawa obowiązującymi podmiot nadzorowany, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez podmiot nadzorowany standardami;
	6. potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;
	7. gwarancje, rękojmie, kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej oraz zasad postępowania w takich sytuacjach;
	8. określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie), zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;
	9. klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) dostawcy usług chmury obliczeniowej, którzy – w związku z realizowanymi usługami – mogą mieć dostęp do przetwarzanych przez podmiot nadzorowany informacji oraz warunki nadawania praw dostępu do tych informacji;
	10. zapewnienie, że zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań wszystkich poddostawców dostawcy usług chmury obliczeniowej, którzy mają dostęp do przetwarzanych informacji, są transparentne i jasno identyfikowane przez podmiot nadzorowany;
	11. źródła autoryzowanych informacji o planowanych zmianach w standardach świadczonych usług (w tym zmianach o charakterze technicznym);
	12. źródła dokumentacji technicznej i deklaracji zgodności (w tym zgodności z obowiązującymi przepisami prawa), wraz z instrukcjami dotyczącymi konfiguracji usług;
	13. zakres dodatkowych informacji i dokumentacji przekazywanych przez dostawcę usług chmury obliczeniowej w związku ze świadczeniem usług;
	14. 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);
	15. 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;
	16. zasady licencjonowania (w tym prawo do aktualizacji bezpieczeństwa używanego oprogramowania i/lub jego komponentów) oraz prawa własności intelektualnej, w tym – jeżeli dotyczą – prawo do dysponowania przetwarzanymi informacjami;
	17. zasady zmiany treści umowy, w tym parametrów technicznych używanych usług;
	18. zasady rozwiązywania umowy, w tym zasady zwrotu i/lub usunięcia przetwarzanych informacji;
	19. zasady wsparcia, w tym zakres i okna czasowe (z uwzględnieniem stref czasowych), tryb i sposób zgłaszania problemów z usługami;
	20. 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, itp.), w celu zapewnienia adekwatności postępowania do poziomu istotności incydentu.
	21. W stosownych przypadkach i 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 środowiska i/lub usług przetwarzania tworzonego dla grupy podmiotów (w tym podmiotu nadzorowanego) w ramach umów o charakterze korporacyjnym lub grupowym.
20. **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:
21. format i strukturę przetwarzanych informacji oraz informację, jeżeli stosowane, o ich maskowaniu, pseudonimizacji lub anonimizacji;
22. sposób szyfrowania informacji oraz miejsce (i/lub sposób) przechowywania kluczy szyfrujących;
23. informację o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany;
24. daty zawarcia umowy z dostawcą usług chmury obliczeniowej i referencje do tej umowy (numer, okres obowiązywania, datę przedłużenia i/lub zmiany, daty rozpoczęcia korzystania z usług);
25. prawo właściwe, któremu podlega umowa;
26. opis zadania realizowanego za pomocą usługi wraz z informacją, czy jest to outsourcing szczególny.
	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.
	2. Podmiot nadzorowany posiada udokumentowany, wiarygodny, 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 i/lub zezwoleniami na prowadzenie określonej działalności.
	3. 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 i/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.
27. **Wymagania dla dostawców usług chmury obliczeniowej[[6]](#footnote-7)**
	1. W zakresie świadczonych usług dostawca usług chmury obliczeniowej spełnia łącznie wymagania zapewnienia zgodności swojego działania z poniższymi normami lub ich odpowiednikami w polskim lub europejskim układzie normalizacji:
28. PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT;
29. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji;
30. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania;
31. ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej;
32. ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej.
	1. CPD dostawcy usług chmury obliczeniowej spełnia wymagania normy PN-EN 50600 minimum klasy 3 lub ANSI/TIA-942 minimum Tier III, lub innego normatywu odpowiedniego i powszechnie uznanego do oceny CPD.
	2. CPD zlokalizowane jest na terytorium państwa Europejskiego Obszaru Gospodarczego. Punkt ten stosuje się z zastrzeżeniem, że podmioty nadzorowane, które:
	3. 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
	4. 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.

