ZWIĄZEK BANKÓW POLSKICH

STANDARD
POLISHCLOUD 2.0

STANDARD WDROŻENIA USŁUGI CHMURY OBLICZENIOWEJ PUBLICZNEJ LUB HYBRYDOWEJ

Warszawa, Luty 2022

Spis treści

Autorzy Standardu

Standard wdrożeń w chmurze obliczeniowej publicznej lub hybrydowej został opracowany w ramach prac grupy roboczej powołanej przy Forum Technologii Bankowych ZBP i Radzie Bankowości Elektronicznej ZBP.

KOORDYNATORZY PROJEKTU ZE STRONY ZWIĄZKU BANKÓW POLSKICH

Bartłomiej Nocoń

Dominik Sadłakowski

Joanna Barbrich

KOORDYNATORZY GRUP ROBOCZYCH

Maciej Leśniewski, Pekao SA

Marek Dryjański, Citi Handlowy

Szymon Ciach, Kancelaria Kochański & Partners

Dorota Rybińska, PKO BP

Łukasz Krzyżanowski, Accenture

ZESPÓŁ REDAKCYJNY

Adam Gutenbaum, PKO BP

Adam Ksit, mBank

Adam Podraza, Ab Initio

Adam Wójcicki, DELL Polska

Adam Wygodny, Pekao SA

Adam Zakrzewski, IBM Polska

Aleksandra Piech Kancelaria Kochański & Partners

Artur Rudziński, Alior Bank

Bartłomiej Suchowierski, GFT Polska

Bogusław Borgosz, BNP Paribas Bank Polska

Dagmara Barańska, Citi Handlowy

Daniel Dyszlewski, Accenture

Daniel Kozłowski, Kancelaria Kochański & Partners

Grażyna Dadej, IBM Polska

Hubert Kuna, Santander Bank Polska

Jarosław Szczepankiewicz, GFT Poland

Karol Smuś, DELL Polska

Karolina Czwarno-Kos, BNP Paribas Bank Polska

Krzysztof Szczepański, Krajowa Izba Rozliczeniowa

Łukasz Cyrulski, GFT Poland

Maciej Kuranc, Kancelaria Kochański & Partners

Maciej Leśniewski, Pekao SA

Magdalena Knapik, BNP Paribas Bank Polska

Marek Dryjański, Citi Handlowy

Marek Dzięciołowski, PKO BP

Marek Pyka, Microsoft

Mateusz Grajnert, GFT Polska

Michał Bugowski, Integral Solutions

Michał Jurga, ING Bank Śląski

Michał Lewandowski, IDEA Bank

Mikołaj Bela, Asseco Poland

Monika Hałasa-Mochocka, Citi Handlowy

Olga Budziszewska, Accenture

Paweł Albert, DELL Polska

Paweł Leszek, Santander Bank Polska

Paweł Sokołowski, SAS Institute

Tomasz Hałys, Asseco Poland

Zbigniew Korbutt-Madajewski, Asseco Poland

Wstęp

ODPOWIEDŹ NA POTRZEBY RYNKU

W 2019 r. Związek Banków Polskich (ZBP) i Forum Technologii Bankowych (FTB), wychodząc naprzeciw oczekiwaniom sektora bankowego w Polsce, dotyczącym wdrażania rozwiązań opartych o chmurę obliczeniową, podjęły inicjatywę zdefiniowania zasad, który ułatwiałyby bankom proces transformacji cyfrowej.

Prowadząc działalność gospodarczą, banki, jak i inne podmioty nadzorowane, są zobowiązane do działania zgodnie z przepisami odpowiednich ustaw, rozporządzeń, jak również rekomendacji i wytycznych nadzoru finansowego. Wykorzystanie najnowszych rozwiązań technologicznych w bankowości na tle tych uwarunkowań jest zadaniem złożonym, które wymaga zaangażowania wielu jednostek banku od strony biznesowej, technologicznej oraz regulacyjnej. Rosnące zainteresowanie usługami chmurowymi wywołało potrzebę standaryzacji procesu ich wdrażania.

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

24 stycznia 2020 r. (wydany w dniu 23 stycznia 2020 r.) UKNF opublikował kolejny komunikat dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej (Komunikat), który wyjaśnia wiele kwestii budzących wcześniej wątpliwości banków. Komunikat, zgodnie z jego brzmieniem, uzupełnia i uszczegóławia wybrane zalecenia w zakresie outsourcingu, opisane między innymi w Rekomendacji D, M oraz ustawie Prawo bankowe. Regulacje te muszą być brane pod uwagę przy określaniu możliwości, a następnie przy faktycznym wdrożeniu rozwiązań opartych o chmurę obliczeniową. Komunikat prezentuje podejście krajowe (model referencyjny), co oznacza, że wytyczne, zalecenia lub inne dokumenty prezentujące stanowisko Europejskiego Urzędu Nadzoru Bankowego (EBA), które odnoszą się do przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej, w tym Wytyczne Europejskiego Urzędu Nadzoru Bankowego z dnia 25 lutego 2019 r., nie mają zastosowania do polskich banków w zakresie wdrożeń chmury obliczeniowej.

Upowszechnienie wykorzystania usług chmury obliczeniowej, wydanie Komunikatów UKNF oraz dotychczasowe doświadczenia płynące z wdrożeń chmurowych spowodowały, że ZBP i FTB, przy aktywnym udziale banków, dostawców usług chmurowych, firm doradczych, postanowił opracować Standard, stanowiący zbiór praktyk i rozwiązań umożliwiających bankom sprawne przejście przez proces adaptacji do chmury, zarówno w całej organizacji, jak i w zakresie jedynie wybranych rozwiązań oferowanych przez dostawców usług chmurowych.

NOWA WERSJA STANDARDU

Stanowiąca niniejsze opracowanie wersja 2.0 Standardu uzupełnia pierwsze wydanie (Standard 1.0, wydany w marcu 2020 r.) i na bazie ponadrocznych doświadczeń w sposób bardziej precyzyjny i szczegółowy prezentuje, jakie zadania, procedury, procesy i analizy Bank oraz Dostawca usługi chmurowej powinny przeprowadzić i udokumentować pod kątem przygotowania Banku do wdrożenia usług chmury obliczeniowej.

ZAŁOŻENIA

Podkreślenia wymaga, że Standard odnosi się do wymogów dotyczących korzystania z rozwiązań chmurowych przez podmioty objęte nadzorem bankowym w rozumieniu Ustawy z dnia 21 lipca 2006 r., ze zmianami o nadzorze nad rynkiem finansowym. Standard nie odnosi się zatem do wymogów dotyczących rozwiązań chmurowych dla innych niż banki podmiotów objętych nadzorem wskazanym w tej ustawie, co w sferze czynności obejmuje wyłącznie czynności bankowe zgodnie z przepisami Prawa bankowego (zgodnie z definicją wskazaną w rozdziale 2 poniżej).

Zasadniczą podstawą Standardu są wymogi komunikatu UKNF z dnia 23 stycznia 2020 r., a co za tym idzie, przedstawia on wymagania w przypadku przetwarzania w podmiotach objętych nadzorem bankowym informacji w chmurze obliczeniowej publicznej lub chmurze obliczeniowej hybrydowej.

Standard uwzględnia również „Pytania i odpowiedzi" (Q&A) UKNF ws. wątpliwości dotyczących przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, opublikowane na oficjalnej stronie internetowej Komisji Nadzoru Finansowego pod linkiem: https:/www.knf.gov.pl/dla_rynku/fin_tech/chmura_obliczeniowa/Q&A (dalej „Q&A chmurowy").

STOSOWANIE STANDARDU

Standard może być wykorzystany jako przykładowy model postępowania (ang. *framework*) przez podmioty sektora bankowego we wdrożeniach chmurowych, natomiast jego stosowanie każdorazowo powinno uwzględniać specyfikę działalności danego podmiotu nadzorowanego.

W przypadku wątpliwości w zakresie zastosowania Standardu w swojej działalności Bank ma możliwość zwrócenia się do UKNF w celu wyjaśnienia danego problemu w kontekście określonego stanu faktycznego.

Standard może być również wykorzystywany przez inne podmioty niż podmioty sektora bankowego, jednak w takiej sytuacji powinny one uwzględnić, że część zagadnień, zwłaszcza ściśle związanych z kwestiami prawnymi, jest specyficzna wyłącznie dla sektora bankowego.

WSPÓŁPRACA

ZBP zachęca podmioty korzystające ze Standardu (nie tylko podmioty nadzorowane) do dzielenia się swoimi spostrzeżeniami w zakresie jego stosowania poprzez kontakt na adres mailowy: PolishCloud@zbp.pl.

Opinie użytkowników pozwolą aktualizować Standard i dalej dostosowywać go do praktyki rynkowej, a także kierować pytania do UKNF w celu wyjaśnienia najbardziej problematycznych zagadnień.

Mamy nadzieję, że Standard w wersji 2.0 będzie dobrym przewodnikiem po zawiłych kwestiach związanych z procesem wdrażania chmury obliczeniowej w Państwa organizacjach, a tym samym przydatnym narzędziem udoskonalania tego procesu.

Pragniemy złożyć szczególne podziękowania wszystkim osobom zaangażowanym w przygotowanie niniejszego dokumentu, w tym w szczególności przewodniczącym oraz członkom Prezydiów Rady Bankowości Elektronicznej oraz Forum Technologii Bankowych działających przy Związku Banków Polskich za ich cenne wsparcie i inspiracje oraz przekazywane doświadczenia w obszarze technologii chmury obliczeniowej.

Autorzy

Terminologia stosowana w Standardzie

Objaśnienie wybranych definicji Komunikatu

W niniejszym Standardzie poniższe terminy mają następujące znaczenie:

DEFINICJE OGÓLNE

1. **Bank** – podmiot nadzorowany w rozumieniu Komunikatu, w zawężeniu do podmiotu objętego nadzorem bankowym, w tym bank w rozumieniu Prawa bankowego (krajowy), oddział banku krajowego za granicą, oddział banku zagranicznego w rozumieniu Prawa bankowego, instytucja kredytowa w rozumieniu Prawa bankowego, oddział instytucji kredytowej w rozumieniu Prawa bankowego, bank krajowy prowadzący działalność na terytorium państwa goszczącego poprzez oddział lub w ramach działalności transgranicznej zgodnie z Prawem bankowym oraz bank spółdzielczy w rozumieniu Ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających (jak już wskazano powyżej, z zakresu niniejszego Standardu wyłączone zostały podmioty nadzorowane w rozumieniu Ustawy o nadzorze nad rynkiem finansowym inne niż podmioty podlegające nadzorowi bankowemu), przy czym:

   a) w stosunku do oddziału banku zagranicznego w rozumieniu Prawa bankowego w oparciu o art. 40 ust. 1 oraz art. 139 Prawa bankowego Komunikat stosujemy odpowiednio w zależności od rodzaju i zakresu czynności wykonywanych przez dany oddział instytucji kredytowej,

   b) w stosunku do oddziału instytucji kredytowej w rozumieniu Prawa bankowego w oparciu o art. 48k ust. 1 oraz 2 Prawa bankowego Komunikat stosujemy odpowiednio w zależności od rodzaju i zakresu czynności wykonywanych przez dany oddział instytucji kredytowej,

   c) w stosunku do oddziału banku krajowego za granicą możliwy może być dodatkowy nadzór nadzorcy finansowego z takiego kraju;

   Dla uniknięcia wątpliwości, nadzorem bankowym, a zatem wyłączonym spod niniejszej definicji, są objęte następujące podmioty:

   a) przedstawicielstwa banku zagranicznego w rozumieniu Prawa bankowego,

b) przedstawicielstwa instytucji kredytowej w rozumieniu Prawa bankowego oraz

c) bank zagraniczny i instytucje kredytowe w ramach działalności transgranicznej, o której mowa w art. 48i Prawa bankowego.

2. **Chmura obliczeniowa** – zgodnie ze znaczeniem nadanym w Komunikacie jest to 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 Dostawcy. Na potrzeby Standardu, przez chmurę obliczeniową rozumiemy chmurę obliczeniową publiczną i chmurę obliczeniową hybrydową.

3. **Chmura obliczeniowa hybrydowa** – zgodnie ze znaczeniem nadanym w Komunikacie jest to 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.

4. **Chmura obliczeniowa publiczna** – zgodnie ze znaczeniem nadanym w Komunikacie jest to chmura obliczeniowa dostępna do użytku publicznego, będąca w posiadaniu lub bezpośrednio zarządzana przez Dostawcę usług chmury obliczeniowej.

5. **Chmura obliczeniowa prywatna** – zgodnie ze znaczeniem nadanym w Komunikacie jest to chmura obliczeniowa dostępna do wyłącznego użytku jednego podmiotu, będąca w posiadaniu lub bezpośrednio zarządzana przez ten podmiot.

6. **Chmura obliczeniowa społecznościowa** – zgodnie ze znaczeniem nadanym w Komunikacie jest to 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.

7. **Informacja prawnie chroniona** – zgodnie ze znaczeniem nadanym w Komunikacie oznacza informację związaną z tajemnicami sektora finansowego, wymienionymi w ustawach sektorowych.

8. **CPD** – zgodnie ze znaczeniem nadanym w Komunikacie – centrum przetwarzania danych.

9. **Dostawca usług chmury obliczeniowej** – zgodnie ze znaczeniem nadanym w Komunikacie jest to podmiot, który dysponuje infrastrukturą i oprogramowaniem służącym do świadczenia usług chmury obliczeniowej oraz świadczy usługi chmury obliczeniowej.

10. **Łańcuch outsourcingowy** – zgodnie ze znaczeniem nadanym w Komunikacie oznacza relację polegającą na:

    a) powierzeniu przez Dostawcę usług chmury obliczeniowej części czynności (służących dostarczaniu usługi chmury obliczeniowej dla podmiotu nadzorowanego) swojemu podostawcy i dalszym (kolejnym) poddostawcom lub

    b) dostarczaniu przez Dostawcę usług chmury obliczeniowej usługi chmury obliczeniowej innemu dostawcy, który wykorzystuje usługę chmury obliczeniowej do świadczenia własnej usługi dla podmiotu nadzorowanego.

11. **EOG** – Europejski Obszar Gospodarczy.

12. **Kodeks cywilny** – oznacza ustawę z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tj. Dz. U. z019 r. poz. 1145, ze zmianami).

13. **Komunikat** – komunikat Urzędu Komisji Nadzoru Finansowego z dnia 23 stycznia 2020 r. dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej.

14. **KNF** – Komisja Nadzoru Finansowego.

15. **UKNF** – Urząd Komisji Nadzoru Finansowego.

16. **Outsourcing chmury obliczeniowej** – zgodnie ze znaczeniem nadanym w Komunikacie 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 służącej do wsparcia realizacji procesu, usługi lub zadania, które podmiot nadzorowany realizowałby samodzielnie, gdyby usługa chmury obliczeniowej była niedostępna.

17. **Outsourcing szczególny chmury obliczeniowej** lub **Outsourcing szczególny** – zgodnie ze znaczeniem nadanym w Komunikacie 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) wpływałaby w sposób istotny na ciągłość wypełniania przez podmiot nadzorowany warunków stanowiących podstawę uprawnienia prowadzenia działalności nadzorowanej lub jej wykonywania lub
    b) zagrażałoby w sposób istotny wynikom finansowym podmiotu nadzorowanego, niezawodności lub ciągłości wykonywania działalności nadzorowanej.

18. **Poddostawca** – zgodnie ze znaczeniem nadanym w Komunikacie jest to 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.

19. **Prawo bankowe** – oznacza ustawę z 29 sierpnia 1997 r. – Prawo bankowe, ze zmianami.

20. **Rekomendacja D** – rekomendacja wydana przez Komisję Nadzoru Finansowego w styczniu 2013 r., dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

21. **Rekomendacja M** – rekomendacja wydana przez Komisję Nadzoru Finansowego w styczniu 2013 r., dotycząca zarządzania ryzykiem operacyjnym w bankach.

22. **RODO** – oznacza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

23. **Standard 1.0** – oznacza opublikowaną 19 marca 2020 roku pierwszą wersję niniejszego opracowania, dostępną pod linkiem: https:/zbp.pl/Dla-Bankow/Bankowosc-elektroniczna/PolishCloud.

24. **Standard** – oznacza niniejsze opracowanie.

25. **Stanowisko UKNF** – stanowisko UKNF z dnia 16 września 2019 r., dotyczące wybranych zagadnień związanych z wejściem w życie Wytycznych EBA w sprawie outsourcingu i ich uwzględnianiem w działalności banków.

26. **Tajemnica bankowa** – ma znaczenie nadane w art. 104 Prawa bankowego, a więc „wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje".

27. **Udokumentowany proces** – zgodnie ze znaczeniem nadanym w Komunikacie oznacza 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.

28. **Ujawnienie informacji** – zgodnie ze znaczeniem nadanym w Komunikacie 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.

29. **Usługa chmury obliczeniowej** – zgodnie ze znaczeniem nadanym w Komunikacie oznacza 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.

30. **Ustawa o nadzorze nad rynkiem finansowym** – oznacza ustawę z dnia 21 lipca 2006 r., ze zmianami o nadzorze nad rynkiem finansowym.

31. **Ustawa o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających** – oznacza ustawę z dnia 7 grudnia 2000 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających.

32. **Wartość informacji** – zgodnie ze znaczeniem nadanym w Komunikacie oznacza konsekwencję dla działalności podmiotu nadzorowanego materializacji ryzyka polegającego na nieuprawnionym ujawnieniu, zmianie lub zniszczeniu informacji.

33. **Wytyczne EBA** – Wytyczne Europejskiego Urzędu Nadzoru Bankowego z dnia 25 lutego 2019 r.

DODATKOWE DEFINICJE PRZYJĘTE W STANDARDZIE

Poniżej zaprezentowano dodatkowo definicje zawarte w Komunikacie wraz ze znaczeniem, w jakim są stosowane w niniejszym Standardzie i zgodnie z przyjętymi Założeniami i Zastrzeżeniami, oraz tam, gdzie to stosowne, opatrzone komentarzem lub wyjaśnieniem:

Chmura obliczeniowa społecznościowa

Chmura obliczeniowa społecznościowa może mieć charakter:

a. chmury obliczeniowej prywatnej, gdy jest dostępna do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy i jest przy tym zarządzana przez podmiot z grupy albo

b. chmury obliczeniowej publicznej, gdy jest dostępna do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy, lecz jest przy tym zarządzana przez Dostawcę.

Chmura obliczeniowa prywatna

Zgodnie ze znaczeniem nadanym w Komunikacie jest to chmura obliczeniowa dostępna do wyłącznego użytku jednego podmiotu, będąca w posiadaniu lub bezpośrednio zarządzana przez ten podmiot. Jako chmurę prywatną w szczególności można traktować infrastrukturę serwerowo-storage'ową (wraz z dedykowanym wdrożeniem oprogramowania zarządzającego chmurą), dedykowaną dla podmiotu nadzorowanego, przy jednoczesnym korzystaniu ze współdzielonych fizycznie zasobów infrastruktury sieciowej. Korzystanie z takich zasobów sieciowych nie zmienia kwalifikacji chmury jako prywatnej.

Informacja prawnie chroniona

Tajemnica bankowa mająca znaczenie nadane w art. 104 Prawa bankowego, a więc: „wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje".

