

Warszawa, 23 stycznia 2020 r.

Komunikat Urzędu Komisji Nadzoru Finansowego
dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej
publicznej lub hybrydowej

I. Definicje

1. Używane pojęcia przyjęto wyłącznie na potrzeby niniejszego komunikatu, uwzględniając specyfikę przetwarzania informacji w chmurze obliczeniowej:
 - 1) **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);
 - 2) **informacja prawnie chroniona** – informacja związana z tajemnicami sektora finansowego wymienionymi w ustawach sektorowych, tj.:
 - a) ustawa z 29 sierpnia 1997 r. Prawo bankowe;
 - b) ustawa z 29 lipca 2005 r. o obrocie instrumentami finansowymi;
 - c) ustawa z 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi;
 - d) ustawa z 26 października 2000 r. o giełdach towarowych;
 - e) ustawa z 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej;
 - f) ustawa z 15 grudnia 2017 r. o dystrybucji ubezpieczeń;
 - g) ustawa z 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych;
 - h) ustawa z 4 października 2018 r. o pracowniczych planach kapitałowych;
 - i) ustawa z 19 sierpnia 2011 r. o usługach płatniczych;
 - j) ustawa z 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych;
 - 3) **chmura obliczeniowa** – pula współdzielonych, dostępnych „na żądanie” przez sieci teleinformatyczne, konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowych, aplikacji, usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale ich dostawcy¹;
 - 4) **chmura obliczeniowa publiczna** – chmura obliczeniowa dostępna do użytku publicznego, będąca w posiadaniu lub bezpośrednio zarządzana przez dostawcę usług chmury obliczeniowej;

¹ National Institute of Standards and Technology, Definition of Cloud Computing, Special Publication 800-145.

- 5) **chmura obliczeniowa prywatna** – chmura obliczeniowa dostępna do wyłącznego użytku jednego podmiotu, będąca w posiadaniu lub bezpośrednio zarządzana przez ten podmiot;
- 6) **chmura obliczeniowa hybrydowa** – chmura obliczeniowa składająca się z połączenia dwóch lub więcej osobnych chmur obliczeniowych (publicznej, prywatnej, społecznościowej), która poprzez standaryzację użycia lub odpowiednią technologię pozwala na przenoszenie czynności przetwarzania informacji pomiędzy chmurami obliczeniowymi, które ją tworzą;
- 7) **chmura obliczeniowa społecznościowa** – chmura obliczeniowa dostępna do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy o współpracy, ze zdefiniowanymi wspólnymi wymaganiami i zasadami m.in. w obszarze zgodności i bezpieczeństwa przetwarzania informacji, będąca w posiadaniu lub bezpośrednio zarządzana przez podmiot(y) z grupy lub na jego (ich) zlecenie;
- 8) **dostawca usług chmury obliczeniowej** – podmiot, który dysponuje infrastrukturą i oprogramowaniem służącym do świadczenia usług chmury obliczeniowej oraz świadczy usługi chmury obliczeniowej;
- 9) **usługa chmury obliczeniowej** – gotowe do użycia, wystandaryzowane zasoby chmury obliczeniowej służące przetwarzaniu informacji, wstępnie skonfigurowane przez dostawcę usług chmury obliczeniowej i przez niego dostarczane; mogą być bezpośrednio dostarczane podmiotowi nadzorowanemu lub stanowić element usług innego dostawcy na różnym poziomie łańcucha outsourcingowego;
- 10) **outsourcing chmury obliczeniowej** – oznacza umowę zawartą w dowolnej formie między podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej, na mocy której dostawca usług chmury obliczeniowej dostarcza podmiotowi nadzorowanemu usługę chmury obliczeniowej, która służy do wsparcia realizacji procesu, usługi lub zadania, które podmiot nadzorowany realizowałby samodzielnie, gdyby usługa chmury obliczeniowej była niedostępna;
- 11) **outsourcing szczególny chmury obliczeniowej** – 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:
 - a) wpływałyby w sposób istotny na ciągłość wypełniania przez podmiot nadzorowany warunków stanowiących podstawę uprawnienia prowadzenia działalności nadzorowanej lub jej wykonywania lub

- b) zagrażałaby w sposób istotny wynikom finansowym podmiotu nadzorowanego, niezawodności lub ciągłości wykonywania działalności nadzorowanej;
- 12) **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 wykazanie wykonania czynności zgodnie z wymaganiami;
- 13) **wartość informacji** – konsekwencja dla działalności podmiotu nadzorowanego materializacji ryzyka polegającego na nieuprawnionym ujawnieniu, zmianie lub zniszczeniu informacji;
- 14) **szyfrowanie „at rest”** – szyfrowanie informacji „w spoczynku” (np. przechowywanych kopii zapasowych, informacji w bazie danych, systemów plików);
- 15) **szyfrowanie „in transit”** – szyfrowanie w trakcie transmisji informacji (np. podczas przesyłania informacji z/do chmury obliczeniowej);
- 16) **łańcuch outsourcingowy** – relacja polegająca na:
- a) powierzeniu przez dostawcę usług chmury obliczeniowej części czynności (służących dostarczaniu usługi chmury obliczeniowej dla podmiotu nadzorowanego) swojemu poddostawcy i dalszym (kolejnym) poddostawcom lub
 - b) relacja polegająca na dostarczaniu przez dostawcę usług chmury obliczeniowej usługi chmury obliczeniowej innemu dostawcy, który wykorzystuje usługę chmury obliczeniowej do świadczenia własnej usługi dla podmiotu nadzorowanego;
- 17) **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;
- 18) **SLA** – Service Level Agreement, umowa o gwarantowanym poziomie świadczenia usługi chmury obliczeniowej;
- 19) **tenant** – instancja usług chmury obliczeniowej przypisanych do podmiotu nadzorowanego. Najważniejszą właściwością tenantu jest jego domyślna, logiczna separacja (konfiguracji oraz przetwarzanych informacji) od innych tenantów. Każdy podmiot nadzorowany może posiadać wiele tenantów u tego samego dostawcy usług chmury obliczeniowej, jednak wszystkie wymagania związane z separacją tenantów muszą być zachowane;