* 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. brak konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego i/lub w innych uruchamianych usługach;
3. zasadę „minimum koniecznego” dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez podmiot nadzorowany oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. Obowiązujące w tym zakresie procedury obsługi mogą być dodatkowo potwierdzone stosownym certyfikatem (np. SOC[[7]](#footnote-8) 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. natywne uruchamianie nowego środowiska (i/lub usługi) separowanego od innych tenantów, z ustawieniami „secure-by-default”.
	1. Spełnienie wymagań może być poświadczone odpowiednim certyfikatem zgodności wystawionym przez niezależną jednostkę certyfikującą, akredytowaną w polskim lub europejskim systemie akredytacji.
6. **Kryptografia**
	1. Podmiot nadzorowany powinien zapewnić, że informacje przetwarzane w chmurze obliczeniowej są szyfrowane. W szczególności podmiot nadzorowany powinien upewnić się, że:
7. posiada dostęp do szczegółowych i aktualnych instrukcji konfiguracji usług oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji;
8. zapewnia dostateczne kompetencje w celu realizacji poprawnej konfiguracji usług, zgodnie z wytycznymi dostawcy usług chmury obliczeniowej, w tym pod kątem stosowania szyfrowania przetwarzanych informacji;
9. używa dedykowanych i/lub zalecanych przez dostawcę ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług, w szczególności w zakresie szyfrowania przetwarzanych informacji;
10. informacje prawnie chronione przetwarzane w chmurze obliczeniowej są szyfrowane zarówno „at rest” jak i „in transit”.
	1. Podmiot nadzorowany powinien zapewnić, że informacje są szyfrowane kluczami generowanymi i/lub dostarczonymi oraz zarządzanymi przez podmiot nadzorowany, chyba że z oszacowania ryzyka wynika, iż dopuszczalne lub wskazane jest używanie kluczy szyfrujących dostarczonych i/lub zarządzanych przez dostawcę usług chmury obliczeniowej.
	2. Podmiot nadzorowany zapewnia, że używane algorytmy szyfrowania nie są powszechnie uważane za skompromitowane.
	3. W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM), to HSM mogą być udostępniane przez dostawcę usług chmurowych, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS[[8]](#footnote-9) 140-2 Level 2 lub równoważne.
	4. Podmiot nadzorowany w udokumentowanym procesie zarządza tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz kontrolą tego procesu.
11. **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 ilości logowanych zdarzeń oraz architektury bezpieczeństwa – nadzór zaleca używanie specjalistycznego oprogramowania do korelowania zapisów ze zdarzeń (SIEM) oraz regularny przegląd i aktualizację reguł korelacji.
	4. Wymagania w stosunku do podmiotu nadzorowanego w zakresie zarządzania dostawcami usług mającymi dostęp zdalny do środowiska chmury obliczeniowej podmiotu nadzorowanego[[9]](#footnote-10):
12. podmiot nadzorowany zapewnia, że wyłącznie uprawniony personel dostawcy usług ma dostęp do wskazanych systemów teleinformatycznych i/lub ich wybranych zakresów;
13. podmiot nadzorowany wymusza używanie przez personel dostawcy usług uwierzytelnienia MFA, przy czym rodzaj i zakres uzależniony jest od wyników szacowania ryzyka;
14. podmiot nadzorowany zapewnia, że dostęp administracyjny lub o charakterze uprzywilejowanym realizowany jest wyłącznie z zaufanych sieci podmiotu nadzorowanego i pod jego 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 brak takiej potrzeby.
15. **Dokumentowanie działań podmiotu nadzorowanego**
	1. 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 co najmniej:
16. organizację służb odpowiedzialnych za cyberbezpieczeństwo, w tym stanowisk i/lub funkcji związanych z monitorowaniem, analizowaniem i raportowaniem incydentów związanych z zasobami przetwarzanymi w chmurze obliczeniowej, wraz z opisanymi wymaganymi kompetencjami, uprawnieniami i odpowiedzialnościami;
17. 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;
18. zasady kategoryzacji informacji i/lub systemów pod kątem przetwarzania w chmurze obliczeniowej;
19. zasady stosowanych zabezpieczeń technologicznych i rozwiązań organizacyjnych;
20. zasady zarządzania ciągłością działania;
21. zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z dostawcą usług chmury obliczeniowej;
22. zasady zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi;
23. zasady przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem chmury obliczeniowej;
24. zasady raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej;
25. umowy z dostawcami usług chmury obliczeniowej wraz z dodatkowymi oświadczeniami jeżeli to konieczne dla potwierdzenia spełnienia wymagań;
26. procesy, procedury i/lub instrukcje dotyczące:
	1. analizy zagrożeń i oceny ryzyka, w tym źródła pozyskiwania informacji o zagrożeniach specyficznych dla stosowanych rozwiązań chmury obliczeniowej oraz sektora finansowego;
	2. zarządzania środowiskiem teleinformatycznym (sieciami, systemami, aplikacjami, bazami danych, itp.), z uwzględnieniem zasobów chmury obliczeniowej, w tym planowanie, rozwój i utrzymywanie;
	3. zarządzania logami;
	4. zarządzania kluczami szyfrującymi;
	5. zarządzania incydentami bezpieczeństwa;
	6. przeprowadzania audytów wewnętrznych bezpieczeństwa środowiska teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej;
	7. zarządzania dostawcami produktów i usług teleinformatycznych.
	8. Dokumentacja jest chroniona przed nieuprawnionym dostępem, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem. Zasady zarządzania dokumentacją podmiot nadzorowany definiuje w ramach systemu zarządzania organizacją.
27. **Zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej**
28. W przypadkach określonych w niniejszym komunikacie podmiot nadzorowany w terminie 14 dni[[10]](#footnote-11) przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej (a w przypadku, gdy przetwarzanie to już jest realizowane – w terminie 90 dni od wejścia w życie postanowień niniejszego komunikatu) 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;
	3. dacie podpisania umowy z dostawcą usług chmury obliczeniowej oraz terminach jej obowiązywania;
	4. lokalizacji (kraj, region) centrum przetwarzania danych (CPD) świadczącym usługę;
	5. spełnieniu wymagań opisanych w niniejszym komunikacie;
	6. osobach do kontaktu w sprawie stosowania chmury obliczeniowej w podmiocie nadzorowanym.
29. Powyższa informacja powinna zostać podpisana przez ustawowego przedstawiciela podmiotu nadzorowanego oraz dostarczona do UKNF przy wykorzystaniu formularza stanowiącego załącznik nr 1 do niniejszego komunikatu.