Outsourcing szczególny chmury obliczeniowej

Wyłącznie pomocniczo, zamieszczamy kryteria (referencje) w zakresie oceny, czy dana czynność jest istotna/podstawowa (w oparciu o kryteria zaproponowane przez Wytyczne EBA):

a. czy umowa outsourcingu dotyczy bezpośrednio czynności bankowej;

b. potencjalny wpływ zakłócenia lub niewykonania przez Dostawcę badanej czynności na uzgodnionym gwarantowanym poziomie usług w trybie ciągłym na:

   i. krótko- i długoterminową odporność i kondycję finansową, w tym, jeżeli dotyczy, jej aktywa, kapitał, koszty, finansowanie, płynność, zyski i straty,
   ii. ciągłość działania i odporność operacyjną,
   iii. ryzyko operacyjne, w tym prowadzenie działalności, technologie informacyjne i komunikacyjne (ICT) i ryzyko prawne,
   iv. ryzyko utraty reputacji,
   v. w stosownych przypadkach, planowanie w zakresie działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji, możliwość przeprowadzenia skutecznej restrukturyzacji i uporządkowanej likwidacji oraz ciągłość operacyjną w sytuacji wczesnej interwencji, działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji;

c. potencjalny wpływ zlecenia badanej czynności na zdolność Banku do:
    i. identyfikacji ryzyka, zarządzania ryzykiem i jego monitorowania,
    ii. spełnienia wszystkich wymogów prawnych i regulacyjnych,
    iii. przeprowadzenia stosownych audytów dotyczących funkcji będących przedmiotem outsourcingu;
d. potencjalny wpływ na usługi świadczone na rzecz klientów;
e. wszelkie umowy outsourcingu, łączna ekspozycja Banku na tego samego Dostawcę oraz potencjalny łączny wpływ umów outsourcingu w tym samym obszarze działalności;
f. rozmiar i złożoność danego obszaru działalności;
g. możliwość rozszerzenia zakresu proponowanej umowy outsourcingu bez zastępowania lub zmiany umowy bazowej;
h. zdolność do przeniesienia proponowanej umowy outsourcingu na innego Dostawcę, jeżeli jest to niezbędne lub pożądane, zarówno na podstawie umowy, jak i w praktyce, w tym szacunkowe ryzyko, przeszkody dla ciągłości działania, koszty i ramy czasowe z tym związane;
i. zdolność do reintegracji czynności zleconej na zasadzie outsourcingu do Banku, jeżeli jest to niezbędne lub pożądane, oraz
j. ochronę danych i możliwy wpływ naruszenia poufności lub niezapewnienie dostępności i integralności danych na instytucję lub instytucję płatniczą i jej klientów, w tym między innymi zgodność z RODO.

Dodatkowo, zgodnie z Q&A chmurowym, Bank, w kontekście kwalifikacji danej czynności lub funkcji jako outsourcingu szczególnego chmury obliczeniowej, powinien przy takiej kwalifikacji brać pod uwagę skalę ocenianego procesu (czynności lub funkcji) i fakt, że może ona się zmieniać w trakcie prowadzonej działalności. Jak wskazuje UKNF: „proces, który wyjściowo nie był oceniany jako krytyczny i istotny, może z biegiem czasu zwiększyć swoją skalę i przez to powinien zostać zakwalifikowany jako kluczowy i krytyczny".

Poddostawca

Poddostawcą w rozumieniu Komunikatu jest podmiot, który:

1. świadczy usługi dla Dostawcy usług chmury obliczeniowej, służące dostarczaniu usługi chmury obliczeniowej dla Banku, oraz
2. posiada lub może posiadać identyfikowany dostęp do informacji przetwarzanych przez Bank.

W zakresie 1. powyżej intencją Komunikatu jest zawężenie zakresu poddostawców do podmiotów, które świadczą na rzecz Dostawcy usług chmurowych tego typu usługi, które są **bezpośrednio i funkcjonalnie** związane z możliwością efektywnego świadczenia usługi chmurowej.

Przykłady:

Poddostawcą będzie podmiot będący poddostawcą Dostawcy, prowadzący działalność centrum hostingowego (chmury w ścisłym tego słowa znaczeniu), w którym będzie zainstalowane i eksploatowane oprogramowanie oferowane Bankowi łącznie z usługą dostawy mocy obliczeniowej w ramach tego centrum.

Nie będzie poddostawcą jednak np. kontrahent centrum hostingowego odpowiadający za utrzymanie czystości, agencja ochrony mienia, a nawet wynajmujący – właściciel budynku.

Z kolei w zakresie 2. powyżej przez identyfikowany dostęp do informacji przetwarzanych przez Bank rozumieć należy taki dostęp, który spełnia następujące kryteria:

a. umożliwia poddostawcy identyfikację Banku jako zleceniodawcy,

b. dochodzi do ujawnienia przetwarzanych danych (informacji) w rozumieniu nadanym przez Komunikat,

przy czym to zapisy kontraktowe lub sposób skonfigurowania szyfrowania informacji powinny decydować o tym, czy podmiot posiada i w jaki sposób może wejść w posiadanie takiego identyfikowanego dostępu (np. gdy technicznie możliwy jest dostęp, natomiast umowa zakazuje wykorzystywania takiej możliwości).

Dodatkowo wskazać należy, że poddostawcą będzie firma współpracująca z Dostawcą, która ma logiczny, a nie fizyczny, dostęp do informacji przetwarzanych przez Bank.

Zasada proporcjonalności

Wyłącznie pomocniczo zamieszczamy wyjaśnienie zasady proporcjonalności, którego brak w Komunikacie. Zgodnie z Wytycznymi EBA, celem zasady proporcjonalności jest zapewnienie, aby zasady zarządzania, w tym te dotyczące outsourcingu, były spójne z indywidualnym profilem ryzyka, charakterem i modelem biznesowym instytucji lub instytucji płatniczej oraz skalą i złożonością jej działalności, tak aby skutecznie osiągnąć cele wymogów regulacyjnych.

Banki, w myśl zasady proporcjonalności, powinny uwzględniać złożony charakter funkcji zlecanych na zasadzie outsourcingu, ryzyko wynikające z umowy outsourcingu, krytyczne lub istotne znaczenie funkcji zlecanej na zasadzie outsourcingu oraz potencjalny wpływ outsourcingu na ciągłość wykonywanej działalności.

Banki, stosując zasadę proporcjonalności, powinny uwzględniać kryteria określone w tytule i wytycznych EUNB (EBA) w sprawie zarządzania wewnętrznego zgodnie z art. 74 ust. 2 dyrektywy 2013/36/UE.

Wydaje się również, że „proporcjonalność" może być utożsamiana z „adekwatnością" w zależności od całościowej sytuacji Banku.

Organizacja dokumentu

Standard został podzielony na rozdziały poświęcone regulacjom mającym wpływ na sposób implementacji usług chmury obliczeniowej w sektorze bankowym, przy czym:

1. w **Rozdziale 5** zacytowano zapisy poszczególnych sekcji Komunikatu chmurowego, wskazano, jakie są wymagania w stosunku do Banku i Dostawcy usług chmurowych w danym punkcie, jakie opracowania/produkty powinny powstać po każdej z zaangażowanych stron, a dodatkowo, tam, gdzie było to możliwe w formie odesłania, zaprezentowano przykładowy dokument/szablon, który może być wykorzystany przez Bank podczas przygotowania do wdrożenia usługi chmurowej;
2. w **Rozdziale 6** zacytowane zostały przepisy Prawa bankowego dotyczące tzw. outsourcingu bankowego wraz z odpowiednim komentarzem dostosowanym do sytuacji, gdy usługa chmury obliczeniowej stanowi jednocześnie taki outsourcing bankowy.

KAŻDY Z ROZDZIAŁÓW ZAWIERA (O ILE MA ZASTOSOWANIE):

1. zacytowanie w nagłówku **rozdziału danego punktu regulacji**,
2. podsumowanie opisu **wymagań** wynikających z danego punktu regulacji,
3. wskazanie **wymagań do zaadresowania (produktów do opracowania) po stronie Banku**, wynikających z zapisów wskazanych wymagań,
4. wskazanie **wymagań do zaadresowania (produktów do opracowania) po stronie Dostawcy**, wynikających z zapisów wskazanych wymagań oraz
5. wskazanie **szablonów/przykładów dokumentów/zestawień, które adresują niektóre z wymagań regulacji**.

Polish Cloud

Komunikat

Wytyczne stosowania

1. W celu zapewnienia prawidłowego funkcjonowania rynku finansowego, jego stabilności oraz bezpieczeństwa, na podstawie art. 4 ust. 1 ustawy o nadzorze nad rynkiem finansowym, Nadzór oczekuje od podmiotów nadzorowanych stosowania niniejszego modelu referencyjnego podczas działań związanych z przygotowaniem, realizacją oraz zakończeniem przetwarzania informacji w chmurze obliczeniowej, traktując go jako sprecyzowanie istniejących wymagań prawnych oraz bez uszczerbku dla tych wymagań, jeżeli:

   1) przetwarzane informacje należą do informacji prawnie chronionych w rozumieniu niniejszego komunikatu lub
   2) przetwarzanie informacji ma charakter outsourcingu szczególnego chmury obliczeniowej w rozumieniu niniejszego komunikatu

   i przetwarzanie informacji jest realizowane w chmurze obliczeniowej publicznej lub hybrydowej (w zakresie jej części opartej o chmurę obliczeniową publiczną).

2. Nadrzędnym zadaniem podmiotu nadzorowanego podczas przetwarzania informacji w chmurze obliczeniowej jest zapewnienie bezpieczeństwa przetwarzanych informacji oraz zgodności sposobu i zakresu tego przetwarzania z prawem. Stosowanie tego komunikatu powinno odbywać się z poszanowaniem zasady proporcjonalności przy równoległym uwzględnieniu modelu referencyjnego. Zasada proporcjonalności powinna znaleźć swoją konkretyzację na etapie szacowania ryzyka związanego z planowaniem czynności przetwarzania oraz adekwatnością stosowanych zabezpieczeń przetwarzanych informacji. UKNF podkreśla, że zasada proporcjonalności nie powinna być interpretowana jako przyzwolenie na zastosowanie przez mniejsze podmioty nadzorowane mniej efektywnych zabezpieczeń przetwarzanych informacji niż opisane w niniejszym komunikacie.
3. Nadzór podkreśla, że opisane w niniejszym komunikacje wymagania powinny być stosowane przez podmioty nadzorowane przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej.
4. W celu właściwego stosowania postanowień niniejszego komunikatu podmiot nadzorowany powinien określić dla każdej planowanej do wykorzystania lub wykorzystywanej usługi chmury obliczeniowej:

   1) czy przetwarzane są informacje prawnie chronione oraz
   2) czy czynność przetwarzania może być definiowana jako outsourcing szczególny chmury obliczeniowej.

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

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

OPIS WYMAGAŃ

1. Komunikat jest wiążący wyłącznie w stosunku do Banku. Dostawca i poddostawcy nie są związani wymogami Komunikatu chmurowego.
2. Komunikat musi być stosowany w dwóch przypadkach:
   a) przetwarzania Tajemnicy bankowej w ramach outsourcingu chmury obliczeniowej lub
   b) Outsourcingu szczególnego chmury obliczeniowej.

   W każdym innym przypadku Komunikat może być stosowany, jeśli Bank (również w porozumieniu z Dostawcą) tak postanowi.
3. Komunikat nie odnosi do chmury obliczeniowej prywatnej, w tym chmury obliczeniowej społecznościowej o charakterze prywatnym.
4. Bank określa typ przetwarzanych danych (informacji) dla danej usługi chmury obliczeniowej ze względu na Tajemnicę bankową oraz typ czynności ze względu na outsourcing szczególny chmury obliczeniowej.

5. W procesie analizy oraz klasyfikacji przetwarzanych danych, Bank powinien odwoływać się do istniejących w Banku zasobów inwentaryzacji procesów krytycznych, wynikających np. z BIA lub Rekomendacji H, dotyczącej systemu kontroli wewnętrznej w bankach, wydanej przez UKNF w kwietniu 2017 roku.
6. Jeśli usługi chmury obliczeniowej są wykorzystywane wyłącznie do przetwarzania danych (informacji) testowych (zanonimizowanych), Komunikatu się nie stosuje.
7. W toku prac nad Standardem zidentyfikowano jako szczególnie istotną kwestię stosowania Komunikatu do usług chmury obliczeniowej wykorzystywanej przez partnerów Banku na własne potrzeby. Przykładowo sytuacja taka dotyczy wykorzystywania przez partnera pakietu biurowego w formule chmury obliczeniowej. W związku z tym zagadnieniem, celem wypracowania sektorowego rozwiązania, ZBP zlecił zewnętrznej kancelarii prawnej przygotowanie opinii prawnej. Opinia prawna nie stanowi treści Standardu, jednakże jako powiązana ściśle z jego tematyką, w celach informacyjnych została załączona jako Dodatek do Standardu. Opinia dostępna jest również na stronie ZBP pod adresem https:/zbp.pl/Dla-Bankow/Bankowosc-elektroniczna/PolishCloud.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Dokument potwierdzający przeprowadzenie analizy w zakresie typu przetwarzanych danych (informacji), planowanej usługi chmury obliczeniowej oraz rodzaju czynności przetwarzania i jej kwalifikacji.
2. Dokument potwierdzający przeprowadzenie analizy w odniesieniu do wymagań outsourcingu szczególnego chmury obliczeniowej.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

Brak

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

Brak

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

OPIS WYMAGAŃ

1. Bank powinien opracować lub zaktualizować swoje procedury w zakresie klasyfikacji i oceny informacji, uwzględniając wymogi Komunikatu.
2. Bank powinien przeprowadzić klasyfikację i ocenę informacji dla danej usługi chmury obliczeniowej, zgodnie z przyjętymi w Banku procedurami.
3. Bank powinien na bieżąco monitorować zmiany wymogów prawnych oraz regulacyjnych w zakresie, który wymagałby ponownej klasyfikacji przetwarzanych informacji. Ponowna klasyfikacja przetwarzanych danych może być także wymagana w sytuacji, gdy rozszerzeniu ulega zakres dotychczasowej usługi chmurowej.
4. Bank powinien, nie rzadziej niż raz w roku, przeglądać i potwierdzać aktualność stosowanej klasyfikacji i oceny informacji w odniesieniu do bieżących warunków swojej działalności.
5. Bank powinien, nie rzadziej niż raz w roku, zweryfikować, czy usługa chmury obliczeniowej lub przetwarzane dane (informacje) nie są przetwarzane w CPD zlokalizowanym w innym regionie niż w momencie rozpoczęcia dostarczania usługi chmury obliczeniowej lub przetwarzania danych (informacji) w chmurze obliczeniowej, przy czym wystarczające jest tu oświadczenie Dostawcy zgodnie z właściwą reprezentacją lub umocowaniem. Bank powinien zapewnić sobie możliwość rozwiązania umowy na usługę chmury obliczeniowej w trybie natychmiastowym w przypadku, jeśli usługa chmury obliczeniowej lub przetwarzane dane (informacje) są przetwarzane w CPD zlokalizowanym w innym regionie niż w momencie rozpoczęcia dostarczania usługi chmury obliczeniowej lub przetwarzania danych (informacji) w chmurze obliczeniowej.
6. Właściwie przeprowadzony proces klasyfikacji informacji przetwarzanej w chmurze obliczeniowej pozwoli Bankowi właściwie wykonać analizę ryzyka, a w konsekwencji dobrać adekwatne mechanizmy oraz zidentyfikować narzędzia i procesy zapewniające należyty poziom bezpieczeństwa. Biorąc pod uwagę istotność procesu klasyfikacji informacji, Bank może wykorzystać listę pytań kontrolnych z Załącznika nr 2 „Klasyfikacja informacji" podczas oceny dojrzałości istniejących w Banku procesów, a ewentualne braki uzupełnić, wprowadzając stosowne zmiany do procesów i polityk.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowany proces klasyfikacji i oceny informacji przetwarzanych w chmurze obliczeniowej dla danej usługi chmury obliczeniowej.
2. Udokumentowane wyniki klasyfikacji danych (informacji), które powinny zostać uwzględnione w planie przetwarzania danych (informacji) w chmurze obliczeniowej dla danej usługi chmury obliczeniowej.
3. Udokumentowany standard klasyfikacji danych (informacji) stosowany przez Bank.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Poinformowanie Banku o planie zmiany miejsca przetwarzania danych (informacji) w chmurze obliczeniowej, jeśli taka zmiana ma nastąpić w stosunku do uzgodnień umowy zawartej między stronami.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

Załącznik nr 2 – Klasyfikacja informacji

VI Wytyczne do szacowania ryzyka

1. Podmiot nadzorowany prowadzi w udokumentowanym procesie kompleksowe szacowanie ryzyka (identyfikację, analizę oraz ocenę zagrożeń, możliwość ich wystąpienia oraz wpływ tego wystąpienia na podmiot nadzorowany), zgodnie z wymaganiami aktualnego wydania normy PN-ISO 27005 (Zarządzanie ryzykiem w bezpieczeństwie informacji) lub jej odpowiednika w europejskim systemie normalizacji, lub na bazie innego, usystematyzowanego podejścia. Szacowanie ryzyka jest prowadzone w sposób ciągły, z uwzględnieniem praktycznej implementacji zasady PDCA („plan – do – check – act").
2. Podmiot nadzorowany uwzględnia w procesie szacowania ryzyka, w kontekście wyników przeprowadzonej klasyfikacji i oceny przetwarzanych informacji w chmurze obliczeniowej, co najmniej:

   1) ogólne zagrożenia dla stosowania chmury obliczeniowej:

      a) rozproszenie geograficzne przetwarzanych informacji, w szczególności w kontekście zapewnienia zgodności procesu przetwarzania informacji z przepisami prawa, regulacjami wewnętrznymi, zobowiązaniami umownymi oraz deklaracjami i innymi uregulowaniami,

      b) możliwość utraty zgodności postępowania podmiotu nadzorowanego z przepisami prawa (w tym wydanych licencji lub zezwoleń) poprzez korzystanie z usług chmury obliczeniowej w sposób niezamierzony albo inny niż zamierzony,

      c) dostęp do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) Dostawcy usług chmury obliczeniowej,

      d) dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się fizycznie przetwarzanie (lokalizacja centrum przetwarzania danych), w szczególności odniesienie do katalogu sytuacji (lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu nadzorowanego, zarówno przez organy administracji krajowej, jak i międzynarodowej,

      e) brak zgodności technologicznej pomiędzy usługami różnych Dostawców chmury obliczeniowej powodujące przywiązanie do jednego Dostawcy usług chmury obliczeniowej poprzez ograniczenie albo brak możliwości przenoszenia (korzystania z identycznych) usług lub przetwarzanych informacji (vendor lock-in),

      f) awarie mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej,

      g) podatność interfejsów zarządzających usługami, które są udostępniane przez Dostawców usług chmury obliczeniowej,

h) ograniczona możliwość wpływania na zakres, kształt i zmiany usług, w tym w szczególności na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług przetwarzania,

i) ograniczona możliwość kontrolowania Dostawcy usług chmury obliczeniowej oraz jego poddostawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej,

j) podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy Dostawcę usług chmury obliczeniowej a podmiot nadzorowany;

2) specyficzne zagrożenia dla stosowanych konkretnych (nazwanych) usług chmury obliczeniowej:

a) możliwości korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego lub w środowisku, które nie podlega kontroli podmiotu nadzorowanego (np. prywatne urządzenia mobilne, dostęp z prywatnych lub publicznych sieci),

b) możliwości jednostronnej zmiany warunków technicznych korzystania z usługi (w szczególności jej parametrów lub zasad konfiguracji),

c) stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług, bez ich należytej weryfikacji i oceny adekwatności dla potrzeb podmiotu nadzorowanego,

d) stosowane mechanizmy uwierzytelniania oraz ich słabości;