- 20) **MFA** – Multi Factor Authentication, metoda wieloskładnikowego uwierzytelniania;
- 21) **CPD** – centrum przetwarzania danych;
- 22) **SIEM** – Security Information and Event Management, system do zarządzania informacją i zdarzeniami bezpieczeństwa;
- 23) **ujawnienie informacji** – bez uszczerbku dla rozumienia przepisów prawa bezwzględnie obowiązujących, oznacza sytuację, podczas której informacje są przetwarzane w chmurze obliczeniowej:
- a) w sposób nieszyfrowany albo
 - b) w sposób zaszyfrowany „at rest” lub „in transit”, ale dostęp do kluczy szyfrujących i szyfrowanej tymi kluczami informacji posiada albo może posiadać dostawca usług chmury obliczeniowej lub jego poddostawca w łańcuchu outsourcingowym.

II. Wprowadzenie

1. Postęp technologiczny w obszarze chmury obliczeniowej powoduje wątpliwości ze strony podmiotów nadzorowanych w zakresie możliwości stosowania tej technologii oraz – w przypadku dopuszczalności takiego rozwiązania – zasad dokonywania outsourcingu, w szczególności podczas przetwarzania informacji prawnie chronionych.
2. Urząd Komisji Nadzoru Finansowego (dalej: UKNF lub Nadzór) 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.
3. 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 chmury obliczeniowej lub outsourcing szczególny chmury obliczeniowej. Niniejszy komunikat nie wyłącza przepisów bezwzględnie obowiązujących w tym zakresie, natomiast celem jest zaprezentowanie, jak Nadzór rozumie te przepisy.
4. Nadzór uznaje ochronę przetwarzania informacji istotnych dla procesów lub działalności podmiotu nadzorowanego lub stanowiących informacje prawnie chronione za zagadnienie o charakterze priorytetowym. Stosowanie nieodpowiednich reżimów prawnych w tym zakresie może wywołać negatywne konsekwencje dla funkcjonowania rynku finansowego oraz wpływa na możliwość wykonywania efektywnego nadzoru nad procesami przetwarzania informacji. Obowiązujące na terenie Europejskiego Obszaru Gospodarczego (EOG) regulacje w tym zakresie, a w szczególności:
 - 1) 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) oraz
 - 2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiejrealizują szereg postulatów i celów związanych z odpowiednią ochroną informacji. Mając na uwadze powyższe okoliczności UKNF rekomenduje przetwarzanie informacji w CPD zlokalizowanych na terenie państw należących do EOG.
5. Niniejszy komunikat jest uzupełnieniem i uszczegółowieniem wybranych zaleceń w zakresie outsourcingu opisanych w:
 - 1) rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach;
 - 2) rekomendacji D-SKOK dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych;
 - 3) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych;

- 4) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji;
- 5) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych;
- 6) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w podmiotach infrastruktury rynku kapitałowego;
- 7) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych.

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

6. Niniejszy komunikat jest podejściem krajowym do outsourcingu przetwarzania informacji w chmurze obliczeniowej dla sektora finansowego (model referencyjny). Tym samym:
 - 1) 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;
 - 2) podmioty nadzorowane, które realizują przetwarzanie informacji w chmurze obliczeniowej w oparciu o wymagania komunikatu UKNF z 23 października 2017 r. powinny dostosować swoje działanie do wymagań niniejszego komunikatu do 1 sierpnia 2020 r.;
 - 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 do przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej, nie mają zastosowania do podmiotów nadzorowanych w tym zakresie.
7. 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) lub w ramach współpracy podmiotów nadzorowanych z ograniczoną liczbą dostawców usług chmury obliczeniowej. Dodatkowo przetwarzanie informacji prawnie chronionych w chmurze obliczeniowej generuje ryzyka związane z ochroną przetwarzanych informacji, niezależnie od charakteru procesu outsourcingowego. Z uwagi na te ryzyka Nadzór oczekuje, że podmioty nadzorowane będą informowały UKNF o zamiarze przetwarzania informacji w usługach chmury obliczeniowej, na zasadach określonych w niniejszym komunikacie.

III. Model referencyjny

1. 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:
 - 1) wytyczne stosowania;
 - 2) wytyczne do klasyfikacji i oceny informacji;
 - 3) wytyczne do szacowania ryzyka;
 - 4) minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej;
 - 5) zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej.

IV. Wytyczne stosowania

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

Matryca stosowania komunikatu		Outsourcing chmury obliczeniowej	
		inny niż szczególny	szczególny
Informacje	inne niż prawnie chronione	Komunikat może być stosowany.	Komunikat powinien być stosowany.
	prawnie chronione	Komunikat powinien być stosowany.	

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

V. Wytyczne do klasyfikacji i oceny informacji

1. Podmiot nadzorowany przeprowadza w udokumentowanym procesie klasyfikację:
 - 1) informacji prawnie chronionych w rozumieniu niniejszego komunikatu;
 - 2) informacji, których ochrona wynika z uregulowań prawnych nieuwzględnionych w niniejszym komunikacie;
 - 3) informacji, które nie podlegają ochronie prawnej.
2. Ocena informacji przeprowadzona jest pod kątem dopuszczalności ich przetwarzania w chmurze obliczeniowej, w szczególności biorąc pod uwagę:
 - 1) zgodność z wymaganiami prawa oraz specyficznymi dla danego sektora lub podmiotu nadzorowanego postanowieniami oraz zobowiązaniami umownymi;
 - 2) zakres klasyfikowanych informacji, ich rodzaj i ważność;
 - 3) wartość informacji dla podmiotu nadzorowanego.
3. Podmiot nadzorowany w procesie klasyfikacji i oceny informacji uwzględnia:
 - 1) skalę prowadzonej działalności;
 - 2) korporacyjne, grupowe lub inne modele lub metody oceny i klasyfikacji, które uwzględniają powyższe założenia i są wspólne dla grupy podmiotów, do których zalicza się podmiot nadzorowany;
 - 3) odpowiedzialność podmiotu nadzorowanego za przetwarzane informacje.