Załącznik nr 1

do komunikatu UKNF dotyczącego

przetwarzania informacji w chmurze obliczeniowej

Informacja podmiotu nadzorowanego w sprawie

przetwarzania informacji w chmurze obliczeniowej

|  |  |
| --- | --- |
| Oznaczenie podmiotu nadzorowanego (nazwa, adres, NIP, REGON) |  |

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

|  |  |
| --- | --- |
| Rodzaj i zakres przetwarzanych informacji: |  |
| Nazwa i adres dostawcy usług chmury obliczeniowej: |  |
| Nazwy usług chmury obliczeniowej lub ich rodzaj: |  |
| Lokalizacje CPD przetwarzanych informacji (państwo, region): |  |
| Data podpisania umowy z dostawcą usług chmury obliczeniowej: |  |
| Okres na jaki została zawarta umowa z dostawcą usług chmury obliczeniowej:  |  |
| Osoby do kontaktu w sprawie stosowania chmury obliczeniowej w podmiocie nadzorowanym (imię, nazwisko, stanowisko, nr telefonu, adres e-mail): |  |

Oświadczamy, że postanowienia *Komunikatu UKNF dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej o charakterze publicznym lub hybrydowym* zostały spełnione i skutecznie wdrożone.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Miejscowość, data Podpisy osób reprezentujących podmiot nadzorowany

1. National Institute of Standards and Technology, Definition of Cloud Computing, Special Publication 800-145. [↑](#footnote-ref-2)
2. Tamże. [↑](#footnote-ref-3)
3. Szacowanie ryzyka powinno 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-4)
4. Okresowa weryfikacja i aktualizacja powinna być prowadzona zgodnie z praktyką i zasadami podmiotu nadzorowanego, jednak nie rzadziej niż raz w roku. [↑](#footnote-ref-5)
5. Precyzyjne wskazanie lokalizacji centrum przetwarzania danych (CPD) może rodzić zagrożenie dla bezpieczeństwa fizycznego przetwarzanych informacji, jednak jako minimum należy operować pojęciami „strefa dostępu”, „region” lub innymi równoważnymi, z podaniem co najmniej kraju oraz przybliżonej lokalizacji CPD, którymi dostawca usług chmury obliczeniowej posługuje się w standardowej komunikacji, np. podając miejscowość lub region kraju. W sytuacji gdy takie określenie nie jest możliwe lub – z uwagi na skalę działania i liczbę miejsc przetwarzania informacji – jest niezasadne, należy podać obszar EOG (dla Europejskiego Obszaru Gospodarczego). [↑](#footnote-ref-6)
6. Wymagania te uwzględnia podmiot nadzorowany w swoim podejściu do stosowania usług chmury obliczeniowej, a w szczególności w procesie szacowania ryzyka. [↑](#footnote-ref-7)
7. System and Organization Controls. [↑](#footnote-ref-8)
8. Federal Information Processing Standard – publiczne standardy dla agencji cywilnych i rządowych w USA. W tym przypadku międzynarodowy standard bezpieczeństwa dla systemów kryptograficznych. [↑](#footnote-ref-9)
9. Wymagania te dotyczą sytuacji, w której podmiot nadzorowany zleca swojemu dostawcy usług teleinformatycznych wykonanie działań na zasobach podmiotu nadzorowanego umieszczonych w chmurze obliczeniowej (np. aktualizacja oprogramowania, prace serwisowe, itp.). 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-10)
10. Chyba że szczególny przepis prawa dotyczący działalności podmiotu nadzorowanego przewiduje inny termin przekazania informacji. [↑](#footnote-ref-11)