3) specyficzne zagrożenia związane z zasobami podmiotu nadzorowanego:

a) wymagane i posiadane zasoby, w tym zasoby ludzkie o ustalonych kompetencjach,

b) zgodność technologiczna posiadanego środowiska teleinformatycznego oraz środowiska chmury obliczeniowej, a w szczególności mechanizmy integracji;

4) wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem;

5) stanowisko nadzoru w sprawie szyfrowania informacji, zgodnie z którym:

a) szyfrowanie informacji nie zmniejsza ważności informacji, nie zmienia też jej klasyfikacji i oceny,

b) szyfrowanie informacji oraz właściwe zarządzanie kluczami szyfrującymi zapobiega ujawnieniu informacji,

c) brak jest gwarancji dla uznania danego algorytmu szyfrowania za „całkowicie bezpieczny", nadzór zaleca więc używanie algorytmów szyfrowania, które – bazując na dostępnych publicznie informacjach (np. opracowaniach merytorycznych, raportach jednostek zajmujących się cyberbezpieczeństwem lub kryptografią) – nie są uznane za skompromitowane, zaś 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 jest to 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 jedynie w granicach szczególnych przepisów prawa regulujących działalność podmiotu nadzorowanego, przy czym nadzór krytycznie ocenia takie wyłączenia albo ograniczenia, jeżeli:

i. w ramach usługi chmury obliczeniowej przetwarzane są informacje prawnie chronione szyfrowane za pomocą kluczy szyfrujących dostarczonych lub zarządzanych przez Dostawcę usług chmury obliczeniowej lub jego poddostawcę lub

ii. przetwarzanie ma charakter outsourcingu szczególnego chmury obliczeniowej;

7) stanowisko nadzoru w sprawie usług (Dostawców usług chmury obliczeniowej), które są wykorzystywane do świadczenia własnych usług przez bezpośrednich dostawców podmiotów nadzorowanych, zgodnie z którym:

   a) podmiot nadzorowany powinien upewnić się, w jakim zakresie świadczona przez bezpośredniego Dostawcę usługa wykorzystuje usługi chmury obliczeniowej, a w szczególności czy dochodzi do przetwarzania informacji prawnie chronionej w usłudze chmury obliczeniowej,

   b) zależnie od faktycznego wykorzystania usług chmury obliczeniowej oraz zakresu przetwarzanych informacji podmiot nadzorowany powinien zapewnić, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień niniejszego komunikatu;

8) stanowisko nadzoru w sprawie prawa właściwego umowy pomiędzy Dostawcą usług chmury obliczeniowej a podmiotem nadzorowanym, zgodnie z którym:

   a) prawem właściwym dla umowy jest prawo polskie lub prawo innego państwa członkowskiego Unii Europejskiej, chyba że strony umowy poddadzą umowę prawu państwa trzeciego, a prawo państwa trzeciego pozwala na skuteczne wykonywanie:

      i. postanowień umowy,

      ii. wszystkich wymogów prawa polskiego ciążących na podmiocie nadzorowanym,

      iii. wytycznych organu nadzoru, w tym również w zakresie niniejszego komunikatu;

   b) w przypadku poddania umowy prawu państwa trzeciego podmiot nadzorowany powinien posiadać pisemną opinię prawną potwierdzającą, że zgodnie z wybranym prawem właściwym umowy wszystkie postanowienia umowy pomiędzy podmiotem nadzorowanym a Dostawcą usług chmury obliczeniowej spełniają wymagania prawa obowiązujące podmiot nadzorowany oraz wymagania niniejszego komunikatu;

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

3. Podmiot nadzorowany w procesie szacowania ryzyka powinien uwzględnić możliwość:

1) korzystania ze zweryfikowanych, aktualizowanych źródeł informacji o zagrożeniach specyficznych dla stosowania usług chmury obliczeniowej, w tym również w odniesieniu do konkretnych (nazwanych) usług;

2) korzystania z pomocy ze strony podmiotów lub osób o specjalistycznych kompetencjach zarówno w obszarze cyberbezpieczeństwa, jak i usług chmury obliczeniowej, szczególnie w sytuacji braku takich kompetencji wewnątrz własnej organizacji podmiotu nadzorowanego;

3) przeanalizowania dostępnych wyników audytów zewnętrznych dostawców usług chmury obliczeniowej w odniesieniu do usług chmury obliczeniowej oraz procesu zarządzania bezpieczeństwem informacji, poszerzając zakres analizy o dostępne certyfikaty wystawione Dostawcy usług chmury obliczeniowej potwierdzające spełnienie wymagań;

4) uprzedniego testowania usług chmury obliczeniowej, także przy wykorzystaniu scenariuszy warunków skrajnych, zarówno w zakresie sposobu działania usługi, jak i jej konfiguracji.

4. Podmiot nadzorowany, na podstawie wyników szacowania ryzyka, zarządza tym ryzykiem, uwzględniając w szczególności:

1) wymagania przepisów prawa, regulacji wewnętrznych oraz postanowień umownych;

2) stopień złożoności organizacyjnej, podział uprawnień i odpowiedzialności podmiotu nadzorowanego, zawarte porozumienia oraz analogiczne czynniki występujące w grupie kapitałowej lub organizacji grupowej, lub o charakterze stowarzyszenia, do których podmiot nadzorowany należy;

3) efektywność stosowanych mechanizmów kontrolnych i monitorujących, zwłaszcza w odniesieniu do:

   a) identyfikacji nowych zagrożeń;

   b) zmian w wykorzystywanej usłudze chmury obliczeniowej lub trybie i zakresie jej wykorzystywania;

   c) zmian w relacji z Dostawcą usług chmury obliczeniowej, w tym możliwość również nieplanowanego zakończenia współpracy zarówno przez podmiot nadzorowany, jak i Dostawcę usług chmury obliczeniowej;

4) kompetencje techniczne i zdolności organizacyjne podmiotu nadzorowanego, w szczególności w kontekście bezpiecznego wykorzystywania usług chmury obliczeniowej oraz realizacji postanowień umownych;

5) zdolność podmiotu nadzorowanego i zgodność z przepisami prawa do transferowania zidentyfikowanego ryzyka lub akceptacji oszacowanego poziomu ryzyka.

5. Wyniki szacowania ryzyka powinny dawać podstawę do twierdzenia, że świadczenie usługi chmury obliczeniowej będzie realizowane zgodnie z wymaganiami prawa obowiązującymi podmiot nadzorowany, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez podmiot nadzorowany standardami.

6. Wyniki szacowania ryzyka powinny zostać formalnie zatwierdzone oraz podlegać okresowej weryfikacji i aktualizacji. Zatwierdzenie powinno obejmować decyzję podmiotu nadzorowanego dotyczącą:

1) usług chmury obliczeniowej, z których podmiot nadzorowany będzie korzystał;

2) rodzaju i zakresu przetwarzanych w ramach tych usług informacji.

OPIS WYMAGAŃ

1. Bank powinien opracować lub zaktualizować swoje procedury w zakresie szacowania i oceny ryzyka, w zakresie korzystania z usług chmury obliczeniowej, uwzględniając przy tym wymogi Komunikatu.

2. Zgodnie z zapisami Komunikatu, dla danej usługi chmury obliczeniowej, Bank powinien przeprowadzić kompleksowe szacowanie ryzyka, biorąc pod uwagę wszelkie zidentyfikowane zagrożenia, ocenę prawdopodobieństwa ich wystąpienia oraz ewentualnego wpływu na Bank.

3. Komunikat wskazuje 21 zagrożeń w dwóch kategoriach: ogólne zagrożenia do stosowania chmury obliczeniowej oraz specyficzne zagrożenia do stosowanych konkretnych usług chmury obliczeniowej.

4. Wskazana w Komunikacie lista zagrożeń może być uzupełniona o dodatkowe zagrożenia, zidentyfikowane przez Bank, a mające potencjalny wpływ na korzystanie z usługi chmury obliczeniowej. W odpowiedzi na zapis w pkt 2 ppkt 9) Komunikatu, prezentujemy listę przykładowych zagrożeń i podatności, która została zawarta w Załączniku nr 3 „Lista przykładowych zagrożeń i podatności" do niniejszego opracowania.

5. Produktem prac nad Standardem 1.0 był załączony do tego dokumentu szablon arkusza szacowania ryzyka. Z uwagi na fakt, że wdrożenia usług opartych o chmurę obliczeniową mogą mieć znaczący wpływ na całą organizację, zasadne wydaje się przeprowadzanie analizy ryzyka w trzech wymiarach: prawnym, organizacyjnym i technicznym. Szablon arkusza szacowania ryzyka został uzupełniony, w stosunku do wersji załączonej do Standardu 1.0, o wskazane powyżej aspekty i stanowi Załącznik nr 4 „Szablon szacowania ryzyka" do niniejszego dokumentu.

6. W ramach prac zespołu nad niniejszym Standardem podjęto próbę interpretacji kilku wymagań, opisanych w Komunikacie, rozdział VI „Wytyczne do szacowania ryzyka", co do których pojawiły się wątpliwości wśród przedstawicieli banków, do których skierowano prośbę o wskazanie obszarów, jakie ich zdaniem powinny być doprecyzowane. Poniżej prezentujemy wskazane zapisy oraz ich interpretację.

   a) Pkt 2 ppkt 4) – Podmiot nadzorowany uwzględnia w procesie szacowania ryzyka […] wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem. Określenie „wartości" przetwarzanych informacji nie powinno być interpretowane jako wymóg oszacowania wartości pieniężnej danej informacji, gdyż w praktyce dokonywanie takiej ewaluacji wydaje się zbyt czasochłonne i kosztowne dla danego procesu wdrożenia usługi chmury obliczeniowej. Pojęcie „wartość" semantycznie powinno korespondować z pojęciem „ważność" również używanym w Komunikacie.

   b) Pkt 2 ppkt 6) – „Stanowisko Nadzoru w sprawie tworzenia łańcucha outsourcingowego". Jeśli usługa chmury obliczeniowej jest jednocześnie usługą stanowiącą outsourcing bankowy w rozumieniu art. 6a–6d Prawa bankowego, najdłuższym łańcuchem outsourcingowym jest jedynie następująca relacja: Bank – Dostawca – poddostawca. Więcej o tej relacji znajduje się w rozdziale 6 Standardu, Sekcja 6.1 (art. 6a Prawa bankowego) 2. (Podoutsourcing).

c) Jeśli usługa chmury obliczeniowej nie stanowi usługi outsourcingu bankowego w rozumieniu art. 6a–6d Prawa bankowego, możliwe są dowolnej długości łańcuchy outsourcingowe.

d) Jeśli usługa chmury obliczeniowej jest jednocześnie outsourcingiem bankowym w rozumieniu art. 6a–6d Prawa bankowego to poddostawcą w odniesieniu do takiej usługi jest w szczególności podmiot, który spełnia wymogi definicji „poddostawcy" z Komunikatu.

e) Kwalifikacja usługi chmury obliczeniowej jako usługi wymagającej stosowania Komunikatu będzie w przeważającej liczbie wypadków stanowiła jednocześnie usługę w ramach outsourcingu bankowego, o którym mowa w art. 6a–6d Prawa bankowego, do której w związku z tym będą miały zastosowanie zasady odpowiedzialności, w tym odpowiedzialność poddostawcy względem Dostawcy, szczegółowo opisane w rozdziale 6 Standardu, Sekcja 6.2 (art. 6b Prawa bankowego).

f) Możliwe jest istnienie usługi chmury obliczeniowej, która wymaga zastosowania Komunikatu, lecz nie stanowi outsourcingu bankowego. Usługa taka musiałaby mieć charakter outsourcingu szczególnego chmury obliczeniowej, w ramach którego nie są przetwarzane Informacje prawnie chronione, ani też nie dochodzi do powierzenia wykonywania czynności faktycznych związanych z działalnością bankową.

g) Na podstawie art. 6b Prawa bankowego oraz Komunikatu nie istnieje obowiązek nawiązania bezpośredniego stosunku prawnego pomiędzy Bankiem a poddostawcą Dostawcy, w związku z czym poddostawca Dostawcy nie ponosi odpowiedzialności kontraktowej względem Banku. Bezpośrednia odpowiedzialność poddostawcy za szkody powstałe wskutek niewykonania lub nienależytego wykonania umowy zaistnieje dopiero w przypadku podjęcia współpracy bezpośrednio z takim poddostawcą będącym jednocześnie np. dostawcą chmurowym.

h) Należy przy tym zwrócić uwagę, że UKNF w Q&A chmurowym wskazuje, że „w sytuacji, gdy podmiot nadzorowany, dokonując analizy ryzyka i jego oszacowania, stwierdzi, że poprzez relację umowną z dostawcą oprogramowania nie jest w stanie zagwarantować realizacji postanowień Komunikatu przez poddostawcę, podmiot nadzorowany powinien:

   i. nawiązać relację umowną z poddostawcą (dostawcą chmurowym) w celu realizacji postanowień Komunikatu (np. w formule umowy trójstronnej);

   ii. zrezygnować z usług świadczonych przez dostawcę oprogramowania, jeżeli niezależnie od formy relacji (np. umowa z poddostawcą) nie będzie możliwe zagwarantowanie wykonania postanowień Komunikatu".

i) UKNF krytycznie ocenia wyłączenia albo ograniczenia odpowiedzialności Dostawcy usług chmury obliczeniowej oraz jego poddostawców wobec podmiotu nadzorowanego, nawet jeśli znajdują się one w granicach szczególnych przepisów prawa, w następujących sytuacjach:

   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.

Biorąc pod uwagę powyższe oczekiwanie UKNF, decyzja o ewentualnej akceptacji ograniczeń odpowiedzialności (o ile dopuszczalna powszechnie obowiązującymi przepisami prawa) powinna być podjęta na podstawie rzetelnej oceny ryzyka wynikającego z takiego ograniczenia dla danej usługi chmury obliczeniowej. Przy po-

dejmowaniu ww. decyzji należy wziąć pod uwagę dopuszczalność akceptacji ograniczenia z punktu widzenia zarządzania bankiem oraz to, czy takie ograniczenie odpowiedzialności jest dla banku ekonomicznie akceptowalne.

j) Komunikat wymaga, aby szacowanie ryzyka dla danej usługi chmury obliczeniowej było przeprowadzone i udokumentowane w sposób zgodny z przyjętą przez Bank metodyką, zakładającą oczekiwany przez Nadzór proces ciągłego monitorowania ryzyka, związanego m.in. z wykorzystywaniem usług chmury obliczeniowej. Komunikat jako przykład udokumentowanego procesu podaje aktualne wydanie normy PN-ISO 27005 (Zarządzanie ryzykiem w bezpieczeństwie informacji) lub jej odpowiednika w europejskim systemie normalizacji, ale dopuszcza wykorzystanie innego, właściwego dla Banku, usystematyzowanego podejścia.

k) Zgodnie z wypracowaną w ramach prac nad niniejszą wersją Standardu interpretacją, punkty 5 i 6 Komunikatu chmurowego powinny być rozumiane następująco:

- **i.** Sposób zatwierdzania wyników szacowania ryzyka dla usługi chmury obliczeniowej powinien być wskazany w odpowiedniej polityce zarządzania ryzykiem bezpieczeństwa teleinformatycznego lub innym równoważnym dokumencie.
- **ii.** Wyniki szacowania ryzyka dla danej usługi chmury obliczeniowej powinny potwierdzać, że usługa będzie realizowana zgodnie z obowiązującymi przepisami prawa, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez Bank standardami działania. W związku z tym, dokument zawierający takie „wyniki szacowania ryzyka" obejmować powinien następujące oświadczenie: „Świadczenie usługi chmury obliczeniowej będzie realizowane zgodnie z wymaganiami prawa obowiązującymi Bank, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi standardami".
- **iii.** Formalne zatwierdzenie „wyników szacowania ryzyka" następuje w sposób właściwy dla akceptacji procesów ze względu na ich istotność lub znaczenie opisanych w odpowiednich dokumentach wewnętrznych danej organizacji. Dla procesów krytycznych lub istotnych przetwarzanych w usłudze chmury obliczeniowej może okazać się konieczna uchwała zarządu Banku.
- **iv.** Weryfikacja i aktualizacja następują według zasad właściwych dla przeglądania i potwierdzania aktualności stosowanej klasyfikacji i oceny informacji (przy czym obie te czynności przeprowadzić można jednocześnie/łącznie).

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowana analiza ryzyka dla danej usługi;
2. Udokumentowana ocena wartości przetwarzanych informacji dla danej usługi;
3. Udokumentowane dla danej usługi zastosowane metody szyfrowania informacji;
4. Udokumentowana procedura zarządzania kluczami szyfrującymi;
5. Udokumentowane potwierdzenie, że zastosowane w danej usłudze algorytmy szyfrowania nie są uznane za skompromitowane;
6. Udokumentowana ocena, że szyfrowanie w ramach danej usługi jest technologicznie możliwe i ekonomicznie zasadne;

7. Udokumentowana ocena tworzenia łańcucha outsourcingowego w ramach danej usługi;
8. Udokumentowane potwierdzenie, czy dostawca/dostawcy IT Banku wykorzystuje/wykorzystują usługi chmurowe;
9. Jeśli dotyczy, pisemna opinia prawna w przypadku poddania umowy z Dostawcą usługi chmurowej prawu państwa trzeciego;
10. Udokumentowana lista przeanalizowanych audytów zewnętrznych/certyfikatów wystawionych Dostawcy usług chmurowych;
11. Udokumentowany raport z testów dla danej usługi;
12. Udokumentowany opis mechanizmów kontrolnych i monitorujących stosowanych w Banku;
13. Opis kompetencji technicznych i zdolności organizacyjnych w kontekście wykorzystywania usług chmurowych oraz realizacji postanowień umownych;
14. Udokumentowane potwierdzenie zdolności i zgodności z przepisami prawa do transferowania zidentyfikowanego ryzyka lub akceptacji oszacowanego poziomu ryzyka;
15. Udokumentowane potwierdzenie, że świadczenie danej usługi będzie realizowane zgodnie z wymaganiami prawa, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi standardami;
16. Udokumentowana decyzja dotycząca korzystania z danej usługi.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

Dodatkowo, wychodząc naprzeciw oczekiwaniom Nadzoru w zakresie ciągłego monitowania wszystkich aspektów usługi chmurowej, a przede wszystkim: jakości świadczonej usługi, bezpieczeństwa przetwarzanych informacji oraz ryzyka związanego z usługą, w ramach prac nad niniejszą wersją Standardu opracowano propozycję podejścia do monitorowania umowy z Dostawcą usług chmury obliczeniowej. Dokument stanowi Załącznik nr 5 „Okresowe monitorowanie umów" do niniejszego opracowania.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

W procesie szacowania ryzyka Bank powinien uwzględnić informacje pozyskane od Dostawcy usługi chmurowej, w tym udokumentowane spełnienie wymagań/posiadanego stanu, w szczególności w zakresie:

1. Lokalizacji CPD, obszaru przetwarzania danych (lokalizacji Centrum Przetwarzania Danych Dostawcy, z których personel uzyskuje dostęp do danych Banku); dopuszczalne jest określenie tego na poziomie kraju/regionu (jednostki administracyjnej, rejonu Dostawcy);
2. Sposobu kontroli i monitorowania dostępu do przetwarzanych informacji przez personel Dostawcy i jego poddostawców;

3. Opisu mechanizmów izolacji zasobów używanych do świadczenia usługi chmury obliczeniowej wraz z informacją o potencjalnych skutkach awarii mechanizmów izolacji;
4. Dokumentacji interfejsów zarządzających usługą chmury obliczeniowej, informacji o zabezpieczeniach interfejsów i ew. o ich podatnościach;
5. Zasad żądania wprowadzania zmian w zakresie oferowanej usługi przez Dostawcę;
6. Możliwości kontrolowania Dostawcy oraz jego poddostawców, bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usługi chmury obliczeniowej;
7. Podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy Dostawcę i Bank;
8. Mechanizmów kontroli dostępu do usługi dla użytkowników, w szczególności metod ograniczenia dostępu z urządzeń prywatnych;
9. Możliwości integracji z innymi, wskazanymi przez Bank technologiami;
10. Stosu technologicznego w obszarze zapewnienia bezpieczeństwa środowiska, danych (informacji) oraz zasobów chmury obliczeniowej, w szczególności mechanizmów szyfrowania;
11. Łańcucha outsourcingowego oraz procesu kontroli i zapewnienia jakości usługi.