4. Podmiot nadzorowany powinien przeprowadzić klasyfikację i ocenę informacji ponownie, gdy:
 - 1) zamierza przetwarzać nowy rodzaj informacji;
 - 2) zamierza wykorzystać nową usługę chmury obliczeniowej;
 - 3) zmiana prawa, regulacji, regulaminów lub postanowień umów, których stroną jest podmiot nadzorowany, wpływa albo może wpływać na zgodność postępowania podmiotu nadzorowanego w kontekście przetwarzania informacji w chmurze obliczeniowej;
 - 4) istotnie zwiększa się albo zmniejsza skala przetwarzania;
 - 5) istotnie zwiększa się wartość przetwarzanych informacji.
5. Podmiot nadzorowany powinien regularnie (lecz nie rzadziej niż raz w roku) przeglądać i potwierdzać aktualność stosowanej klasyfikacji i oceny informacji do bieżących warunków swojego działania.

VI. Wytyczne do szacowania ryzyka

1. Podmiot nadzorowany prowadzi w udokumentowanym procesie kompleksowe szacowanie ryzyka (identyfikację, analizę oraz ocenę zagrożeń, możliwość ich wystąpienia oraz wpływ tego wystąpienia na podmiot nadzorowany), zgodnie z wymaganiami aktualnego wydania normy PN-ISO 27005 (Zarządzanie ryzykiem w bezpieczeństwie informacji) lub jej odpowiednika w europejskim systemie normalizacji, lub na bazie innego, usystematyzowanego podejścia². Szacowanie ryzyka jest prowadzone w sposób ciągły, z uwzględnieniem praktycznej implementacji zasady PDCA („plan – do – check – act”).
2. Podmiot nadzorowany uwzględnia w procesie szacowania ryzyka, w kontekście wyników przeprowadzonej klasyfikacji i oceny przetwarzanych informacji w chmurze obliczeniowej, co najmniej:
 - 1) ogólne zagrożenia dla stosowania chmury obliczeniowej:
 - a) rozproszenie geograficzne przetwarzanych informacji, w szczególności w kontekście zapewnienia zgodności procesu przetwarzania informacji z przepisami prawa, regulacjami wewnętrznymi, zobowiązaniami umownymi oraz deklaracjami i innymi uregulowaniami;
 - b) możliwość utraty zgodności postępowania podmiotu nadzorowanego z przepisami prawa (w tym wydanych licencji lub zezwoleń) poprzez korzystanie z usług chmury obliczeniowej w sposób niezamierzony albo inny niż zamierzony;
 - c) dostęp do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) dostawcy usług chmury obliczeniowej;
 - d) dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się fizycznie przetwarzanie (lokalizacja centrum przetwarzania danych), w szczególności odniesienie do katalogu sytuacji (lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu

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

- nadzorowanego, zarówno przez organy administracji krajowej jak i międzynarodowej;
- e) brak zgodności technologicznej pomiędzy usługami różnych dostawców chmury obliczeniowej powodujące przywiązanie do jednego dostawcy usług chmury obliczeniowej poprzez ograniczenie albo brak możliwości przenoszenia (korzystania z identycznych) usług lub przetwarzanych informacji (vendor lock-in);
 - f) awarie mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej;
 - g) podatność interfejsów zarządzających usługami, które są udostępniane przez dostawców usług chmury obliczeniowej;
 - h) ograniczona możliwość wpływania na zakres, kształt i zmiany usług, w tym w szczególności na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług przetwarzania;
 - i) ograniczona możliwość kontrolowania dostawcy usług chmury obliczeniowej oraz jego poddostawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej;
 - j) podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy dostawcą usług chmury obliczeniowej a podmiot nadzorowany;
- 2) specyficzne zagrożenia dla stosowanych konkretnych (nazwanych) usług chmury obliczeniowej:
- a) możliwości korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego lub w środowisku, które nie podlega kontroli podmiotu nadzorowanego (np. prywatne urządzenia mobilne, dostęp z prywatnych lub publicznych sieci);
 - b) możliwości jednostronnej zmiany warunków technicznych korzystania z usługi (w szczególności jej parametrów lub zasad konfiguracji);
 - c) stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług, bez ich należytej weryfikacji i oceny adekwatności dla potrzeb podmiotu nadzorowanego;
 - d) stosowane mechanizmy uwierzytelniania oraz ich słabości;
- 3) specyficzne zagrożenia związane z zasobami podmiotu nadzorowanego:
- a) wymagane i posiadane zasoby, w tym zasoby ludzkie o ustalonych kompetencjach;
 - b) zgodność technologiczna posiadanego środowiska teleinformatycznego oraz środowiska chmury obliczeniowej, a w szczególności mechanizmy integracji;
- 4) wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem;
- 5) stanowisko nadzoru w sprawie szyfrowania informacji, zgodnie z którym:
- a) szyfrowanie informacji nie zmniejsza ważności informacji, nie zmienia też jej klasyfikacji i oceny;
 - b) szyfrowanie informacji oraz właściwe zarządzanie kluczami szyfrującymi zapobiega ujawnieniu informacji;
 - c) brak jest gwarancji dla uznania danego algorytmu szyfrowania za „całkowicie bezpieczny”. Nadzór zaleca używanie algorytmów szyfrowania, które – bazując na dostępnych publicznie informacjach (np.

- opracowaniach merytorycznych, raportach jednostek zajmujących się cyberbezpieczeństwem lub kryptografią) – nie są uznane za skompromitowane. W przypadku używania algorytmu uznanego za skompromitowany, podmiot nadzorowany powinien niezwłocznie podjąć działania w celu zapewnienia bezpieczeństwa przetwarzanych informacji;
- d) informacje przetwarzane w chmurze obliczeniowej powinny być szyfrowane zawsze, gdy to jest technologicznie możliwe i – w ocenie podmiotu nadzorowanego – ekonomicznie zasadne;
 - e) informacje prawnie chronione muszą być szyfrowane zawsze „at rest” oraz „in transit”. Nadzór dopuszcza sytuację, w której informacje prawnie chronione są szyfrowane „at rest” natychmiast po ich przesłaniu do chmury obliczeniowej przy założeniu jednoczesnego stosowania szyfrowania „in transit” i nie traktuje takiej sytuacji jako ujawnienia przetwarzanych informacji;
 - f) Nadzór dopuszcza sytuację, w której podmiot nadzorowany powierza swojemu dostawcy usług (w tym dostawcy usług chmury obliczeniowej) generowanie lub zarządzanie kluczami szyfrującymi, które są używane do szyfrowania informacji przetwarzanej w usługach chmury obliczeniowej innego dostawcy usług chmury obliczeniowej, przy czym podmiot nadzorowany powinien w procesie szacowania ryzyka uwzględnić możliwość utraty swojego dostępu do kluczy szyfrujących;
- 6) stanowisko nadzoru w sprawie tworzenia łańcucha outsourcingowego, zgodnie z którym:
- a) tworzenie łańcucha outsourcingowego powinno być każdorazowo oceniane przez podmiot nadzorowany z perspektywy przepisów szczególnych prawa dotyczących konkretnie realizowanych czynności przetwarzania informacji w chmurze obliczeniowej, a w szczególności:
 - i. tworzenie łańcucha outsourcingowego w zakresie działalności nadzorowanej jest dopuszczalne wyłącznie w granicach przewidzianych przepisami prawa;
 - ii. tworzenie łańcucha outsourcingowego w zakresie innym niż w zakresie działalności nadzorowanej jest dopuszczalne, o ile nie jest wprost zakazane przez przepisy prawa lub postanowienia umowne;
 - b) zakres odpowiedzialności dostawcy usług chmury obliczeniowej oraz jego poddostawców wobec podmiotu nadzorowanego może ulegać ograniczeniu albo wyłączeniu wyłącznie w granicach szczególnych przepisów prawa regulujących działalność podmiotu nadzorowanego, przy czym Nadzór krytycznie ocenia takie wyłączenia albo ograniczenia, jeżeli:
 - i. w ramach usługi chmury obliczeniowej przetwarzane są informacje prawnie chronione szyfrowane za pomocą kluczy szyfrujących dostarczonych lub zarządzanych przez dostawcę usług chmury obliczeniowej lub jego poddostawcę lub
 - ii. przetwarzanie ma charakter outsourcingu szczególnego chmury obliczeniowej;
- 7) stanowisko nadzoru w sprawie usług (dostawców usług chmury obliczeniowej), które są wykorzystywane do świadczenia własnych usług przez bezpośrednich dostawców podmiotów nadzorowanych, zgodnie z którym:

- a) podmiot nadzorowany powinien upewnić się, w jakim zakresie świadczona przez bezpośredniego dostawcę usług wykorzystuje usługi chmury obliczeniowej, a w szczególności czy dochodzi do przetwarzania informacji prawnie chronionej w usłudze chmury obliczeniowej;
 - b) zależnie od faktycznego wykorzystania usług chmury obliczeniowej oraz zakresu przetwarzanych informacji podmiot nadzorowany powinien zapewnić, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień niniejszego komunikatu;
 - 8) stanowisko nadzoru w sprawie prawa właściwego umowy pomiędzy dostawcą usług chmury obliczeniowej a podmiotem nadzorowanym, zgodnie z którym:
 - a) prawem właściwym dla umowy jest prawo polskie lub prawo innego państwa członkowskiego Unii Europejskiej, chyba że strony umowy poddadzą umowę prawu państwa trzeciego, a prawo państwa trzeciego pozwala na skuteczne wykonywanie:
 - i. postanowień umowy;
 - ii. wszystkich wymogów prawa polskiego ciążących na podmiocie nadzorowanym;
 - iii. wytycznych organu nadzoru, w tym również w zakresie niniejszego komunikatu;
 - b) w przypadku poddania umowy prawu państwa trzeciego podmiot nadzorowany powinien posiadać pisemną opinię prawną potwierdzającą, że zgodnie z wybranym prawem właściwym umowy wszystkie postanowienia umowy pomiędzy podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej spełniają wymagania prawa obowiązujące podmiot nadzorowany oraz wymagania niniejszego komunikatu;
 - 9) inne istotne zagrożenia, które podmiot nadzorowany identyfikuje w związku z wykorzystywaniem usług chmury obliczeniowej.
3. Podmiot nadzorowany w procesie szacowania ryzyka powinien uwzględnić potencjalną możliwość:
- 1) korzystania ze zweryfikowanych, aktualizowanych źródeł informacji o zagrożeniach specyficznych dla stosowania usług chmury obliczeniowej, w tym również w odniesieniu do konkretnych (nazwanych) usług;
 - 2) korzystania z pomocy ze strony podmiotów lub osób o specjalistycznych kompetencjach zarówno w obszarze cyberbezpieczeństwa jak i usług chmury obliczeniowej, szczególnie w sytuacji braku takich kompetencji wewnątrz własnej organizacji podmiotu nadzorowanego;
 - 3) przeanalizowania dostępnych wyników audytów zewnętrznych dostawców usług chmury obliczeniowej w odniesieniu do usług chmury obliczeniowej oraz procesu zarządzania bezpieczeństwem informacji, poszerzając zakres analizy o dostępne certyfikaty wystawione dostawcy usług chmury obliczeniowej potwierdzające spełnienie wymagań;
 - 4) uprzedniego testowania usług chmury obliczeniowej, także przy wykorzystaniu scenariuszy warunków skrajnych, zarówno w zakresie sposobu działania usługi jak i jej konfiguracji.