Przykładowy zestaw wymagań w stosunku do Dostawcy usług chmurowych znajduje się w dwóch załącznikach do niniejszego Standardu – „Ankiecie dla Dostawców usługi chmurowej" (Załącznik nr 7) oraz „Ankiecie dla Dostawców – udokumentowanie konfiguracji usługi" (Załącznik nr 8).

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik 1** – Lista produktów do opracowania po stronie Banku;
2. **Załącznik 3** – Lista przykładowych zagrożeń i podatności;
3. **Załącznik 4** – Szablon szacowania ryzyka;
4. **Załącznik 5** – Okresowe monitorowanie umów;
5. **Załącznik 7** – Ankieta dla Dostawców usługi chmurowej;
6. **Załącznik 8** – Ankieta dla Dostawców – udokumentowanie konfiguracji usługi;
7. **Załącznik 9** – Fazy projektu wdrożenia usługi chmurowej – materiał pomocniczy.

Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej

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

3. Zapewnienie kompetencji

3.1. Podmiot nadzorowany zapewnia w udokumentowanym procesie właściwe kompetencje dla planowanych lub prowadzonych działań przetwarzania informacji w środowisku chmury obliczeniowej. Kompetencje te zawierają wymagania w odniesieniu do wykształcenia, wyszkolenia, umiejętności i doświadczenia pracowników lub współpracowników podmiotu nadzorowanego zaangażowanych w proces planowania, realizacji, testowania i utrzymywania/przetwarzania informacji w chmurze obliczeniowej oraz zawierania i przeglądania umowy z tym związanej.

3.2. Podmiot nadzorowany zapewnia rozumienie konsekwencji stosowania określonej architektury chmury obliczeniowej, zasad konfiguracji, podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji, zależnie od zakresu i rodzaju planowanego lub stosowanego środowiska chmury obliczeniowej oraz modelu świadczonej usługi, z uwzględnieniem wymagań ciągłości działania podmiotu nadzorowanego oraz posiadanej infrastruktury teleinformatycznej. Rozumienie konsekwencji danego wyboru ma odniesienie w dokumentacji szacowania ryzyka, zapewnieniu właściwych zasobów zarówno pod względem jakościowym, jak i ilościowym oraz dodatkowo we wszystkich pracach (a także umowach) związanych z tworzeniem lub rozwojem oprogramowania przeznaczonego do używania w chmurze obliczeniowej oraz integracji usług bazujących na zasobach własnych podmiotu nadzorowanego.

3.3. Kompetencje pracowników lub współpracowników podmiotu nadzorowanego odpowiedzialnych za bezpieczeństwo oraz planowanie, konfigurację i zarządzanie oraz monitoring usług chmury obliczeniowej powinny być potwierdzone odpowiednią dokumentacją szkoleniową lub imiennymi zaświadczeniami w zakresie odpowiednim do używanych usług chmury obliczeniowej (lub wynikać z umiejętności i doświadczenia), w tym również specyficznych lub specyficznie konfigurowanych dla danego Dostawcy usług chmury obliczeniowej. Wymaganie

to odnosi się również do kompetencji osób odpowiedzialnych za przegląd lub weryfikację dokumentacji audytów, certyfikatów i innych dokumentów Dostawcy usług chmury obliczeniowej, w tym umowy na świadczenie usług chmury obliczeniowej oraz dokumentów o charakterze technicznym.

OPIS WYMAGAŃ

1. Bank, w celu zapewnienia bezpieczeństwa przetwarzanych w chmurze obliczeniowej informacji (lub co do których istnieje zamiar przetwarzania), powinien zapewnić właściwy poziom wiedzy i umiejętności pracowników i współpracowników, przy czym taki właściwy poziom wiedzy i umiejętności określa się co do zasady na podstawie wyników oszacowania ryzyka. Utrzymanie i systematyczne podnoszenie kwalifikacji (wiedzy i umiejętności) powinno być częścią dobrych praktyk Banku. W przypadku stwierdzenia ewentualnych braków należy je zaadresować poprzez stosowne szkolenia lub skorzystać ze wsparcia firm świadczących usługi konsultacyjno-doradcze w zakresie chmury obliczeniowej. Kompetencje pracowników i współpracowników powinny być udokumentowane, np. w formie certyfikatów szkoleniowych lub certyfikatów Dostawców.
2. Bank powinien określić role w organizacji wraz z zakresem głównych zadań podczas wdrożenia lub przy utrzymaniu rozwiązań chmurowych oraz dopasować do nich wymagane obszary kompetencji. Przykładowymi obszarami ról i dopasowanymi do nich kompetencjami w ramach wdrażania i utrzymania rozwiązań w publicznej chmurze obliczeniowej są:
   1) architektura (rola Architekt);
   2) bezpieczeństwo (rola Inżynier bezpieczeństwa);
   3) rozwój (role Developer, Inżynier DevOps);
   4) utrzymanie (role Administrator, Administrator sieci, Inżynier DevOps);
   5) biznes (rola Opiekun biznesowy usługi);
   6) finanse (rola Kontroler finansowy).
3. Role i dopasowane do nich kompetencje powinny zapewniać bezpieczeństwo, spójność architektoniczną oraz dostarczać odpowiednie wsparcie rozwiązań, a także rozliczalność i kontrolę finansową wykorzystywanych usług chmury obliczeniowej.
4. Bank w ramach utrzymania produkcyjnych systemów przetwarzających informacje w chmurze obliczeniowej powinien posiadać aktywne wsparcie Dostawców lub korzystać ze wsparcia firm świadczących usługi konsultacyjno-doradcze w zakresie chmury obliczeniowej.
5. Właściwy nadzór (ang. *governance*), pomaga uzyskać pewność, że wdrożone w chmurze obliczeniowej rozwiązania skutecznie adresują potrzeby biznesowe interesariuszy, zapewniając jednocześnie zgodność regulacyjną. Efektywny nadzór pomaga uzyskać równowagę między realizacją celów i minimalizacją ryzyka. W ocenie skuteczności prowadzonego przez Bank nadzoru pomocna może się okazać analiza odpowiedzi na pytania z Załącznika nr 10 „Nadzór (governance)", dotyczące uwzględnienia w nadzorze aspektów przetwarzania chmurowego.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane potwierdzenie zapewnienia kompetencji projektowych dla projektów chmurowych;
2. Udokumentowane potwierdzenie zapewnienia kompetencji związanych z zarządzaniem umowami z Dostawcami usług chmurowych;
3. Udokumentowana architektura chmury obliczeniowej dla danej usługi;
4. Udokumentowane zasady konfiguracji dla danej usługi;
5. Udokumentowany podział odpowiedzialności między Bank i Dostawcę danej usługi chmury obliczeniowej;
6. Udokumentowane potwierdzenie wykonania szkoleń/posiadania kompetencji w obszarze planowania, konfiguracji, zarządzania oraz monitoringu usług chmury obliczeniowej;
7. Udokumentowane potwierdzenie wykonania szkoleń/posiadania kompetencji w obszarze bezpieczeństwa usług chmury obliczeniowej;
8. Udokumentowane potwierdzenie wykonania szkoleń/posiadania kompetencji w obszarze przeglądu lub weryfikacji audytów, certyfikatów i innych dokumentów Dostawcy usług chmury obliczeniowej;
9. Udokumentowane potwierdzenie wykonania szkoleń/posiadania kompetencji w obszarze przeglądu lub weryfikacji umowy na świadczenie usług chmury obliczeniowej.

Uwaga 1: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

Uwaga 2: w Załączniku 11 „Wybrane definicje i pojęcia związane z bezpieczeństwem informacji" wyjaśnione zostały pokrótce wybrane definicje i pojęcia związane z bezpieczeństwem informacji.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Udokumentowane szkolenia, potwierdzone certyfikatami;
2. Udokumentowane wsparcie personelu Dostawcy na rzecz Banku.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik nr 10** „Nadzór (governance)".

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 RPO tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;

b) klarowną definicję i wskazanie lokalizacji przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;

c) prawo właściwe dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów);

d) potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;

e) własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu (wygaśnięciu, rozwiązaniu), także w sposób nieplanowany;

f) gwarancje, rękojmie, ubezpieczenia (polisy ubezpieczeniowe Dostawcy usług chmury obliczeniowej), kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej oraz zasad postępowania w takich sytuacjach, o ile ma to zastosowanie;

g) określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie) zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;

h) klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) Dostawcy usług chmury obliczeniowej oraz warunki nadawania praw dostępu do informacji przetwarzanych przez podmiot nadzorowany;

i) klarowne wskazanie zasad, zgodnie z którymi zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań poddostawców Dostawcy usług chmury obliczeniowej są transparentne i jasno identyfikowane przez podmiot nadzorowany;

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

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

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

m) prawo podmiotu nadzorowanego do przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji, w tym prawo do przeprowadzenia audytu 2-giej lub 3-ciej strony na zlecenie podmiotu nadzorowanego (o ile taka potrzeba wynika z szacowania ryzyka);

n) prawo dla nadzoru do wykonania obowiązków kontrolnych, w tym kontroli pomieszczeń i dokumentacji związanej z przetwarzaniem informacji podmiotu nadzorowanego, procesów i procedur, organizacji i zarządzania oraz potwierdzeń zgodności;

o) zasady licencjonowania (w tym prawo do aktualizacji bezpieczeństwa używanego oprogramowania lub jego komponentów) oraz prawa własności intelektualnej, w tym – jeżeli dotyczą – prawo do dysponowania przetwarzanymi informacjami;

p) zasady zmiany treści umowy, w tym parametrów technicznych używanych usług chmury obliczeniowej;

q) zasady rozwiązywania umowy, w tym zasady i terminy zwrotu lub usunięcia przetwarzanych informacji;

r) zasady wsparcia, w tym zakres i okna czasowe (z uwzględnieniem stref czasowych), tryb i sposób zgłaszania problemów z usługami chmury obliczeniowej;

s) zasady wymiany informacji, w tym w szczególności w zakresie bezpieczeństwa oraz zarządzania bieżącymi incydentami, obejmujące zarówno pracowników podmiotu nadzorowanego, jak i Dostawcy usług chmury obliczeniowej, a w przypadku istotnego narażenia na skutki danego incydentu – również innych stron (np. klientów, poddostawców), w celu zapewnienia adekwatności postępowania do poziomu istotności incydentu.

4.2. Bez uszczerbku dla wymagań prawa oraz z uwzględnieniem postanowień niniejszego komunikatu, podmiot nadzorowany może korzystać z ramowych umów udostępnianych przez Dostawców usług chmury obliczeniowej, w szczególności gdy dotyczą one usług chmury obliczeniowej tworzonych dla grupy podmiotów (w tym podmiotu nadzorowanego) w ramach umów o charakterze korporacyjnym lub grupowym, w tym również chmury obliczeniowej społecznościowej.

W takim przypadku podmiot nadzorowany powinien:

a) Zweryfikować, w jakim zakresie umowa ramowa oraz powiązane z nią dokumenty, wyniki szacowania ryzyka oraz wymagania prawne, organizacyjne i techniczne uwzględniają postanowienia niniejszego komunikatu oraz są adekwatne dla sytuacji podmiotu nadzorowanego i jego zamiarów związanych z przetwarzaniem informacji w chmurze obliczeniowej;

b) ocenić konieczność lub możliwość samodzielnego stosowania wymagań niniejszego komunikatu w zakresie, który nie jest zgodny z umową ramową i powiązanymi z nią dokumentami.

OPIS WYMAGAŃ

1. Bank jest zobowiązany do zawarcia pisemnej umowy z Dostawcą. Prawem właściwym dla umowy powinno być prawo polskie lub prawo innego państwa członkowskiego Unii Europejskiej, chyba że strony umowy poddadzą umowę prawu państwa trzeciego, a prawo państwa trzeciego pozwala na skuteczne wykonywanie:
   1) postanowień umowy;
   2) wszystkich wymogów prawa polskiego ciążących na Banku;
   3) wytycznych organu nadzoru, w tym również w zakresie Komunikatu.
2. Wydaje się, że w przypadku przetwarzania Tajemnicy bankowej w chmurze obliczeniowej oraz outsourcingu szczególnego, a zatem w dwóch przypadkach, gdy zawsze wymagane jest stosowanie Komunikatu, usługa chmury obliczeniowej stanowić będzie w zdecydowanej większości (a w przypadku przetwarzana Tajemnicy bankowej zawsze) outsourcing bankowy w rozumieniu art. 6a i nast. Prawa bankowego. Konieczne zatem będzie dodatkowo spełnienie wymogów nałożonych przepisami Prawa bankowego.
3. Zgodnie z Kodeksem cywilnym umowa ma formę pisemną, gdy jest zawarta na piśmie, przy czym oświadczenie woli złożone w formie elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym jest równoważne formie pisemnej.
4. W przypadku poddania umowy prawu państwa trzeciego Bank powinien posiadać pisemną opinię prawną potwierdzającą, że zgodnie z wybranym prawem właściwym umowy wszystkie postanowienia umowy pomiędzy Bankiem a Dostawcą spełniają wymagania prawa oraz wymagania Komunikatu, obowiązujące Bank.
5. Umowa z Dostawcą powinna zawierać te elementy (katalog zamknięty) lub wskazywać ich źródła wymienione w punkcie 4.1 powyżej, które są zasadne w odniesieniu do używanych usług i zakresu przetwarzanych informacji. Dodatkowo, zgodnie z punktem 4.2, Bank może korzystać z ramowych umów udostępnianych przez Dostawców, przy założeniu braku uszczerbku dla wymagań prawa oraz z uwzględnieniem postanowień Komunikatu. Objaśnienia do wybranych elementów umowy z Dostawcą wskazanych w punkcie 4.1 znajdują się w Załączniku nr 12 „Objaśnienia i lista wybranych klauzul wraz z przykładami".
6. W przypadku poddania umowy prawu państwa spoza EOG Bank powinien przeprowadzić analizę prawną dotyczącą możliwości skutecznego wykonywania postanowień umowy, wszystkich wymogów prawa polskiego ciążących na Banku oraz wytycznych organu nadzoru w zakresie Komunikatu.
7. Bank w ramach umowy z Dostawcami powinien mieć w jasny sposób określone wszystkie lokalizacje przetwarzania informacji zarówno u Dostawcy, jak i poddostawców.
8. Umowa pomiędzy Bankiem a jego Dostawcą powinna precyzować warunki oraz zasady dotyczące przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji. Dodatkowo takie samo doprecyzowanie powinno dotyczyć wszystkich poddostawców objętych klauzulą audytu 3-ciej strony.
9. Umowa z Dostawcą powinna zawierać jasno określone zasady usunięcia danych z urządzeń służących do przetwarzania informacji oraz ich backupu. Dostawca powinien uwzględniać również sytuacje, w których nośniki danych podlegają wymianie na skutek ich uszkodzenia.

10. Umowa z Dostawcą powinna zawierać jasno określone zasady zapewnienia kopii awaryjnych (backup) przetwarzanych informacji, w przypadku gdy podział odpowiedzialności przewiduje odpowiedzialność Dostawcy za zapewnienie kopii awaryjnych przetwarzanych informacji i taka potrzeba wynika z regulacji prawnych.

11. W ramach prac nad Standardem opracowano propozycję podejścia do monitorowania umowy z Dostawcą usług chmury obliczeniowej. Dokument stanowi Załącznik nr 5 „Okresowe monitorowanie umów" do niniejszego opracowania.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Umowa w formie pisemnej z Dostawcą wraz z niezbędnymi dokumentami (oświadczenia, regulaminy, warunki korzystania z usług itp.).

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Podpisanie umowy z Bankiem, uwzględniającej wymagania Komunikatu i bezwzględnie obowiązujące przepisy prawa.
2. Dostawca odpowiada za podpisanie umów ze swoimi poddostawcami, które gwarantują możliwość wykonania audytu przez Bank na podstawie umowy pomiędzy Bankiem a Dostawcą, w zakresie i na zasadach analogicznych do tych zdefiniowanych przez Bank wobec Dostawcy.
3. Dostawca powinien dostarczyć odpowiednie certyfikaty potwierdzające skuteczne usunięcie danych zgodnie z pkt 4.1.q) Komunikatu. Procedura usunięcia danych powinna również uwzględniać sytuacje, w których nośniki danych służące do przetwarzania informacji Banku będą utylizowane lub wykorzystywane wtórnie do innych celów.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik nr 5** Okresowe monitorowanie umów;
2. **Załącznik nr 12** Objaśnienia i lista wybranych klauzul wraz z przykładami.

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.

OPIS WYMAGAŃ

1. Bank w ramach bieżącego i planowanego przetwarzania informacji w chmurze obliczeniowej powinien posiadać udokumentowany plan przetwarzania informacji w chmurze obliczeniowej zgodnie z załącznikiem nr 13 „Plan przetwarzania informacji w chmurze obliczeniowej" do Standardu. Plan ten w szczególności powinien zawierać (najlepiej w postaci szczegółowej dokumentacji):
   1) opis zadania realizowanego za pomocą usługi chmury obliczeniowej;
   2) rodzaj (chronione, niechronione), klasę (publiczne, wewnętrzne, poufne) i typ (produkcyjne, testowe) przetwarzanych informacji, ze wskazaniem, czy przetwarzanie spełnia kryteria outsourcingu szczególnego chmury obliczeniowej;
   3) mechanizmy zabezpieczenia informacji (pseudonimizacja, anonimizacja), mechanizmy szyfrowania informacji, w tym zasady zarządzania i przechowywania kluczy szyfrujących oraz opis kontroli dostępu do informacji.
2. Plan powinien precyzyjnie określić, jakie dane (informacje) Bank, w ramach konkretnej inicjatywy, przetwarza w chmurze obliczeniowej.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowany Plan przetwarzania informacji w chmurze obliczeniowej dla danej usługi.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

Brak

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. Załącznik nr 13 „Plan przetwarzania informacji w chmurze obliczeniowej".

5.2. **[Testy]** Uruchomienie produkcyjne stosowania usług chmury obliczeniowej powinien poprzedzać okres testowy, podczas którego na danych testowych (generowanych maszynowo lub w inny przypadkowy sposób), w udokumentowanym procesie, testowane są scenariusze adekwatne do oszacowanego ryzyka.

OPIS WYMAGAŃ

1. Bank powinien przeprowadzić i udokumentować fazę testów usługi. Testy powinny być przeprowadzone na danych testowych; scenariusze testów powinny być adekwatne do oszacowanego ryzyka (zgodnie z rozdziałem VI Komunikatu – Wytyczne do szacowania ryzyka).

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane scenariusze testowe dla danej usługi.
2. Formalne wyniki testów dla danej usługi.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

Brak

SZABLONY/PRZYKŁADOWE DOKUMENTY/ZESTAWIENIA

Brak

5.3. **[Plan wycofania]** Podmiot nadzorowany posiada udokumentowany, przetestowany plan wycofania swojego zaangażowania w przetwarzanie informacji w usługach chmury obliczeniowej danego Dostawcy (również w sytuacji awaryjnej) bez uszczerbku dla zachowania zgodności swojego działania z wymaganiami prawa i innych regulacji, w tym w szczególności związanych z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.