4. Podmiot nadzorowany, na podstawie wyników szacowania ryzyka, zarządza tym ryzykiem, uwzględniając w szczególności:
 - 1) wymagania przepisów prawa, regulacji wewnętrznych oraz postanowień umownych;
 - 2) stopień złożoności organizacyjnej, podział uprawnień i odpowiedzialności podmiotu nadzorowanego, zawarte porozumienia, oraz analogiczne czynniki występujące w grupie kapitałowej lub organizacji grupowej, lub o charakterze stowarzyszenia, do których podmiot nadzorowany należy;
 - 3) efektywność stosowanych mechanizmów kontrolnych i monitorujących, zwłaszcza w odniesieniu do:
 - a) identyfikacji nowych zagrożeń;
 - b) zmian w wykorzystywanej usłudze chmury obliczeniowej lub trybie i zakresie jej wykorzystywania;
 - c) zmian w relacji z dostawcą usług chmury obliczeniowej, w tym możliwość również nieplanowanego zakończenia współpracy zarówno przez podmiot nadzorowany jak i dostawcę usług chmury obliczeniowej;
 - 4) kompetencje techniczne i zdolności organizacyjne podmiotu nadzorowanego, w szczególności w kontekście bezpiecznego wykorzystywania usług chmury obliczeniowej oraz realizacji postanowień umownych;
 - 5) zdolność podmiotu nadzorowanego i zgodność z przepisami prawa do transferowania zidentyfikowanego ryzyka lub akceptacji oszacowanego poziomu ryzyka.
5. Wyniki szacowania ryzyka powinny dawać podstawę do twierdzenia, że świadczenie usługi chmury obliczeniowej będzie realizowane zgodnie z wymaganiami prawa obowiązującymi podmiot nadzorowany, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez podmiot nadzorowany standardami.
6. Wyniki szacowania ryzyka powinny zostać formalnie zatwierdzone oraz podlegać okresowej weryfikacji i aktualizacji³. 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.

VII. Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej

1. Niniejsze minimalne wymagania techniczne i organizacyjne dla przetwarzania informacji w chmurze obliczeniowej stanowią referencyjne odniesienie, które podmiot nadzorowany powinien weryfikować pod kątem adekwatności do wyników oszacowania ryzyka oraz zapewnić ich spełnienie.
2. Środki techniczne i zasoby organizacyjne służące bezpieczeństwu przetwarzanych informacji powinny wynikać z przeprowadzonego procesu szacowania ryzyka, jednak – niezależnie od wyników tego szacowania – nie mogą osłabiać wymagań opisanych poniżej.

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

3. Zapewnienie kompetencji

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

4. Umowa z dostawcą usług chmury obliczeniowej

- 4.1. Podmiot nadzorowany posiada sformalizowaną umowę (oraz inne dokumenty, w tym oświadczenia, regulaminy, warunki korzystania z usług, także w wersji elektronicznej) z dostawcą usług chmury obliczeniowej, która – tam, gdzie to zasadne w odniesieniu do używanych usług i zakresu przetwarzanych informacji – zawiera lub wskazuje źródła informacji, obejmujące:
 - a) klarowny podział odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji, z uwzględnieniem modelu świadczenia usług, ciągłości działania usług (z uwzględnieniem parametrów RTO i RPO⁴ tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;

⁴ RTO – Recovery Time Objective, czas od momentu awarii systemu teleinformatycznego do momentu przywrócenia jego normalnego działania.

RPO – Recovery Point Objective, maksymalny czas pomiędzy wykonaniem kopii zapasowej informacji a momentem wystąpienia awarii usługi chmury obliczeniowej. Oznacza również potencjalną i akceptowaną przez podmiot nadzorowany możliwość utraty wyników przetwarzania informacji przez wskazany czas.

- b) klarowną definicję i wskazanie lokalizacji⁵ przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;
- c) prawo właściwe dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów);
- d) potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;
- e) własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu (wygaśnięciu, rozwiązaniu), także w sposób nieplanowany;
- f) gwarancje, rękojmię, ubezpieczenia (polisy ubezpieczeniowe dostawcy usług chmury obliczeniowej), kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej oraz zasad postępowania w takich sytuacjach, o ile ma to zastosowanie;
- g) określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie), zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;
- h) klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) dostawcy usług chmury obliczeniowej oraz warunki nadawania praw dostępu do informacji przetwarzanych przez podmiot nadzorowany;
- i) klarowne wskazanie zasad, zgodnie z którymi zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań poddostawców dostawcy usług chmury obliczeniowej są transparentne i jasno identyfikowane przez podmiot nadzorowany;
- j) źródła autoryzowanych informacji o planowanych zmianach w standardach świadczonych usług chmury obliczeniowej (w tym zmianach o charakterze technicznym);
- k) źródła dokumentacji technicznej i deklaracji zgodności (w tym zgodności z obowiązującymi przepisami prawa), wraz z instrukcjami dotyczącymi konfiguracji usług chmury obliczeniowej;
- l) zakres dodatkowych informacji i dokumentacji przekazywanych przez dostawcę usług chmury obliczeniowej w związku ze świadczeniem usług chmury obliczeniowej;
- m) prawo podmiotu nadzorowanego do przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji, w tym prawo do przeprowadzenia audytu 2-giej lub 3-ciej strony na zlecenie podmiotu nadzorowanego (o ile taka potrzeba wynika z szacowania ryzyka);
- n) prawo dla nadzoru do wykonania obowiązków kontrolnych, w tym kontroli pomieszczeń i dokumentacji związanej z przetwarzaniem informacji podmiotu nadzorowanego, procesów i procedur, organizacji i zarządzania oraz potwierdzeń zgodności;

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

- o) zasady licencjonowania (w tym prawo do aktualizacji bezpieczeństwa używanego oprogramowania lub jego komponentów) oraz prawa własności intelektualnej, w tym – jeżeli dotyczą – prawo do dysponowania przetwarzanymi informacjami;
 - p) zasady zmiany treści umowy, w tym parametrów technicznych używanych usług chmury obliczeniowej;
 - q) zasady rozwiązywania umowy, w tym zasady i terminy zwrotu lub usunięcia przetwarzanych informacji;
 - r) zasady wsparcia, w tym zakres i okna czasowe (z uwzględnieniem stref czasowych), tryb i sposób zgłaszania problemów z usługami chmury obliczeniowej;
 - s) zasady wymiany informacji, w tym w szczególności w zakresie bezpieczeństwa oraz zarządzania bieżącymi incydentami, obejmujące zarówno pracowników podmiotu nadzorowanego jak i dostawcy usług chmury obliczeniowej, a w przypadku istotnego narażenia na skutki danego incydentu – również innych stron (np. klientów, poddostawców), w celu zapewnienia adekwatności postępowania do poziomu istotności incydentu.
- 4.2. Bez uszczerbku dla wymagań prawa oraz z uwzględnieniem postanowień niniejszego komunikatu, podmiot nadzorowany może korzystać z ramowych umów udostępnianych przez dostawców usług chmury obliczeniowej, w szczególności gdy dotyczą one usług chmury obliczeniowej tworzonych dla grupy podmiotów (w tym podmiotu nadzorowanego) w ramach umów o charakterze korporacyjnym lub grupowym, w tym również chmury obliczeniowej społecznościowej.

W takim przypadku podmiot nadzorowany powinien:

- a) zweryfikować w jakim zakresie umowa ramowa oraz powiązane z nią dokumenty, wyniki szacowania ryzyka oraz wymagania prawne, organizacyjne i techniczne uwzględniają postanowienia niniejszego komunikatu oraz są adekwatne dla sytuacji podmiotu nadzorowanego i jego zamiarów związanych z przetwarzaniem informacji w chmurze obliczeniowej;
- b) ocenić konieczność lub możliwość samodzielnego stosowania wymagań niniejszego komunikatu w zakresie, który nie jest zgodny z umową ramową i powiązanymi z nią dokumentami.

5. Plan przetwarzania informacji w chmurze obliczeniowej

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

- a) rodzaj (opis) przetwarzanych informacji oraz informację, jeżeli stosowane, o ich pseudonimizacji lub anonimizacji;
- b) sposób szyfrowania informacji oraz miejsce (lub sposób) zarządzania kluczami szyfrującymi;
- c) informację o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany;
- d) datę zawarcia umowy z dostawcą usług chmury obliczeniowej i referencje do tej umowy (numer, okres obowiązywania, datę przedłużenia lub zmiany, daty rozpoczęcia korzystania z usług), a w przypadku gdy umowa nie jest jeszcze zawarta – przewidywaną datę jej zawarcia;

- e) prawo właściwe, któremu podlega umowa;
 - f) opis zadania realizowanego za pomocą usługi chmury obliczeniowej wraz z informacją, czy jest to outsourcing szczególny chmury obliczeniowej w rozumieniu niniejszego komunikatu lub czy przetwarzane są informacje prawnie chronione.
- 5.2. Uruchomienie produkcyjne stosowania usług chmury obliczeniowej powinien poprzedzać okres testowy, podczas którego na danych testowych (generowanych maszynowo lub w inny przypadkowy sposób), w udokumentowanym procesie, testowane są scenariusze adekwatne do oszacowanego ryzyka.
- 5.3. Podmiot nadzorowany posiada udokumentowany, przetestowany plan wycofania swojego zaangażowania w przetwarzanie informacji w usługach chmury obliczeniowej danego dostawcy (również w sytuacji awaryjnej), bez uszczerbku dla zachowania zgodności swojego działania z wymaganiami prawa i innych regulacji, w tym w szczególności związanych z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.
- 5.4. Podmiot nadzorowany powinien posiadać udokumentowany plan ciągłości działania uwzględniający potencjalną możliwość utraty kontroli nad przetwarzanymi informacjami u danego dostawcy usług chmury obliczeniowej oraz możliwość przerwania ciągłości działania usługi. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej dostawców usług chmury obliczeniowej, podmiot nadzorowany regularnie weryfikuje własną zdolność do utrzymania deklarowanych założeń, w szczególności zgodność konfiguracji usług i odtwarzalności środowiska teleinformatycznego, zwłaszcza po zmianach technologicznych u jednego z dostawców usług chmury obliczeniowej.

6. Wymagania dla dostawców usług chmury obliczeniowej⁶

- 6.1. W zakresie świadczonych usług chmury obliczeniowej i odpowiednio do ich skali dostawca usług chmury obliczeniowej spełnia wymagania zapewnienia zgodności swojego działania z poniższymi normami lub ich odpowiednikami w polskim lub europejskim układzie normalizacji, chyba że podmiot nadzorowany akceptuje (na podstawie wyników szacowania ryzyka) brak konieczności spełnienia tego wymagania albo jego części:
- a) PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT;
 - b) PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji;
 - c) PN-EN ISO 22301 dotyczące zarządzania ciągłością działania;
 - d) ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej;
 - e) ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej.
- 6.2. CPD dostawcy usług chmury obliczeniowej spełnia wymagania normy PN-EN 50600 (Wyposażenie i infrastruktura centrów przetwarzania danych) minimum klasy 3 lub ANSI/TIA-942 minimum Tier III, lub innego normatywu odpowiedniego i uznanego do oceny CPD lub zawierającego wymagania z nim związane, przy czym podmiot nadzorowany może zaakceptować (w uzasadnionych przypadkach i na podstawie szacowania ryzyka) brak spełnienia części wymagań.

⁶ Wymagania te uwzględnia podmiot nadzorowany w swoim podejściu do stosowania usług chmury obliczeniowej, a w szczególności w procesie szacowania ryzyka.