OPIS WYMAGAŃ

1. Bank posiada plan wycofania się z usługi chmury obliczeniowej zarówno w sytuacji zmiany strategii, jak i w sytuacji awaryjnej.
2. Plan powinien zapewnić, że w sytuacji awaryjnej nie dojdzie do uszczerbku dla zachowania zgodności działania Banku z wymaganiami prawa i z innymi regulacjami, w tym związanymi z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.
3. Plan wycofania się z usługi może zakładać powrót do środowiska on-premise, migrację do innego Dostawcy lub inne uzasadnione biznesowo scenariusze.
4. Plan powinien być przetestowany, przy czym zakres i podejście do testów powinny wynikać z analizy ryzyka (zgodnie z rozdziałem VI Komunikatu – Wytyczne do szacowania ryzyka) i uwzględniać takie kwestie jak wolumeny danych, wymagane zasoby etc. Dokumentacja testowa powinna zawierać odpowiednie dowody audytowe, np. scenariusze testowe, oczekiwane wyniki, logi czy zrzuty z ekranu, potwierdzające fakt przeprowadzenia testów zgodnie z założeniami.
5. Bank powinien zadbać o odpowiednie wymagania certyfikowanego usunięcia danych zgodnie z opisem wymagań w pkt 4. Umowa z Dostawcą usług chmury obliczeniowej ppkt 4.1.q) Komunikatu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Plan wycofania się z danej usługi chmury obliczeniowej.
2. Scenariusze testowe i wyniki testów dla planu wycofania się z usługi chmury obliczeniowej w związku z zakończeniem umowy.
3. Scenariusze testowe i wyniki testów dla planu wycofania się z usługi chmury obliczeniowej w związku z sytuacją awaryjną.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Procedura i/lub wzór certyfikatu, potwierdzające skuteczne usunięcie danych zgodnie z opisem pkt 4. Umowa z Dostawcą usług chmury obliczeniowej, ppkt 4.1.q) Komunikatu.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik nr 14** Szablon scenariusza wyjścia z relacji z Dostawcą;
2. **Załącznik nr 15** Wyjście z chmury – główne zagadnienia.

5.4. **[Plan ciągłości działania]** Podmiot nadzorowany powinien posiadać udokumentowany plan ciągłości działania uwzględniający możliwość utraty kontroli nad przetwarzanymi informacjami u danego Dostawcy usług chmury obliczeniowej oraz możliwość przerwania ciągłości działania usługi. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej Dostawców usług chmury obliczeniowej podmiot nadzorowany regularnie weryfikuje własną zdolność do utrzymania deklarowanych założeń, w szczególności zgodność konfiguracji usług i odtwarzalności środowiska teleinformatycznego, zwłaszcza po zmianach technologicznych u jednego z Dostawców usług chmury obliczeniowej.

OPIS WYMAGAŃ

1. Bank powinien rozszerzyć posiadane plany ciągłości działania o scenariusz uwzględniający możliwość utraty kontroli nad przetwarzanymi informacjami u danego Dostawcy oraz możliwość przerwania ciągłości działania usługi chmury obliczeniowej.
2. Plan ciągłości działania może być oparty na różnych scenariuszach, w szczególności zakładać wykorzystanie środowiska on-premise, wykorzystanie innego Dostawcy lub tymczasową alternatywną realizację procesów (np. manualnie).
3. Bank może polegać na planach ciągłości działania po stronie Dostawcy pod warunkiem posiadania nadzoru nad działaniami Dostawcy w tym zakresie, tj. regularnej weryfikacji adekwatności planu oraz wyników testów planu ciągłości działania i planów awaryjnych (np. poprzez weryfikacje wyników niezależnych audytów, certyfikacje etc.).
4. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej Dostawców Bank powinien regularnie weryfikować możliwość realizacji tego scenariusza, zwłaszcza po zmianach technologicznych u jednego z Dostawców.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Plan ciągłości działania dla usługi chmury obliczeniowej, zawierający jako minimum opisane procesy i procedury w sytuacjach:
   1) możliwości utraty kontroli nad przetwarzanymi informacjami u danego Dostawcy;
   2) możliwości przerwania ciągłości działania usługi chmury obliczeniowej.
2. Dokumentacja związana z Planowaniem Ciągłości Działania zgodnie z metodyką przyjętą w Banku (zawierająca w szczególności wyniki testów ciągłości działania).
3. W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej Chmur obliczeniowych lub dwóch lub więcej Dostawców:
   1) dokumentacja weryfikacji możliwości realizacji tego scenariusza, np. przeprowadzenie testowej migracji próbki danych lub usług pomiędzy dwoma usługami chmury obliczeniowej;
   2) potwierdzenie przeprowadzania okresowej weryfikacji możliwości realizacji scenariusza z podpunktu powyżej, w szczególności dotycząca weryfikacji możliwości realizacji scenariusza po zmianach technologicznych u jednego z Dostawców.

Może okazać się konieczne zaangażowanie Dostawcy chmury do udziału w tworzeniu planu ciągłości działania, niezależnie od tego, że nie jest nawiązana z nim relacja umowna. UKNF zwraca uwagę, że w przypadku łańcucha outsourcingowego przewidzianego w rozdziale VI pkt 2 ppkt 7 Komunikatu, ryzyko związane z ciągłością działania związane jest z funkcjonowaniem dwóch podmiotów: Dostawcy usługi i Dostawcy chmury. Plan ciągłości działania, jakkolwiek możliwy do ujęcia w jednym dokumencie, powinien zatem obejmować przypadki utraty kontroli nad przetwarzanymi informacjami jako efekt zaistnienia zdarzeń dotyczących działalności jednego i drugiego Dostawcy. Powinien również uwzględniać sposób działania w przypadku jednoczesnego wystąpienia negatywnych zdarzeń po stronie Dostawcy usługi i Dostawcy chmury, co jest możliwe np. w sytuacji, kiedy oba podmioty należą do jednej grupy kapitałowej.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

Plan ciągłości działania.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

Brak

6. Wymagania dla Dostawców usług chmury obliczeniowej

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.

[...]

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

OPIS WYMAGAŃ

1. Bank, w zależności od oceny ryzyka, podejmuje decyzję o konieczności częściowego lub pełnego spełnienia przez Dostawcę:
   1) wskazanych w Komunikacie norm ISO;
   2) wymagań w zakresie CPD.
2. Bank akceptując odstępstwa od spełnienia wymogów wskazanych w Komunikacie norm, powinien udokumentować motywy takiego podejścia np. poprzez wskazanie, że zaakceptowane przez Bank CPD spełnia inne wymogi. Powyższe wymagania dotyczą zarówno przypadku podjęcia współpracy bezpośrednio z Dostawcą chmurowym, jak i dostawcą IT, który wykorzystuje chmurę obliczeniową do świadczenia usług na rzecz Banku.
3. Zakres ww. wymagań dla każdego wdrożenia powinien być przez Bank udokumentowany.

4. W zależności od decyzji Banku, Dostawca powinien zobowiązać się w umowie do zapewnienia zgodności usługi chmury obliczeniowej z ww. normami lub ich odpowiednikami (normami BS, normami PN-ISO etc.).
5. Zapewnienie zgodności może być realizowane poprzez uzyskanie przez Dostawcę niezależnej certyfikacji (wydanej przez jednostkę certyfikującą); w przypadku gdy Dostawca nie posiada formalnej certyfikacji, powinien on wykazać zgodność z ww. normami poprzez udokumentowanie realizacji poszczególnych wymagań norm.
6. Zakres certyfikacji powinien obejmować w całości usługę świadczoną na rzecz Banku, w szczególności zgodnie z punktem 6.2, wszystkie CPD, w których przetwarzane są dane (informacje) Banku.
7. Dokumentacja związana z certyfikacją, tj. certyfikat oraz wyniki audytów certyfikacyjnych lub dokumentacja zgodności dostarczona przez Dostawcę, powinny być przekazane przed zawarciem umowy oraz co najmniej raz w roku udostępniane Bankowi.
8. Bank powinien regularnie weryfikować dokumentację związaną z certyfikacją; w przypadku, gdy ww. dokumentacja wykaże istotne niezgodności, Bank powinien uzgodnić z Dostawcą plan naprawczy oraz monitorować jego realizację.
9. Aby w kompletny sposób podejść do oceny Dostawcy rozwiązania bazującego na usłudze chmurowej w kontekście wymagań Komunikatu chmurowego, w Załączniku nr 7 „Ankieta dla Dostawców usługi chmurowej" oraz Załączniku nr 8 „Ankieta dla Dostawców – udokumentowanie konfiguracji usługi" zaproponowano listę pytań, które należy uzgodnić z planowanym dostawcą rozwiązania, aby potwierdzić gotowość proponowanego rozwiązania/usługi w kontekście wspomnianych wymagań, a z którymi zgodność m.in. będzie musiał wykazać Bank przed UKNF, w celu uruchomienia przetwarzania chmurowego w ramach tego rozwiązania/usługi.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane wymagania Banku w zakresie norm i standardów, w szczególności dokumentacja akceptacji ryzyka w przypadku rezygnacji z wymagań.
2. Pozyskanie certyfikatu od Dostawcy lub innej dokumentacji zgodności Dostawcy z normami.
3. Udokumentowany proces regularnej oceny dokumentacji związanej z certyfikacją/ zgodnością.
4. Udokumentowany proces zarządzania planami naprawczymi uzgodnionymi z Dostawcą w przypadku istotnych niezgodności z normami.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Certyfikacja zgodnie z ww. normami, obejmująca zakresem usługę świadczoną na rzecz Banku, lub dokumentacja zgodności z ww. normami przygotowana przez Dostawcę.

Dokumenty certyfikacji oraz dokumentacja zgodności z ww. normami powinny być integralną częścią umowy podpisywanej z Bankiem.

2. Wymogi dotyczące certyfikacji powinny obejmować również poddostawców w sytuacji, kiedy w ich CPD przetwarzane są dane (informacje) Banku.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik nr 7.** Ankieta dla Dostawców usługi chmurowej;
2. **Załącznik nr 8.** Ankieta dla Dostawców – udokumentowanie konfiguracji usługi;
3. **Załącznik nr 16.** Szablon dokumentacji kontroli ISO27001;
4. **Załącznik nr 17.** Lista zagadnień dla wyboru Dostawców związanych z bezpieczeństwem.

6.3. **[Lokalizacja CPD]** 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 które wykorzystują usługę chmury obliczeniowej w zakresie realizacji usługi kluczowej lub

b) są operatorami infrastruktury krytycznej w rozumieniu ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym i którzy wykorzystują usługę chmury obliczeniowej w zakresie realizacji zadań operowania infrastrukturą krytyczną

powinny w pierwszej kolejności wykorzystywać CPD znajdujące się na terenie Rzeczypospolitej Polskiej, o ile – w ocenie podmiotu nadzorowanego – oferowane warunki umowne, ekonomiczne, operacyjne, SLA czy funkcjonalne są nie gorsze od CPD znajdujących się poza terytorium Rzeczypospolitej Polskiej.

OPIS WYMAGAŃ

1. Rekomendowany jest wybór Dostawców oferujących CPD na terenie EOG, co nie wyklucza możliwości przetwarzania danych (informacji) przez Dostawcę poza EOG.
2. Jeżeli usługa ma być świadczona w CPD na terenie EOG (lub w Polsce zgodnie z punktem 6.3.), Bank korzystający z usług globalnego Dostawcy powinien zdefiniować mechanizmy kontrolne zapewniające, że usługi, które wykorzystuje, są świadczone w CPD na terenie EOG (lub w Polsce zgodnie z pkt 6.3. powyżej).

3. W przypadku gdy CPD zlokalizowane jest na terenie EOG, ale usługa jest również wspierana przez personel mający dostęp (logiczny, a nie fizyczny, uniemożliwiający logiczny dostęp do danych) do danych (informacji) zlokalizowany poza EOG, wymagane jest zapewnienie zgodności z przepisami w tym zakresie (w szczególności wymagane jest uzyskanie zezwolenia KNF).
4. Podmioty będące operatorami infrastruktury krytycznej lub będące operatorami usługi kluczowej powinny preferować CPD znajdujące się na terenie Polski, o ile oferuje ono nie gorsze warunki (bezpieczeństwo, koszt, SLA itp.) niż usługi zlokalizowane poza Polską. W związku z tym, Banki będące ww. operatorami powinny przed wyborem Dostawcy zweryfikować dostępność analogicznej usługi korzystającej z CPD w Polsce i zapewnić udokumentowane porównanie tych usług – w szczególności porównując (szacując zgodnie z Komunikatem) ryzyko i koszty dla poszczególnych wariantów.
5. Wszystkie powyższe wymagania odnoszą się również do poddostawców (jeśli dotyczy).

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Jednoznaczne wskazanie lokalizacji CPD wykorzystywanych w usłudze. Jeżeli poszczególne usługi chmury obliczeniowej Dostawcy zlokalizowane są w różnych lokalizacjach CPD, należy wskazać lokalizację dla każdej z nich osobno.
2. Dla operatorów infrastruktury krytycznej lub operatorów usługi kluczowej (większość Banków) – dokumentacja lub mechanizmy kontrolne potwierdzające lokalizacje CPD w Polsce (jeśli dotyczy).
3. W przypadku, gdy uzasadniony jest wybór CPD poza EOG (lub poza Polską, zgodnie z punktem 6 Wymagania dla Dostawców usług chmury obliczeniowej, podpunkt 6.3. Komunikatu), udokumentowana analiza uzasadniająca taką decyzję (kwestie kosztów, ryzyka, operacyjne i/lub funkcjonalne lub ryzyka).

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Jednoznaczne wskazanie wszystkich lokalizacji CPD (kraj/region) wykorzystywanych w poszczególnych usługach (w formie oświadczenia Dostawcy).

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

Brak.

6.4. **[Dostęp do przetwarzanych informacji]** Dostawca usług chmury obliczeniowej zapewnia w swoim postępowaniu udokumentowaną zasadę ochrony przetwa-

rzanych przez podmiot nadzorowany informacji przed nieautoryzowanym dostępem lub użyciem przez swoich pracowników lub poddostawców poprzez co najmniej:

a) domyślną zasadę braku dostępu do przetwarzanych informacji podmiotu nadzorowanego;

b) domyślną zasadę braku konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego lub w innych uruchamianych usługach chmury obliczeniowej;

c) zasadę „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez podmiot nadzorowany (w tym również usunięcia usterek) oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. Obowiązujące w tym zakresie procedury obsługi mogą być dodatkowo potwierdzone stosownym certyfikatem (np. SOC 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji;

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

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

OPIS WYMAGAŃ

1. Dostawca powinien przedstawić dokumentację mechanizmów kontroli dostępu do danych (informacji) przetwarzanych w usłudze chmury obliczeniowej, w tym dla swoich pracowników (współpracowników) i poddostawców.
2. Dostawca nie powinien mieć stałego dostępu administracyjnego i serwisowego na poziomie urządzeń (serwerów, switchy, macierzy dyskowych etc.) ani oprogramowania stanowiącego element dostarczanej usługi dla Banku (platformy chmury obliczeniowej, baz danych, aplikacji etc.). Wszelkie czynności administracyjne i serwisowe powinny być logowane i audytowane.
3. Dostawca domyślnie nie powinien mieć żadnego dostępu do danych (informacji).
4. Dostawca powinien zagwarantować Bankowi odpowiednie mechanizmy kontroli i limitowanie praw dostępu jak opisane powyżej w odniesieniu do swoich poddostawców.
5. Dostęp do danych (informacji) dla Dostawcy powinien być nadawany tymczasowo na podstawie udokumentowanego żądania powiązanego z konkretnymi pracami administracyjnymi, rozwojowymi lub wsparciem użytkowników (zleconymi przez Bank).

6. Dostawca powinien przekazać dokumentację potwierdzającą separację tenantów oraz dokumentację mechanizmów zapewniających poprawność separacji, tak aby możliwa była okresowa weryfikacja konfiguracji. Separacja powinna być realizowana co najmniej na poziomie logicznym – na poziomie odpowiednich konfiguracji logicznych i uprawnień na platformie chmury obliczeniowej Dostawcy, bez możliwości dostępu do zasobów przynależnych do innych tenantów.
7. Nowo uruchamiane środowiska i/lub usługi powinny być domyślnie odseparowane od innych tenantów korzystających z chmury obliczeniowej Dostawcy (od momentu uruchomienia) i skonfigurowane zgodnie z najlepszymi praktykami bezpieczeństwa (hardening).

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Dokumentacja mechanizmów kontroli dostępu, przy założeniu, że jako minimum przyjęto:
   a) potwierdzenie domyślnego braku dostępu do danych (informacji), kont administracyjnych, serwisowych etc.;
   b) opis mechanizmów nadawania dostępu administracyjnego.
2. Potwierdzenie zasady „minimum koniecznego" przy dostępie serwisowym.
3. Dokumentacja mechanizmów separacji danych (informacji):
   a) wytycznych, wzorcowych konfiguracji, opisów zasad itp., które w jednoznaczny sposób definiują separację przetwarzania;
   b) wytycznych, wzorcowych konfiguracji, opisów zasad weryfikacji poprawności konfiguracji.
4. Dokumentacja konfiguracji bezpieczeństwa nowo uruchamianych serwerów i usług („secure-by-default").
5. Opcjonalnie, certyfikaty i dokumentacja certyfikacji (wyniki audytu itp.) w zakresie funkcjonowania mechanizmów kontroli dostępu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

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 podwykonawców 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 Bank (w tym również usunięcia usterek) oraz na czas ich trwania, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. Obowiązujące w tym zakresie procedury obsługi mogą być dodatkowo potwierdzone stosownym certyfikatem (np. SOC 2 Type 2) wydanym przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji;

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

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

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik nr 7** – Ankieta dla Dostawców usługi chmurowej;
2. **Załącznik nr 8** – Ankieta dla Dostawców – udokumentowanie konfiguracji usługi.

7. Kryptografia

7.1. Podmiot nadzorowany powinien zapewnić, że informacje przetwarzane w chmurze obliczeniowej są szyfrowane zgodnie z zasadami określonymi w niniejszym komunikacie. W szczególności podmiot nadzorowany powinien upewnić się, że:

a) posiada dostęp do szczegółowych i aktualnych instrukcji konfiguracji usług chmury obliczeniowej oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji;

b) zapewnia dostateczne kompetencje w celu realizacji poprawnej konfiguracji usług chmury obliczeniowej, zgodnie z wytycznymi Dostawcy usług chmury obliczeniowej, w tym pod kątem stosowania szyfrowania przetwarzanych informacji;

c) używa dedykowanych lub zalecanych przez Dostawcę usług chmury obliczeniowej ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług chmury obliczeniowej;

d) informacje prawnie chronione przetwarzane w chmurze obliczeniowej są szyfrowane zarówno „at rest", jak i „in transit".

OPIS WYMAGAŃ

1. Wymagane jest szyfrowanie informacji przetwarzanych w chmurze obliczeniowej. Mechanizmy i zakres wykorzystywania zabezpieczeń kryptograficznych powinny wy-

nikać z analizy ryzyka (zgodnie z rozdziałem VI pkt 2 ppkt 5 z ustępami Komunikatu). W szczególności wymagane jest:

1) szyfrowanie, zarówno podczas przesyłu, jak i podczas spoczynku („at rest" oraz „in transit") Tajemnicy bankowej;
2) przekazanie Bankowi przez Dostawców dokumentacji mechanizmów szyfrowania danych (informacji), a także mechanizmów weryfikacji poprawności konfiguracji i działania ww. mechanizmów;
3) posiadanie przez Bank kompetencji w zakresie poprawnej konfiguracji usług, w tym mechanizmów szyfrowania;
4) korzystanie przez Bank z zalecanych ustawień podnoszących bezpieczeństwo (tzw. hardening); ustawienia te powinny zostać udokumentowane.

2. Aby ułatwić Bankom i Dostawcom usług chmurowych odpowiednie przygotowanie kwestii dotyczących kryptografii, można skorzystać z listy pytań zawartych w Załączniku nr 18 „Kryptografia", które Bank powinien sobie zadać w celu oceny kompletności/gotowości tego aspektu bezpieczeństwa dla planowanego/realizowanego przetwarzania chmurowego w ramach usługi.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane potwierdzenie dostępu do instrukcji konfiguracji usług chmury obliczeniowej oraz metod weryfikacji poprawności ich konfiguracji i działania.
2. Udokumentowane potwierdzenie kompetencji w obszarze realizacji poprawnej konfiguracji zgodnie z wytycznymi Dostawcy usługi chmurowej.
3. Udokumentowane potwierdzenie używanych ustawień konfiguracyjnych dla danej usługi.
4. Udokumentowane potwierdzenie, że informacje prawnie chronione przetwarzane w danej usłudze są szyfrowane zarówno „at rest", jak i „in transit".

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Dokumentacja mechanizmów szyfrowania oraz metody weryfikacji poprawności konfiguracji szyfrowania.
2. Potwierdzenie posiadanych kompetencji – patrz rozdział VII pkt 3 Komunikatu.
3. Dokumentacja hardeningu usługi, w szczególności mechanizmów szyfrowania.
4. Potwierdzenie szyfrowania danych (informacji) w spoczynku i podczas przesyłu (dokumentacja techniczna, zrzuty ekranu etc.).

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik nr 18** – Kryptografia.

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.

[...]

7.4. Podmiot nadzorowany w udokumentowanym procesie zarządza tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz kontrolą tego procesu.

7.5. Proces zarządzania kluczami szyfrującymi powinien uwzględniać przechowywanie w ramach własnej infrastruktury kopii kluczy szyfrujących, które zostały wygenerowane lub są zarządzane przez Dostawcę usług chmury obliczeniowej i są używane w procesie outsourcingu szczególnego chmury obliczeniowej, chyba że z oszacowania ryzyka wynika uzasadniony brak takiej potrzeby.

OPIS WYMAGAŃ

1. Bank powinien zapewnić, że informacje są szyfrowane kluczami generowanymi oraz zarządzanymi przez Bank. Brak spełnienia tego wymogu powinien zostać poparty stosowną analizą ryzyka (patrz rozdział VII pkt 7 ppkt 7.2 Komunikatu).
2. Proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących powinien być udokumentowany i posiadać określone mechanizmy kontrolne.
3. W przypadku wykorzystania kluczy wygenerowanych lub zarządzanych przez Dostawcę Bank powinien zapewnić, że proces wspomniany w pkt 2 powyżej zapewnia przechowywanie kluczy w infrastrukturze Banku, chyba że analiza ryzyka dopuszcza brak takiego mechanizmu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Dokumentacja techniczna potwierdzająca, że informacje są szyfrowane kluczami generowanymi/ dostarczonymi oraz zarządzanymi przez Bank.

W przypadku gdy pkt 1 powyżej nie jest spełniony, analiza ryzyka, z której wynika dopuszczalność używania kluczy szyfrujących generowanych/dostarczonych i zarządzanych przez Dostawcę.

2. Sformalizowany (udokumentowany) proces (procedura) zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz przechowywaniem kopii zapasowych kluczy w infrastrukturze Banku.

W przypadku gdy proces zarządzania kluczami szyfrującymi nie zapewnia przechowywania kopii kluczy w infrastrukturze Banku, analiza ryzyka, z której wynika dopuszczalny brak takiej potrzeby.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

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

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

Brak

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

OPIS WYMAGAŃ

1. W zależności od wyników analizy ryzyka (rozdział VI Komunikatu, Wytyczne do szacowania ryzyka, pkt 2 ppkt 5 z ustępami) możliwe jest stosowanie HSM. HSM może być udostępniony przez Dostawcę lub być zarządzany przez Bank. Bez względu na to, która strona udostępnia HSM, musi on spełniać wymagania FIPS 140-2 Level 2 lub równoważne.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Dokumentacja wykorzystywanych HSM potwierdzająca spełnienie wymagania FIPS 140-2 Level 2 lub równoważnego (w szczególności FIPS 140-3, który jest następcą wymagań FIPS 140-2).

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Jak wyżej, w przypadku gdy HSM jest udostępniony przez Dostawcę.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

Brak

8. Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej

8.1. Podmiot nadzorowany posiada udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej, stosownie do zakresu używanych usług chmury obliczeniowej, przetwarzanych informacji i wyników szacowania ryzyka.

8.2. Podmiot nadzorowany zabezpiecza logi przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa wynikającymi z szacowania ryzyka oraz obowiązującymi przepisami szczegółowymi w tym zakresie.

8.3. Uprawniony personel podmiotu nadzorowanego dokonuje przeglądu logów zgodnie z udokumentowanymi procedurami i zasadami bezpieczeństwa, przy czym – zależnie od skali działania, rodzaju i liczby logowanych zdarzeń oraz architektury bezpieczeństwa – Nadzór zaleca używanie specjalistycznego oprogramowania do korelowania zapisów ze zdarzeń (SIEM) oraz regularny przegląd i aktualizację reguł korelacji.

OPIS WYMAGAŃ

1. Istotnym elementem związanym z wykorzystaniem usług chmury obliczeniowej jest kwestia monitorowania środowiska przetwarzania informacji w usłudze.
2. Zgodnie z wytycznymi Komunikatu, w zakresie monitorowania środowiska przetwarzania informacji w usłudze chmury obliczeniowej Bank powinien:
   1) posiadać udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej, stosownie do zakresu używanych usług chmury obliczeniowej, przetwarzanych informacji i wyników szacowania ryzyka;
   2) zabezpieczać logi przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa wynikającymi z szacowania ryzyka oraz obowiązującymi przepisami szczegółowymi w tym zakresie;

3) w zależności od skali działania, ilości logów itp. rozważyć przekazywanie logów z chmury obliczeniowej do systemu SIEM oraz opracowanie reguł korelacji pozwalających na wykrycie incydentu bezpieczeństwa w chmurze obliczeniowej.

3. Monitorowanie może odbywać się na różnych poziomach stosu technologicznego, przy czym istotne jest spojrzenie na ten aspekt w dwóch perspektywach – platformowej oraz aplikacyjnej, które mogą różnić się zakresem odpowiedzialności realizowanych działań przez zaangażowane podmioty (Bank, Dostawca rozwiązania, Dostawca usług przetwarzania w chmurze) oraz zakresem informacji logowanych przez narzędzia do monitorowania. Ze względu na fakt, iż logi mogą również zawierać informacje będące Tajemnicą bankową, w ramach analizy wymagań związanych z systemem monitorowania pomocne może być uwzględnienie pytań zawartych w Załączniku nr 19 „Monitorowanie".

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane zasady zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej.
2. Udokumentowana procedura zabezpieczania logów dla danej usługi.
3. Udokumentowane potwierdzenie dokonania przeglądu logów w ramach danej usługi.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Dokumentacja w zakresie logowania zdarzeń w chmurze obliczeniowej, a także możliwości integracji mechanizmów logowania w chmurze z systemem SIEM wykorzystywanym w Banku.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik nr 19** – Monitorowanie

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

a) podmiot nadzorowany zapewnia, że wyłącznie uprawniony personel Dostawcy usług ma dostęp do wskazanych systemów teleinformatycznych lub ich wybranych zakresów;

b) podmiot nadzorowany wymaga używania przez personel Dostawcy usług uwierzytelnienia MFA, przy czym rodzaj i zakres uzależniony jest od wyników szacowania ryzyka;

c) podmiot nadzorowany zapewnia, że dostęp administracyjny lub o charakterze uprzywilejowanym realizowany jest z zaufanych sieci podmiotu nadzorowanego lub Dostawcy usług i pod kontrolą (w tym np. poprzez nagrywanie sesji i jej parametrów, a następnie poprzez analizowanie prawidłowości i celowości realizowanych czynności), chyba że z szacowania ryzyka wynika uzasadniony brak takiej potrzeby.

OPIS WYMAGAŃ

1. Bank powinien zapewnić poprzez mechanizmy kontrolne lub zapisy umowne, że dostęp do systemów wykorzystywanych w usłudze chmury obliczeniowej ma wyłącznie uprawniony personel po stronie Dostawcy.
2. Dostęp personelu Dostawcy usług do systemów wykorzystywanych w chmurze obliczeniowej powinien być zabezpieczony przez silne, wieloskładnikowe uwierzytelnienie.
3. Personel Dostawcy powinien uzyskiwać dostęp wyłącznie z bezpiecznych stacji roboczych/terminali, zlokalizowanych w bezpiecznej (zaufanej) lokalizacji sieciowej.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowane procedury lub zapisy umowne potwierdzające ograniczenie dostępu wyłącznie do uprawnionego personelu Dostawcy z bezpiecznych lokalizacji sieciowych i stacji roboczych/terminali.
2. Opis mechanizmów uwierzytelnienia.
3. Udokumentowane procedury okresowej weryfikacji dostępu Dostawcy do systemów wykorzystywanych w usłudze.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Używanie przez personel Dostawcy, mający dostęp zdalny do środowiska chmury obliczeniowej Banku, uwierzytelnienia MFA oraz bezpiecznych stacji w bezpiecznych lokalizacjach sieciowych.

2. W zależności od wyników analizy ryzyka przeprowadzanej przez Bank, określenie innych mechanizmów zapewniających monitorowanie dostępu i rozliczalność działań Dostawcy, np. nagrywanie sesji i jej parametrów w przypadku dostępu administracyjnego Dostawcy lub dostępu personelu Banku o charakterze uprzywilejowanym.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

Brak

9. Dokumentowanie działań podmiotu nadzorowanego

9.1. Tam, gdzie jest to zasadne, zależnie od zakresu i rodzaju przetwarzanych informacji, zasad i regulacji obowiązujących i przyjętych w organizacji (z uwzględnieniem powiązań korporacyjnych i grupowych, jeżeli występują) oraz wyników szacowania ryzyka i przy uwzględnieniu zasady proporcjonalności, podmiot nadzorowany posiada dokumentację zawierającą:

a) organizację pracowników lub współpracowników odpowiedzialnych za cyberbezpieczeństwo, w tym stanowisk lub funkcji związanych z monitorowaniem, analizowaniem i raportowaniem incydentów związanych z informacjami przetwarzanymi w chmurze obliczeniowej, wraz z opisanymi wymaganymi kompetencjami, uprawnieniami i odpowiedzialnościami;

b) architekturę sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych podmiotu nadzorowanego z sieciami niezaufanymi, w tym architekturę rozwiązania w chmurze obliczeniowej, także z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych;

c) zasady kategoryzacji informacji lub systemów pod kątem przetwarzania w chmurze obliczeniowej lub odniesienie do obecnie funkcjonujących klasyfikacji, jeżeli mogą być stosowane;

d) zasady stosowanych zabezpieczeń technologicznych i rozwiązań organizacyjnych;

e) zasady zarządzania ciągłością działania;

f) zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z Dostawcą usług chmury obliczeniowej;

g) zasady zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi;

h) zasady przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem usług chmury obliczeniowej;

i) zasady raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej;

j) umowy z Dostawcami usług chmury obliczeniowej wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań;

k) procesy, procedury lub instrukcje dotyczące:

i. analizy zagrożeń i szacowania ryzyka, w tym źródła pozyskiwania informacji o zagrożeniach specyficznych dla stosowanych usług chmury obliczeniowej oraz sektora finansowego;

ii. zarządzania środowiskiem teleinformatycznym (sieciami, systemami, aplikacjami, bazami danych itp.), z uwzględnieniem usług chmury obliczeniowej, w tym planowanie, rozwój i utrzymywanie;

iii. zarządzania logami;

iv. zarządzania kluczami szyfrującymi;

v. zarządzania incydentami bezpieczeństwa;

vi. przeprowadzania audytów wewnętrznych bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej.

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

OPIS WYMAGAŃ

Rozdział VII pkt 9 Komunikatu określa wymogi organizacyjne i dokumentacyjne, które Bank powinien posiadać (np. w charakterze polityk lub innych regulacji), chcąc wdrażać usługi chmury obliczeniowej.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

1. Udokumentowanie organizacji pracowników lub współpracowników Banku odpowiedzialnych za cyberbezpieczeństwo, z uwzględnieniem elementów z pkt 9 a).
2. Udokumentowanie architektury sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych Banku z sieciami niezaufanymi, w tym architektury wdrażanego rozwiązania w chmurze obliczeniowej z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych.
3. Udokumentowanie zasad kategoryzacji informacji lub systemów pod kątem przetwarzania w chmurze.
4. Udokumentowane zasady (polityka) stosowanych w organizacji zabezpieczeń technologicznych i rozwiązań organizacyjnych w odniesieniu do rozwiązań w chmurze obliczeniowej.

5. Udokumentowane zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z Dostawcą usług chmury obliczeniowej.
6. Udokumentowane zasady (polityka) zarządzania ciągłością działania.
7. Dla wdrażanej usługi chmury obliczeniowej, udokumentowane zasady bieżącego zabezpieczania przetwarzanych informacji, jak również dla sytuacji planowanego lub nieplanowanego zakończenia współpracy z Dostawcą.
8. Udokumentowane zasady (polityka) zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi.
9. Udokumentowane zasady (polityka) przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem Chmury obliczeniowej (np. coroczny przegląd).
10. Udokumentowane zasady (polityka) raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej.
11. Umowa z Dostawcą wraz z dodatkowymi oświadczeniami, jeżeli to konieczne dla potwierdzenia spełnienia wymagań.
12. Udokumentowane zasady analizy zagrożeń i szacowania ryzyka dla stosowanych usług chmury obliczeniowej.
13. Udokumentowane zasady zarządzania środowiskiem teleinformatycznym, z uwzględnieniem usług chmury obliczeniowej.
14. Udokumentowane zasady zarządzania incydentami bezpieczeństwa.
15. Udokumentowane zasady przeprowadzania audytów wewnętrznych bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej.
16. Udokumentowane zasady zarządzania politykami i dokumentacją w ramach systemu zarządzania organizacją, zapewniające ochronę przed nieuprawnionym dostępem, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

1. Udokumentowanie architektury rozwiązania w chmurze obliczeniowej, z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych.

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik nr 1** – Lista produktów do opracowania po stronie Banku;
2. **Załącznik nr 7** – Ankieta dla Dostawców usługi chmurowej;
3. **Załącznik nr 8** – Ankieta dla Dostawców – udokumentowanie konfiguracji usługi.

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

1. W przypadkach outsourcingu szczególnego chmury obliczeniowej lub przetwarzania informacji prawnie chronionej podmiot nadzorowany w terminie 14 dni przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej (a w przypadku, gdy przetwarzanie to już jest realizowane – nie później niż 1 sierpnia 2020 r.) informuje UKNF o:

1) rodzaju i zakresie informacji planowanych do przetwarzania/przetwarzanych w chmurze obliczeniowej;
2) nazwie Dostawcy usług chmury obliczeniowej oraz rodzaju planowanych do używania/używanych usług chmury obliczeniowej;
3) dacie podpisania umowy z Dostawcą usług chmury obliczeniowej oraz terminach jej obowiązywania, a w przypadku gdy umowa nie jest jeszcze zawarta – przewidywaną datę jej zawarcia;
4) lokalizacji (kraj, region albo inne równoważne) centrum przetwarzania danych (CPD) świadczącym usługę chmury obliczeniowej;
5) spełnieniu wymagań opisanych w niniejszym komunikacie;
6) osobach lub stanowiskach do kontaktu w sprawie stosowania chmury obliczeniowej w podmiocie nadzorowanym.

2. Powyższa informacja powinna zostać podpisana przez uprawnionego przedstawiciela podmiotu nadzorowanego oraz dostarczona do UKNF przy wykorzystaniu formularza stanowiącego załącznik nr 1 do niniejszego komunikatu.

OPIS WYMAGAŃ

1. Komunikat wymaga poinformowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej wyłącznie w dwóch przypadkach:
   i. usługi chmury obliczeniowej stanowią outsourcing szczególny lub
   ii. w chmurze obliczeniowej przetwarzana jest Tajemnica bankowa.
2. Zgłoszenia należy dokonać 14 dni przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej, co oznacza, że znaczenia nie ma samo zawarcie umowy outsourcingowej, ale przekazanie danych (informacji) do Dostawcy, w tym objętych Tajemnicą bankową (bez względu na to, czy w fazie przedprodukcyjnej, czy już w fazie produkcyjnej).
3. Uprawnionym do podpisania informacji, o której mowa w rozdziale VIII Komunikatu, jest zarówno zarząd Banku (zgodnie z reprezentacją w KRS), jak i osoby właściwie przez zarząd umocowane. Decyzja może mieć formę uchwały zarządu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE BANKU

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

Uwaga: pełna lista produktów do opracowania po stronie Banku, bazująca na wszystkich rozdziałach Komunikatu, znajduje się w Załączniku nr 1 „Lista produktów do opracowania po stronie Banku" do niniejszego Standardu.

WYMAGANIA DO ZAADRESOWANIA/ PRODUKTY DO OPRACOWANIA PO STRONIE DOSTAWCY

Brak

SZABLONY/PRZYKŁADY DOKUMENTÓW/ZESTAWIENIA

1. **Załącznik 21** – Przykład notyfikacji do UKNF

Prawo Bankowe

Poniższy komentarz do przepisów Prawa bankowego dotyczy wyłącznie sytuacji, gdy usługa chmury obliczeniowej stanowi jednocześnie outsourcing bankowy w rozumieniu art. 6a i nast. Prawa bankowego (na potrzeby niniejszego rozdziału 6 „Outsourcing bankowy"). Jak już wskazano w niniejszym Standardzie (oraz tak długo, jak UKNF nie wypowie się odmiennie w tej sprawie), usługa chmury obliczeniowej, na podstawie której dochodzi do przetwarzania Tajemnicy bankowej, stanowi zawsze outsourcing bankowy. Jeśli zaś chodzi o outsourcing szczególny, to do outsourcingu bankowego dochodzić będzie w większości przypadków.