- 6.3. Nadzór rekomenduje, aby CPD zlokalizowane było na terytorium państwa Europejskiego Obszaru Gospodarczego (EOG). Punkt ten stosuje się z zastrzeżeniem, że podmioty nadzorowane, które:
- a) zostały uznane stosowną decyzją za operatorów usług kluczowych w rozumieniu art. 5 ust. 2 ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa i którzy wykorzystują usługę chmury obliczeniowej w zakresie realizacji usługi kluczowej lub
 - b) są operatorami infrastruktury krytycznej w rozumieniu ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym i którzy wykorzystują usługę chmury obliczeniowej w zakresie realizacji zadań operowania infrastrukturą krytyczną
- powinny w pierwszej kolejności wykorzystywać CPD znajdujące się na terenie Rzeczypospolitej Polskiej, o ile – w ocenie podmiotu nadzorowanego – oferowane warunki umowne, ekonomiczne, operacyjne, SLA czy funkcjonalne są nie gorsze od CPD znajdujących się poza terytorium Rzeczypospolitej Polskiej.
- 6.4. Dostawca usług chmury obliczeniowej zapewnia w swoim postępowaniu udokumentowaną zasadę ochrony przetwarzanych przez podmiot nadzorowany informacji przed nieautoryzowanym dostępem lub użyciem przez swoich pracowników lub poddostawców poprzez co najmniej:
- a) domyślną zasadę braku dostępu do przetwarzanych informacji podmiotu nadzorowanego;
 - b) domyślną zasadę braku konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego lub w innych uruchamianych usługach chmury obliczeniowej;
 - c) zasadę „minimum koniecznego” dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez podmiot nadzorowany (w tym również usunięcia usterek) oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. Obowiązujące w tym zakresie procedury obsługi mogą być dodatkowo potwierdzone stosownym certyfikatem (np. SOC⁷ 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji;
 - d) udostępnienie wytycznych, wzorcowych konfiguracji, opisów zasad, itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji;
 - e) domyślne uruchamianie nowego środowiska (lub usługi chmury obliczeniowej) separowanego od innych tenantów, z ustawieniami „secure-by-default”⁸.
- 6.5. Spełnienie wymagań może być poświadczane odpowiednimi certyfikatami zgodności wystawionym przez niezależne jednostki certyfikujące, akredytowane w polskim lub europejskim systemie akredytacji.

⁷ System and Organization Controls.

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

7. Kryptografia

- 7.1. Podmiot nadzorowany powinien zapewnić, że informacje przetwarzane w chmurze obliczeniowej są szyfrowane zgodnie z zasadami określonymi w niniejszym komunikacie. W szczególności podmiot nadzorowany powinien upewnić się, że:
- a) posiada dostęp do szczegółowych i aktualnych instrukcji konfiguracji usług chmury obliczeniowej oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji;
 - b) zapewnia dostateczne kompetencje w celu realizacji poprawnej konfiguracji usług chmury obliczeniowej, zgodnie z wytycznymi dostawcy usług chmury obliczeniowej, w tym pod kątem stosowania szyfrowania przetwarzanych informacji;
 - c) używa dedykowanych lub zalecanych przez dostawcę usług chmury obliczeniowej ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług chmury obliczeniowej;
 - d) informacje prawnie chronione przetwarzane w chmurze obliczeniowej są szyfrowane zarówno „at rest” jak i „in transit”.
- 7.2. Podmiot nadzorowany powinien zapewnić, że informacje są szyfrowane kluczami generowanymi oraz zarządzanymi przez podmiot nadzorowany, chyba że z oszacowania ryzyka wynika, iż dopuszczalne lub wskazane jest używanie kluczy szyfrujących generowanych lub zarządzanych przez dostawcę usług chmury obliczeniowej.
- 7.3. W przypadku, gdy z szacowania ryzyka wynika konieczność utrzymywania i zarządzania kluczami szyfrującymi przy wykorzystaniu sprzętowych rozwiązań (HSM⁹), to HSM mogą być udostępniane przez dostawcę usług chmury obliczeniowej, przy uwzględnieniu tego elementu w szacowaniu ryzyka. HSM powinny spełniać wymagania minimum FIPS¹⁰ 140-2 Level 2 lub równoważne.
- 7.4. Podmiot nadzorowany w udokumentowanym procesie zarządza tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz kontrolą tego procesu.
- 7.5. Proces zarządzania kluczami szyfrującymi powinien uwzględniać przechowywanie w ramach własnej infrastruktury kopii kluczy szyfrujących, które zostały wygenerowane lub są zarządzane przez dostawcę usług chmury obliczeniowej i są używane w procesie outsourcingu szczególnego chmury obliczeniowej, chyba że z oszacowania ryzyka wynika uzasadniony brak takiej potrzeby.

8. Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej

- 8.1. Podmiot nadzorowany posiada udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej, stosownie do zakresu używanych usług chmury obliczeniowej, przetwarzanych informacji i wyników szacowania ryzyka.
- 8.2. Podmiot nadzorowany zabezpiecza logi przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa wynikającymi z szacowania ryzyka oraz obowiązującymi przepisami szczegółowymi w tym zakresie.

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

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

- 8.3. Uprawniony personel podmiotu nadzorowanego dokonuje przeglądu logów zgodnie z udokumentowanymi procedurami i zasadami bezpieczeństwa, przy czym – zależnie od skali działania, rodzaju i liczby logowanych zdarzeń oraz architektury bezpieczeństwa – Nadzór zaleca używanie specjalistycznego oprogramowania do korelowania zapisów ze zdarzeń (SIEM) oraz regularny przegląd i aktualizację reguł korelacji.
- 8.4. Wymagania w stosunku do podmiotu nadzorowanego w zakresie zarządzania dostawcami usług mającymi dostęp zdalny do usług chmury obliczeniowej wykorzystywanych przez podmiot nadzorowany¹¹:
- a) podmiot nadzorowany zapewnia, że wyłącznie uprawniony personel dostawcy usług ma dostęp do wskazanych systemów teleinformatycznych lub ich wybranych zakresów;
 - b) podmiot nadzorowany wymaga używania przez personel dostawcy usług uwierzytelnienia MFA, przy czym rodzaj i zakres uzależniony jest od wyników szacowania ryzyka;
 - c) podmiot nadzorowany zapewnia, że dostęp administracyjny lub o charakterze uprzywilejowanym realizowany jest z zaufanych sieci podmiotu nadzorowanego lub dostawcy usług i pod kontrolą (w tym np. poprzez nagrywanie sesji i jej parametrów, a następnie poprzez analizowanie prawidłowości i celowości realizowanych czynności), chyba że z szacowania ryzyka wynika uzasadniony brak takiej potrzeby.