Art. 6a Prawa Bankowego

1. UMOWA OUTSOURCINGU BANKOWEGO

1. Umowa o świadczenie usługi chmury obliczeniowej jest umową outsourcingu bankowego, zawsze gdy spełnia którekolwiek z poniższych kryteriów:
   1) jej przedmiotem jest realizacja czynności wskazanych w art. 5 oraz art. 6 Prawa bankowego i polega na świadczeniu usług wskazanych w art. 1 ust. 1) od a) do j) Prawa bankowego (umowa agencyjna) lub
   2) jej przedmiotem jest realizacja powierzonych przez Bank czynności faktycznych związanych z działalnością Bankową (art. 6a ust 1 pkt 2) Prawa bankowego) lub
   3) w ramach jej realizacji Dostawca lub jego poddostawcy będą mieli dostęp do Tajemnicy bankowej.
2. Umowa o świadczenie usługi chmury obliczeniowej stanowi umowę agencyjną uregulowaną przepisami Kodeksu cywilnego od art. 758 do art. 764(9), jeśli dotyczy czynności wskazanych w art. 5 oraz art. 6 Prawa bankowego i polega na świadczeniu usług wskazanych w art. 1 ust. 1) od a) do j) Prawa bankowego (art. 758 § 1 Kodeksu cywilnego: „Przez umowę agencyjną przyjmujący zlecenie (agent) zobowiązuje się, w zakresie działalności swego przedsiębiorstwa, do stałego pośredniczenia, za wynagrodzeniem, przy zawieraniu z klientami umów na rzecz dającego zlecenie przedsiębiorcy albo do zawierania ich w jego imieniu");
3. Jeśli umowa outsourcingowa dotyczy innych czynności niż wskazane w pkt 1.3. powyżej, stanowi umowę nienazwaną opartą o zasadę swobody umów (zwykle umowę o świadczenie usług). W takiej sytuacji będzie najczęściej stanowić powierzenie realizacji czynności faktycznych związanych z działalnością Bankową (art. 6a ust. 1 pkt 2) Prawa bankowego).
4. Umowa outsourcingowa w rozumieniu art. 6a Prawa bankowego powinna być zawsze zawarta na piśmie (co do wymogu pisemności zob. szerzej uwagi do Wymogów dla umowy).
5. Umowy outsourcingu w rozumieniu art. 6a Prawa bankowego będą wymagały dodatkowo zezwolenia KNF, gdy usługi chmury obliczeniowej polegać będą na wykonywaniu w imieniu i na rzecz Banku pośrednictwa w zakresie czynności wymienionych w art. 5 i 6 Prawa bankowego, polegającego na wykonywaniu innych czynności, niż te opisane w art. 6a ust. 1 pkt 1) lit. a–l.
6. Zezwolenie KNF jest również konieczne w przypadku tzw. outsourcingu zagranicznego – szczegółowy komentarz do art. 6d Prawa bankowego poniżej.

2. PODOUTSOURCING

1. Dla usług chmury obliczeniowej kwalifikujących się jako outsourcing w rozumieniu art. 6a–6d Prawa bankowego możliwość podoutsourcingu jest uregulowana w Prawie bankowym i Komunikacie:
   1) podoutsourcing łańcuchowy w rozumieniu art. 6a ust. 7 Prawa bankowego dopuszczalny jest wyłącznie jeden poziom w dół, tj. Bank – Dostawca – poddostawca;
   2) w celu weryfikacji, czy występuje podoutsourcing łańcuchowy wykraczający poza art. 6a ust. 7 Prawa bankowego, w szczególności wykorzystać można definicję „poddostawcy" w rozumieniu Komunikatu. Definicja ta omówiona jest szczegółowo w pierwszej części Standardu. Dalsze powierzenie czynności niespełniające kryteriów podoutsourcingu łańcuchowego w rozumieniu art. 6a ust. 7 Prawa bankowego nie jest limitowane;
   3) wymagana jest zgoda Banku na podoutsourcing w umowie na usługi chmury obliczeniowej, a umowa powinna określać zasady zaangażowania podwykonawców; oraz
   4) podoutsourcing nie może dotyczyć całości przedmiotu usługi, możliwość podoutsourcingu dotyczy tylko czynności pomocniczych i technicznych potrzebnych do realizacji usługi chmury obliczeniowej.

KOMENTARZ

1. Warto zaznaczyć, że zgodnie z sugestią UKNF w ramach Q&A Chmurowego, w celu ograniczenia ryzyka niedozwolonego podoutsourcingu łańcuchowego, Bank może nawiązać relację umowną z poddostawcą w formule umowy trójstronnej.
2. Umowy z Dostawcami ze względu na przedmiot świadczonej usługi będą w przeważającej mierze umowami nienazwanymi niewymagającymi zezwolenia KNF (z zastrzeżeniem dalszych komentarzy), które polegać będą na świadczeniu czynności faktycznych związanych z działalnością bankową.
3. Wyjaśnienie pojęcia czynności faktycznych związanych z działalnością bankową wskazanych w art. 6a ust 1. pkt 2) Prawa bankowego: przez czynności faktyczne rozumie się wszystkie czynności, które nie są czynnościami bankowymi wskazanymi w art. 5 oraz art. 6 Prawa bankowego, lecz pozostają z nimi w bezpośrednim i funkcjonalnym związku.

Art. 6b Prawa Bankowego

3. ODPOWIEDZIALNOŚĆ W RAMACH UMOWY NA USŁUGI CHMURY OBLICZENIOWEJ

1. Odpowiedzialność Dostawcy względem Banku:
   1) Pełna odpowiedzialność wobec Banku za szkody wyrządzone klientom za niewykonanie lub nienależyte wykonanie umowy na usługę chmury obliczeniowej. **Nie można wyłączyć ani ograniczyć.**

2) Możliwość modyfikacji polegającej jedynie na rozszerzeniu takiej odpowiedzialności (odpowiedzialność na zasadzie ryzyka, wskazanie mechanizmu obliczania szkody, rozszerzenie odpowiedzialności o utracone korzyści).

2. Odpowiedzialność Banku względem klienta Banku:

1) Pełna odpowiedzialność Banku wobec klienta Banku za szkody wyrządzone za niewykonanie lub nienależyte wykonanie umowy na usługi chmury obliczeniowej. **Nie można wyłączyć ani ograniczyć.**
2) Możliwość modyfikacji polegającej jedynie na rozszerzeniu takiej odpowiedzialności (odpowiedzialność na zasadzie ryzyka, wskazanie mechanizmu obliczania szkody, rozszerzenie odpowiedzialności o utracone korzyści).

KOMENTARZ

1. Odpowiedzialność z art. 6b Prawa bankowego jest odpowiedzialnością kontraktową wyrażoną w art. 471 Kodeksu cywilnego i powstającą w razie braku zachowania należytej staranności przez osobę wykonującą umowę. Oznacza to zatem, że to właśnie ta odpowiedzialność na podstawie łączącej strony umowy nie może zostać ograniczona. Innymi słowy, nie można ograniczać odpowiedzialności kontraktowej Banku względem klienta Banku i Dostawcy względem Banku w zakresie łączącego strony stosunku prawnego, jakim jest outsourcing bankowy w przypadku stosowania usług chmury obliczeniowej.

2. Pomiędzy klientem Banku a Dostawcą nie powstanie żaden stosunek prawny, który byłby podstawą odpowiedzialności Dostawcy względem klienta Banku.

3. Art. 6b Prawa bankowego nie dotyczy relacji na linii Dostawca – poddostawca, tym samym nie dotyczy też odpowiedzialności na linii Bank – poddostawca tj. w przypadku współpracy w modelu Bank – dostawca IT (Fintech) – poddostawca (Dostawca chmurowy), to ten ostatni nie będzie odpowiadał wobec Banku.

4. Art. 6b Prawa bankowego nie wymaga nawiązywania stosunku umownego pomiędzy Bankiem a poddostawcą.

Art. 6c Prawa Bankowego

4. WYKONANIE UMOWY O USŁUGI CHMURY OBLICZENIOWEJ I EWIDENCJA UMÓW

1. Umowa na usługi chmury obliczeniowej może zostać zawarta i być wykonywana, tylko gdy:

1) Bank i Dostawca będą posiadać plany działania zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową;
2) powierzenie wykonywania czynności w ramach umowy na usługi chmury obliczeniowej nie wpłynie niekorzystnie na prowadzenie przez Bank działalności zgodnie z przepisami prawa, ostrożne i stabilne zarządzanie Bankiem, skuteczność systemu kontroli wewnętrznej w Banku, możliwość wykonywania obowiązków przez biegłe-

go rewidenta upoważnionego do badania sprawozdań finansowych Banku na podstawie zawartej z Bankiem umowy oraz ochronę Tajemnicy bankowej **(zaleca się uzyskanie opinii prawnej w tym zakresie)**;

3) Bank uwzględni ryzyko związane z powierzeniem wykonywania takich czynności w systemie zarządzania ryzykiem.

KOMENTARZ

1. Bank ma obowiązek wprowadzenia umowy na usługi chmury obliczeniowej do ewidencji umów, określając w niej co najmniej:

   1) Dane (informacje) identyfikujące Dostawcę,
   2) zakres usługi chmury obliczeniowej,
   3) miejsce wykonania,
   4) okres obowiązywania umowy.

Art. 6d Prawa Bankowego

5. ZEZWOLENIE NA ZAWARCIE UMOWY NA USŁUGI CHMURY OBLICZENIOWEJ

1. Zezwolenia KNF wymagać będą:

   1) zawarcie umowy na usługi chmury obliczeniowej z Dostawcą, którego siedziba znajduje się w kraju innym niż państwo należące do EOG; lub
   2) zawarcie umowy na usługi chmury obliczeniowej, która wykonywana będzie poza państwem należącym do EOG (wymagane jest badanie, jaka część usług wykonywana jest w EOG lub poza EOG).

Wytyczne EBA w sprawie outsourcingu

Zgodnie ze Stanowiskiem UKNF do kwestii związanych z outsourcingiem, do chmury obliczeniowej nie będą miały zastosowania Wytyczne EBA. Nie oznacza to jednak, że procedury i polityki wewnętrzne powinny być zupełnie odrębne dla outsourcingu do chmury obliczeniowej i pozostałego outsourcingu bankowego. Właściwe jest podejście, w którym istniejące procedury i polityki stworzone na potrzeby implementacji Wytycznych EBA dostosowywane są pod kątem dodatkowej zgodności z Komunikatem chmurowym. Tylko te polityki i procedury, które są:

i. wyjątkowe i odmienne ze względu na to, że przewidziane wyłącznie przez Komunikat chmurowy, lub
ii. odmiennie uregulowane przez Komunikat chmurowy w sposób niedający się pogodzić z politykami i procedurami dotyczącymi outsourcingu innego niż chmurowy,

powinny być sporządzone odrębnie.

Załączniki

Załącznik nr 1

do Standardu PolishCloud 2.0

Lista produktów do opracowania po stronie Banku

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
1.	Potwierdzenie, czy w ramach usługi będą przetwarzane informacje prawnie chronione i czy usługa będzie definiowana jako outsourcing szczególny chmury obliczeniowej	Określenie dla każdej planowanej do wykorzystania usługi chmurowej: - czy przetwarzane są informacje prawnie chronione, - czy czynność przetwarzania może być definiowana jako outsourcing szczególny chmury obliczeniowej.	Rozdział IV Wytyczne stosowania, pkt 4	Potwierdzenie może stanowić element zapisów formularza szacowania ryzyka.
2.	Klasyfikacja informacji	Klasyfikacja: - informacji prawnie chronionych w rozumieniu Komunikatu UKNF, - informacji, których ochrona wynika z uregulowań prawnych nieuwzględnionych w Komunikacie UKNF, - informacji, które nie podlegają ochronie prawnej.	Rozdział V Wytyczne do klasyfikacji i oceny informacji, pkt 1	Klasyfikacja może uwzględniać modele lub metody oceny i klasyfikacji informacji, stosowane wewnętrznie przez Bank, a tym samym stanowi wkład do procesu szacowania ryzyka dla usług chmurowych; klasyfikacja informacji dla danej usługi chmurowej może być uwzględniona w formularzu szacowania ryzyka.
3.	Analiza ryzyka dla usługi ...	Szacowanie ryzyka, zawierające identyfikację, analizę oraz ocenę zagrożeń, możliwość ich wystąpienia oraz wpływ tego wystąpienia na Bank.	Rozdział VI Wytyczne do szacowania ryzyka, z punktami i podpunktami	Proces analizy ryzyka powinien być zgodny z wymaganiami aktualnego wydania normy PN-ISO 27005 (Zarządzanie ryzykiem w bezpieczeństwie informacji) lub jej odpowiednika w europejskim systemie normalizacji, lub na bazie innego, usystematyzowanego podejścia (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.
4.	Wartość przetwarzanych informacji dla usługi ...	Wartość przetwarzanych informacji oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem	Rozdział VI Wytyczne do szacowania ryzyka, pkt 2 ppkt 4)	Wartość przetwarzanych informacji dla danej usługi chmurowej, powinna być powiązana/wynikać z formularza klasyfikacji informacji oraz może stanowić element zapisów formularza szacowania ryzyka.
5.	Zastosowane dla usługi ... metody szyfrowania informacji	Zastosowane szyfrowanie informacji		Metody szyfrowania informacji, zastosowane dla danej usługi, mogą stanowić element zapisów formularza szacowania ryzyka.
6.	Procedura zarządzania kluczami szyfrującymi	Procedura zarządzania kluczami szyfrującymi		
7.	Potwierdzenie, że zastosowane w usłudze ... algorytmy szyfrowania nie są uznane za skompromitowane	Potwierdzenie, że zastosowane algorytmy szyfrowania nie są uznane za skompromitowane.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 2 ppkt 5) ust. c	Taka informacja może być zawarta w zasadach kryptografii, obowiązujących w Banku, określających dopuszczalne nieskompromitowane metody szyfrowania informacji. W formularzu szacowania ryzyka powinno znaleźć się odniesienie do takich zasad, jeśli obowiązują. Dodatkowo, potwierdzenie powinno być oparte o przeprowadzoną weryfikację, że algorytmy nie są uznane za skompromitowane. Zastosowane algorytmy powinny być na bieżąco monitorowane pod kątem ewentualnej kompromitacji.

Załącznik nr 1

Lista produktów do opracowania po stronie Banku

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
8.	Ocena, że szyfrowanie w ramach usługi ... jest technologicznie możliwe i ekonomicznie zasadne.	Ocena Banku, że szyfrowanie jest technologicznie możliwe i ekonomicznie zasadne.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 2 ppkt 5) ust. d	Wszystkie aspekty szyfrowania powinny być elementem szacowania ryzyka i wynikać z danych pozyskanych od Dostawcy usługi chmurowej. Zasadność ekonomiczna szyfrowania powinna wynikać z analizy oczekiwanych efektów projektu vs. poniesione nakłady i koszty, z zastrzeżeniem, że taka ocena nie dotyczy usług, w ramach których przetwarzane są informacje prawnie chronione lub usługa została zakwalifikowana jako outsourcing szczególny. W tych przypadkach szyfrowanie jest bezwarunkowo wymagane.
9.	Ocena tworzenia łańcucha outsourcingowego w ramach usługi ...	Ocena tworzenia łańcucha outsourcingowego z perspektywy przepisów szczególnych prawa dotyczących konkretnie realizowanych czynności przetwarzania informacji w chmurze obliczeniowej.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 2 ppkt 6) ust. a	
10.	Potwierdzenie, czy Dostawca IT wykorzystuje usługi chmurowe	Potwierdzenie upewnienia się przez Bank, w jakim zakresie świadczona przez bezpośredniego Dostawcę usługa wykorzystuje usługi chmury obliczeniowej, a w szczególności czy dochodzi do przetwarzania informacji prawnie chronionej w usłudze chmury obliczeniowej.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 2 ppkt 7) ust. a	Potwierdzenie czy Dostawca IT wykorzystuje usługi chmurowe może stanowić element zapisów umownych i/lub być wskazane w informacjach zawartych w ankiecie dla Dostawcy.
11.	Opinia prawna	Pisemna opinia prawna w przypadku poddania umowy z Dostawcą usług chmurowych prawu państwa trzeciego.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 2 ppkt 8) lit. b)	Do zastosowania, jeśli dotyczy. Zalecane jest jednak, aby w przypadku umowy poddanej prawu z obszaru EOG podmiot nadzorowany miał wiedzę dotyczącą uwarunkowań danego prawa oraz realizacji swoich praw np. prekluzja dowodowa, sposoby doręczeń, język, ilość pełnomocników, udział organizacji na prawach uczestnika postępowania (np. izby handlowe, polskie agencje, przedstawicielstwa) itp.
12.	Lista przeanalizowanych audytów zewnętrznych/certyfikatów wystawionych Dostawcy usług chmurowych	Lista przeanalizowanych dostępnych wyników audytów zewnętrznych Dostawców usług chmury obliczeniowej w odniesieniu do usług chmury obliczeniowej oraz procesu zarządzania bezpieczeństwem informacji, w tym certyfikatów wystawionych Dostawcy usług chmury obliczeniowej, potwierdzających spełnienie wymagań.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 3 ppkt 3)	Lista przeanalizowanych audytów zewnętrznych/certyfikatów wystawionych Dostawcy usług chmurowych może być wskazana w informacjach zawartych w ankiecie dla Dostawcy.
13.	Raport z testów – usługa ...	Wyniki testów usług chmury obliczeniowej, również przy wykorzystaniu scenariuszy warunków skrajnych, zarówno w zakresie sposobu działania usługi, jak i jej konfiguracji.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 3 ppkt 4)	Raport z testów dla danej usługi chmurowej powinien być przygotowany zgodnie z zasadami prowadzenia projektów, obowiązującymi w Banku.
14.	Mechanizmy kontrolne i monitorujące stosowane w Banku	Opis stosowanych mechanizmów kontrolnych i monitorujących, zwłaszcza w odniesieniu do: - identyfikacji nowych zagrożeń, - zmian w wykorzystywanej usłudze chmury obliczeniowej lub trybie i zakresie jej wykorzystywania, - zmian w relacji z Dostawcą usług chmury obliczeniowej, w tym możliwość również nieplanowanego zakończenia współpracy, zarówno przez Bank, jak i Dostawcę usług chmurowych.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 4 ppkt 3) ust. a, b i c	
15.	Opis kompetencji technicznych i zdolności organizacyjnych w kontekście wykorzystywania usług chmurowych oraz realizacji postanowień umownych	Opis kompetencji technicznych i zdolności organizacyjnych Banku w kontekście bezpiecznego wykorzystywania usług chmurowych oraz realizacji postanowień umownych	Rozdział VI Wytyczne do szacowania ryzyka, pkt 4 ppkt 4)	

Załącznik nr 1

Lista produktów do opracowania po stronie Banku

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
16.	Potwierdzenie zdolności i zgodność z przepisami prawa do transferowania zidentyfikowanego ryzyka lub akceptacji oszacowanego poziomu ryzyka	Potwierdzenie zdolności Banku i zgodność z przepisami prawa do transferowania zidentyfikowanego ryzyka lub akceptacji oszacowanego poziomu ryzyka	Rozdział VI Wytyczne do szacowania ryzyka, pkt 4 ppkt 5)	
17.	Potwierdzenie, że świadczenie usługi ... będzie realizowane zgodnie z wymaganiami prawa, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi standardami	Potwierdzenie, że biorąc pod uwagę wyniki szacowania ryzyka, świadczenie usługi chmury obliczeniowej będzie realizowane zgodnie z wymaganiami prawa, obowiązującymi Bank, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez Bank standardami.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 5	
18.	Decyzja dotycząca korzystania z usługi ...	Formalna decyzja Banku dotycząca: - usługi/usług chmury obliczeniowej, z której/których Bank będzie korzystał, - rodzaj i zakres przetwarzanych w ramach tej usługi/tych usług informacji.	Rozdział VI Wytyczne do szacowania ryzyka, pkt 6	Zgodnie z opinią zespołu Aspektów Prawnych, formalną decyzję podejmuje zarząd Banku w odpowiedniej uchwale.
19.	Potwierdzenie zapewnienia kompetencji projektowych dla projektów chmurowych	Potwierdzenie zapewnienia właściwych kompetencji dla prowadzonych działań przetwarzania informacji w środowisku chmury obliczeniowej. Kompetencje te zawierają wymagania w odniesieniu do wykształcenia, wyszkolenia, umiejętności i doświadczenia pracowników lub współpracowników Banku, zaangażowanych w proces planowania, realizacji, testowania i utrzymywania przetwarzania informacji w chmurze obliczeniowej.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 3 ppkt 3.1.	Kompetencje (jakościowe i ilościowe) dla prowadzonych działań w chmurze powinny być zawarte w zasadach prowadzenia projektów, obowiązujących w Banku.
20.	Potwierdzenie zapewnienia kompetencji związanych z zarządzaniem umowami z Dostawcami usług chmurowych	Potwierdzenie zapewnienia właściwych kompetencji dla prowadzonych działań przetwarzania informacji w środowisku chmury obliczeniowej. Kompetencje te zawierają wymagania w odniesieniu do wykształcenia, wyszkolenia, umiejętności i doświadczenia pracowników lub współpracowników Banku, zaangażowanych w proces zawierania i przeglądania umowy z tym związanej.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 3 ppkt 3.1.	Kompetencje (jakościowe i ilościowe) dla prowadzonych działań w chmurze po stronie Dostawcy powinny być zawarte w umowie.
21.	Architektura chmury obliczeniowej dla usługi ...	Potwierdzenie konsekwencji zastosowania określonej architektury chmury obliczeniowej w stosowanym środowisku chmury obliczeniowej oraz modelu świadczonej usługi, z uwzględnieniem wymagań ciągłości działania oraz posiadanej infrastruktury	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 3 ppkt 3.2.	Potwierdzenie powinno być ujęte w dokumentacji szacowania ryzyka, zapewnienia właściwych zasobów, zarówno pod względem jakościowym, jak i ilościowym, oraz dodatkowo we wszystkich pracach i umowach, związanych z oprogramowaniem wykorzystywanym w chmurze.
22.	Zasady konfiguracji dla usługi ...	Potwierdzenie konsekwencji zastosowania określonych zasad konfiguracji w stosowanym środowisku chmury obliczeniowej oraz modelu świadczonej usługi, z uwzględnieniem ciągłości działania oraz posiadanej infrastruktury	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 3 ppkt 3.2.	Potwierdzenie powinno być ujęte w dokumentacji szacowania ryzyka, zapewnienia właściwych zasobów, zarówno pod względem jakościowym, jak i ilościowym, oraz dodatkowo we wszystkich pracach i umowach, związanych z oprogramowaniem wykorzystywanym w chmurze.