9. Dokumentowanie działań podmiotu nadzorowanego

- 9.1. Tam gdzie jest to zasadne, zależnie od zakresu i rodzaju przetwarzanych informacji, zasad i regulacji obowiązujących i przyjętych w organizacji (z uwzględnieniem powiązań korporacyjnych i grupowych, jeżeli występują) oraz wyników szacowania ryzyka i przy uwzględnieniu zasady proporcjonalności, podmiot nadzorowany posiada dokumentację zawierającą:
- a) organizację pracowników lub współpracowników odpowiedzialnych za cyberbezpieczeństwo, w tym stanowisk lub funkcji związanych z monitorowaniem, analizowaniem i raportowaniem incydentów związanych z informacjami przetwarzanymi w chmurze obliczeniowej, wraz z opisanymi wymaganymi kompetencjami, uprawnieniami i odpowiedzialnościami;
 - b) architekturę sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych podmiotu nadzorowanego z sieciami niezaufanymi, w tym architekturę rozwiązania w chmurze obliczeniowej, także z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych;
 - c) zasady kategoryzacji informacji lub systemów pod kątem przetwarzania w chmurze obliczeniowej lub odniesienie do obecnie funkcjonujących klasyfikacji, jeżeli mogą być stosowane;
 - d) zasady stosowanych zabezpieczeń technologicznych i rozwiązań organizacyjnych;
 - e) zasady zarządzania ciągłością działania;

¹¹ Wymagania te dotyczą sytuacji, w której podmiot nadzorowany zleca swojemu dostawcy usług wykonanie działań na zasobach podmiotu nadzorowanego umieszczonych w chmurze obliczeniowej (np. aktualizacja oprogramowania, prace serwisowe). Wymagania te nie dotyczą usług wsparcia świadczonych przez dostawcę usług chmury obliczeniowej w zakresie standardów obsługi wynikających z umowy na świadczenie usług chmury obliczeniowej.

- f) zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z dostawcą usług chmury obliczeniowej;
- g) zasady zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi;
- h) zasady przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem usług chmury obliczeniowej;
- i) zasady raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej;
- j) umowy z dostawcami usług chmury obliczeniowej wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań;
- k) procesy, procedury lub instrukcje dotyczące:
 - i. analizy zagrożeń i szacowania ryzyka, w tym źródła pozyskiwania informacji o zagrożeniach specyficznych dla stosowanych usług chmury obliczeniowej oraz sektora finansowego;
 - ii. zarządzania środowiskiem teleinformatycznym (sieciami, systemami, aplikacjami, bazami danych, itp.), z uwzględnieniem usług chmury obliczeniowej, w tym planowanie, rozwój i utrzymywanie;
 - iii. zarządzania logami;
 - iv. zarządzania kluczami szyfrującymi;
 - v. zarządzania incydentami bezpieczeństwa;
 - vi. przeprowadzania audytów wewnętrznych bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej.

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

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 dni¹² 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;

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

- 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.

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 publicznej lub hybrydowej*, 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 lub przewidywany termin jej zawarcia:	
Okres na jaki została zawarta umowa z dostawcą usług chmury obliczeniowej:	
Osoby do kontaktu w sprawie stosowania chmury obliczeniowej w podmiocie nadzorowanym (imię, nazwisko lub stanowisko, nr telefonu, adres e-mail):	

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

Miejscowość, data

Podpisy osób reprezentujących podmiot nadzorowany

PRZYKŁAD WYPEŁNIENIA ZAŁĄCZNIKA NR 1

Informacja podmiotu nadzorowanego w sprawie przetwarzania informacji w chmurze obliczeniowej

Oznaczenie podmiotu nadzorowanego (nazwa, adres, NIP, REGON)	BANK S.A., ul. Polska 11/11, 00 – 001 Warszawa, NIP: 1234567890, REGON: 987654321
--	---

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

Rodzaj i zakres przetwarzanych informacji:	Informacje o reklamacjach klientów banku: dane osobowe klientów, nagrania rozmów na infolinii, decyzje w procesie reklamacyjnym, pisma reklamacyjne i odpowiedzi na nie
Nazwa i adres dostawcy usług chmury obliczeniowej:	Dostawca Chmury S.A., ul. Chmurowa 90, 00 – 001 Warszawa
Nazwy usług chmury obliczeniowej lub ich rodzaj:	Serwery wirtualne, storage, sieci wirtualne, aplikacja CRM
Lokalizacje CPD przetwarzanych informacji (państwo, region):	Warszawa, Wrocław, Frankfurt (Niemcy), Dublin (Irlandia)
Data podpisania umowy z dostawcą usług chmury obliczeniowej lub przewidywany termin jej zawarcia:	10.2020 – przewidywany termin zawarcia umowy
Okres na jaki została zawarta umowa z dostawcą usług chmury obliczeniowej:	Na okres 3 lat od daty zawarcia umowy
Osoby do kontaktu w sprawie stosowania chmury obliczeniowej w podmiocie nadzorowanym (imię, nazwisko lub stanowisko, nr telefonu, adres e-mail):	Jan Kowalski, Administrator, tel. 22 00 000 00, e-mail: jan.kowalski@domena_banku_sa.pl

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

Warszawa, 01.08.2020

Członek Zarządu Banku

Prokurent Banku

Miejscowość, data

Podpisy osób reprezentujących podmiot nadzorowany