Załącznik nr 1

Lista produktów do opracowania po stronie Banku

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
23.	Podział odpowiedzialności między Banki Dostawcę dla usługi	Potwierdzenie konsekwencji zastosowania określonego podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji w stosowanym środowisku chmury obliczeniowej oraz modelu świadczonej usługi, z uwzględnieniem ciągłości działania oraz posiadanej infrastruktury	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 3 ppkt 3.2.	Potwierdzenie powinno być ujęte w dokumentacji szacowania ryzyka, zapewnienia właściwych zasobów, zarówno pod względem jakościowym, jak i ilościowym, oraz dodatkowo we wszystkich pracach i umowach, związanych z oprogramowaniem wykorzystywanym w chmurze.
24.	Potwierdzenie wykonania szkoleń/ posiadania kompetencji w obszarze planowania, konfiguracji, zarządzania oraz monitoringu usług chmury obliczeniowej	Dokumentacja szkoleniowa lub imienne zaświadczenia potwierdzające kompetencje pracowników lub współpracowników Banku, odpowiedzialnych za bezpieczeństwo usług chmury obliczeniowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 3 ppkt 3.3.	
25.	Potwierdzenie wykonania szkoleń/ posiadania kompetencji w obszarze bezpieczeństwa usług chmury obliczeniowej	Dokumentacja szkoleniowa lub imienne zaświadczenia potwierdzające kompetencje pracowników lub współpracowników Banku, odpowiedzialnych za planowanie, konfigurację i zarządzanie oraz monitoring usług chmury obliczeniowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 3 ppkt 3.3.	
26.	Potwierdzenie wykonania szkoleń/ posiadania kompetencji w obszarze przeglądu lub weryfikacji audytów, certyfikatów i innych dokumentów Dostawcy usług chmury obliczeniowej	Dokumentacja szkoleniowa lub imienne zaświadczenia potwierdzające kompetencje osób odpowiedzialnych za przegląd lub weryfikację audytów, certyfikatów i innych dokumentów Dostawcy usług chmury obliczeniowej, w tym dokumentów o charakterze technicznym	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 3 ppkt 3.3.	
27.	Potwierdzenie wykonania szkoleń/ posiadania kompetencji w obszarze przeglądu lub weryfikacji umowy na świadczenie usług chmury obliczeniowej	Dokumentacja szkoleniowa lub imienne zaświadczenia potwierdzające kompetencje osób odpowiedzialnych za przegląd lub weryfikację umowy na świadczenie usług chmury obliczeniowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 3 ppkt 3.3.	
28.	Umowa	Umowa z Dostawcą usług chmury obliczeniowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 4	
29.	Plan przetwarzania informacji w chmurze obliczeniowej	Plan przetwarzania informacji w chmurze obliczeniowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 5	
30.	Scenariusze testowe dla usługi ...	Scenariusze testowe dla usługi ... do wykonania na danych testowych (generowanych maszynowo lub w inny przypadkowy sposób)	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 5 ppkt 5.2.	Scenariusze testowe powinny być przygotowane zgodnie z obowiązującymi w Banku zasadami prowadzenia projektów oraz być adekwatne do zakresu danej usługi. Zakres scenariuszy może odnosić się również do założeń przyjętych podczas szacowania ryzyka dla danej usługi.

Załącznik nr 1

Lista produktów do opracowania po stronie Banku

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
31.	Wyniki testów dla usługi ...	Wyniki testów usług chmury obliczeniowej, przeprowadzonych na podstawie scenariuszy testowych dla usługi ..., również przy wykorzystaniu scenariuszy warunków skrajnych, zarówno w zakresie sposobu działania usługi, jak i jej konfiguracji	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 5 ppkt 5.2.	Wyniki testów powinny być brane pod uwagę podczas procesu szacowania ryzyka dla danej usługi.
32.	Plan wycofania się z usługi ...	Plan wycofania się z usługi, w wyniku zakończenia umowy lub sytuacji awaryjnej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 5 ppkt 5.3.	
33.	Scenariusze testowe planu wycofania się z usługi ... w związku z zakończeniem umowy	Scenariusze testowe planu wycofania się z usługi ... w związku z zakończeniem umowy	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 5 ppkt 5.3.	
34.	Wyniki testów planu wycofania się z usługi ... w związku z zakończeniem umowy	Wyniki testów planu wycofania się z usługi ... w związku z zakończeniem umowy	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 5 ppkt 5.3.	
35.	Scenariusze testowe planu wycofania się z usługi ... w związku z sytuacją awaryjną	Scenariusze testowe planu wycofania się z usługi ... w związku z sytuacją awaryjną	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 5 ppkt 5.3.	
36.	Wyniki testów planu wycofania się z usługi ... w związku z sytuacją awaryjną	Wyniki testów planu wycofania się z usługi ... w związku z sytuacją awaryjną	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 5 ppkt 5.4.	
37.	Plan ciągłości działania	Plan ciągłości działania uwzględniający możliwość utraty kontroli nad przetwarzanymi informacjami u danego Dostawcy usług chmury obliczeniowej oraz możliwość przerwania ciągłości działania usługi	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 5 ppkt 5.4.	W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej Dostawców usług chmury obliczeniowej Bank powinien regularnie weryfikować 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.

Załącznik nr 1

Lista produktów do opracowania po stronie Banku

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
38.	Testy Planu ciągłości działania	Testy Planu ciągłości działania uwzględniające możliwość utraty kontroli nad przetwarzanymi informacjami u danego Dostawcy usług chmury obliczeniowej oraz możliwość przerwania ciągło-ści działania usługi	Rozdział VII Minimalne wymagania dla prze-twarzania informacji w chmurze obliczenio-wej, pkt 5 ppkt 5.4.	W przypadku planu ciągłości działania opartego o wykorzystanie dwóch lub więcej chmur obliczeniowych lub dwóch lub więcej Dostawców usług chmury obliczeniowej Bank powinien regularnie testować 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.
39.	Wymagania w zakresie norm i standardów	Udokumentowane wymagania Banku w zakresie norm i standar-dów, w szczególności dokumentacja akceptacji ryzyka w przy-padku rezygnacji z wymagań wskazanych w Komunikacie	Rozdział VII Minimalne wymagania dla prze-twarzania informacji w chmurze obliczenio-wej, pkt 6 ppkt 6.1., 6.2. i 6.5.	
40.	Certyfikaty/dokumenty potwierdza-jące zgodność Dostawcy usługi … z normami obowiązującymi w Banku.	Pozyskanie od Dostawcy certyfikatu lub innej dokumentacji, po-twierdzającej zgodność Dostawcy usługi chmurowej z normami	Rozdział VII Minimalne wymagania dla prze-twarzania informacji w chmurze obliczenio-wej, pkt 6 ppkt 6.1., 6.2. i 6.5.	Na podstawie uzyskanych informacji, Bank powinien zweryfikować czy korzystanie/ zamiar korzystania z danej usługi chmurowej nie jest sprzeczne z obowiązującymi regulacjami wewnętrznymi (np. lokalizacja CPD w umowie chmurowej, a wymogi cyber-bezpieczeństwa) i regulaminami, udostępnianymi klientom Banku np. dot. bankowości elektronicznej. Odniesienie do produktu znajduje się również w pkt 12 powyżej.
41.	Zasady przeprowadzania oceny do-kumentacji związanej z certyfikacją/ zgodnością przetwarzania informacji w chmurze	Udokumentowany proces regularnej oceny dokumentacji związ-anej z certyfikacją/zgodnością	Rozdział VII Minimalne wymagania dla prze-twarzania informacji w chmurze obliczenio-wej, pkt 6 ppkt 6.1., 6.2. i 6.5.	
42.	Zasady zarządzania planem naprawczym uzgodnionym z Dostawcą usługi chmury obliczeniowej	Udokumentowany proces zarządzania planami naprawczymi uzgodnionymi z Dostawcą w przypadku istotnych niezgodności z normami	Rozdział VII Minimalne wymagania dla prze-twarzania informacji w chmurze obliczenio-wej, pkt 6 ppkt 6.1., 6.2. i 6.5.	
43.	Potwierdzenie dostępu do instrukcji konfiguracji usług chmury oblicze-niowej oraz metod weryfikacji po-prawności ich konfiguracji i działania	Potwierdzenie dostępu do szczegółowych i aktualnych instruk-cji konfiguracji usług chmury obliczeniowej oraz metod wery-fikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania danych	Rozdział VII Minimalne wymagania dla prze-twarzania informacji w chmurze obliczenio-wej, pkt 7 ppkt 7.1. ust a)	Potwierdzenie powinno być ujęte w dokumencie 'Ankieta dla Dostawców – udokumen-towanie konfiguracji usługi'.
44.	Potwierdzenie kompetencji w obszarze realizacji poprawnej konfiguracji zgodnie z wytycznymi Dostawcy usługi chmurowej	Potwierdzenie kompetencji w celu realizacji poprawnej kon-figuracji usług chmury obliczeniowej zgodnie z wytycznymi Dostawcy usług chmury obliczeniowej, w tym pod kątem stoso-wania szyfrowania przetwarzanych informacji	Rozdział VII Minimalne wymagania dla prze-twarzania informacji w chmurze obliczenio-wej, pkt 7 ppkt 7.1. ust b)	Potwierdzenie powinno wynikać z doświadczeń nabytych przez pracowników w obsłu-dze chmury obliczeniowej, ukończonych szkoleń oraz posiadanych certyfikatów.

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
45.	Potwierdzenie używanych ustawień konfiguracyjnych dla usługi ...	Potwierdzenie, że Bank używa dedykowanych lub zalecanych przez Dostawcę usług chmury obliczeniowej ustawień konfiguracyjnych, podnoszących bezpieczeństwo świadczonych usług chmury obliczeniowej.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 7 ppkt 7.1. ust c)	
46.	Potwierdzenie, że informacje prawnie chronione przetwarzane w usłudze ... są szyfrowane zarówno „at rest", jak i „in transit"	Potwierdzenie, że informacje prawnie chronione przetwarzane w chmurze obliczeniowej są szyfrowane zarówno „at rest", jak i „in transit".	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 7 ppkt 7.1. ust d)	
47.	Mechanizmy szyfrowania oraz metody weryfikacji poprawności konfiguracji szyfrowania.	Dokumentacja mechanizmów szyfrowania oraz metody weryfikacji poprawności konfiguracji szyfrowania	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 7	Odniesienie do produktu znajduje się również w pkt 14 powyżej.
48.	Potwierdzenie, że informacje przetwarzane w usłudze ... są szyfrowane kluczami generowanymi oraz zarządzanymi przez Bank	Potwierdzenie, że informacje są szyfrowane kluczami generowanymi oraz zarządzanymi przez Bank.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 7 ppkt 7.2.	Należy pamiętać, że zgodnie z zapisami Komunikatu, analiza ryzyka może dopuścić lub uznać za wskazane używanie kluczy szyfrujących generowanych lub zarządzanych przez Dostawcę usług chmury obliczeniowej.
49.	Wykorzystywane HSM	Dokumentacja wykorzystywanych HSM potwierdzająca spełnienie wymagania FIPS 140-2 Level 2 lub równoważnego	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 7 ppkt 7.3.	
50.	Procedura zarządzania kluczami szyfrującymi	Proces zarządzania kluczami szyfrującymi powinien uwzględniać tworzenie, wykorzystanie (w tym zasady dostępu), ochronę, niszczenie i kontrolę procesu niszczenia, oraz 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.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 7 ppkt 7.4. i 7.5.	
51.	Zasady zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej	Zasady zbierania logów powinny być stosowne do zakresu używanych usług chmury obliczeniowej, przetwarzanych informacji i wyników szacowania ryzyka.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 8 ppkt 8.1.	

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
52.	Procedura zabezpieczania logów dla usługi	Procedura zabezpieczania logów przed nieautoryzowanym dostępem, modyfikacją lub usunięciem przez okres zgodny z ustalonymi zasadami bezpieczeństwa, wynikającymi z obowiązujących przepisów, jak również z analizy ryzyka wykonanej dla danej usługi chmurowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 8 ppkt 8.2.	
53.	Potwierdzenie dokonania przeglądu logów w ramach usługi ...	Potwierdzenie dokonania przeglądu logów	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 8 ppkt 8.2.	Przegląd powinien być prowadzony zgodnie z procedurami i zasadami bezpieczeństwa Banku. Zależnie od skali działania, rodzaju i liczby logowanych zdarzeń oraz architektury bezpieczeństwa, UKNF zaleca używanie specjalistycznego oprogramowania do korelowania zapisów ze zdarzeń (SIEM) oraz regularny przegląd i aktualizację reguł korelacji.
54.	Umowa z Dostawcą IT	W przypadku Dostawców usług IT, mających dostęp zdalny do usług chmury obliczeniowej, wykorzystywanych przez Bank, Bank powinien zapewnić, że wyłącznie uprawniony personel Dostawcy usług IT ma dostęp do wskazanych systemów teleinformatycznych lub ich wybranych zasobów, personel Dostawcy IT używa usług uwierzytelnienia MFA, przy czym rodzaj i zakres uzależniony jest od wyników analizy ryzyka usługi chmurowej, do której Dostawca IT ma mieć dostęp.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 8 ppkt 8.4. ust. a) i b)	
55.	Zasady kontroli dostępu administracyjnego lub o charakterze uprzywilejowanym dla Dostawców IT	Bank zapewnia, że dostęp administracyjny lub o charakterze uprzywilejowanym realizowany jest przez Dostawcę IT z zaufanych sieci Banku lub Dostawcy IT i pod kontrolą (w tym np. poprzez nagrywanie sesji i jej parametrów, a następnie poprzez analizowanie prawidłowości i celowości realizowanych czynności).	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 8 ppkt 8.4. ust. c)	Zasady kontroli dostępu administracyjnego lub o charakterze uprzywilejowanym dla Dostawcy IT powinny być ujęte w umowie.
56.	Mechanizmy uwierzytelniania	Opis mechanizmów uwierzytelnienia	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 8 ppkt 8.4. ust. c)	
57.	Procedura okresowej weryfikacji dostępu Dostawcy usługi chmury obliczeniowej do systemów wykorzystywanych w usłudze	Udokumentowane procedury okresowej weryfikacji dostępu Dostawcy do systemów wykorzystywanych w usłudze	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 8 ppkt 8.4. ust. c)	
58.	Organizacja w obszarze cyberbezpieczeństwa	Dokument zawierający 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 odpowiedzialności	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. a)	Opis organizacji w obszarze cyberbezpieczeństwa powinien stanowić element regulaminu wewnętrznego jednostki bezpieczeństwa/cyberbezpieczeństwa/polityki chmurowej, odwołującego się do regulacji dotyczących zarządzania incydentami bezpieczeństwa.

Załącznik nr 1

Lista produktów do opracowania po stronie Banku

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
59.	Architektura sieci, systemów i aplikacji dla usługi	Dokument zawierający architekturę sieci, systemów i aplikacji oraz punktów styku sieci wewnętrznych Banku z sieciami niezaufanymi, w tym architekturę rozwiązania w chmurze obliczeniowej, także z uwzględnieniem środowisk testowych oraz scenariuszy awaryjnych	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. b)	
60.	Zasady kategoryzacji informacji lub systemów pod kątem przetwarzania w chmurze obliczeniowej	Zasady kategoryzacji informacji lub systemów pod kątem przetwarzania w chmurze obliczeniowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. c)	Zgodnie z wewnętrznymi przepisami Banku.
61.	Zasady stosowanych przez Bank zabezpieczeń technologicznych i rozwiązań organizacyjnych	Zasady stosowanych przez Bank zabezpieczeń technologicznych i rozwiązań organizacyjnych.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. d)	Zgodnie z wewnętrznymi przepisami Banku.
62.	Zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z Dostawcą usług chmury obliczeniowej	Zasady bieżącego zabezpieczania przetwarzanych informacji oraz w sytuacji planowanego lub nieplanowanego zakończenia współpracy z Dostawcą usług chmury obliczeniowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. f)	Zgodnie z wewnętrznymi przepisami Banku.
63.	Zasady zarządzania zgodnością z prawem (m.in. procesy licencjonowania oprogramowania), w tym zgodnością z wymogami regulacyjnymi.	Zasady zarządzania zgodnością z prawem	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. g)	
64.	Zasady przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem usług chmury obliczeniowej.	Zasady przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z używaniem usług chmury obliczeniowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. h)	
65.	Zasady raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej.	Zasady raportowania, przeglądania i weryfikowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. i)	
66.	Zasady analizy zagrożeń i szacowania ryzyka dla stosowanych usług chmury obliczeniowej	Zasady analizy zagrożeń i szacowania ryzyka, w tym źródła pozyskiwania informacji o zagrożeniach specyficznych dla stosowanych usług chmury obliczeniowej oraz sektora finansowego.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. k) i.	

L.p.	Nazwa opracowania	Zawartość opracowania	Pkt z Komunikatu UKNF	Komentarz
67.	Zasady zarządzania środowiskiem teleinformatycznym, z uwzględnieniem usług chmury obliczeniowej	Zasady zarządzania środowiskiem teleinformatycznym (sieciami, systemami, aplikacjami, bazami danych itp.), z uwzględnieniem usług chmury obliczeniowej, w tym planowanie, rozwój i utrzymywanie tego środowiska.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. k) ii.	
68.	Zasady zarządzania incydentami bezpieczeństwa	Zasady zarządzania incydentami bezpieczeństwa.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. k) v.	
69.	Zasady przeprowadzania audytów wewnętrznych bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej	Zasady przeprowadzania audytów wewnętrznych bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.1. ust. k) vi.	
70.	Zasady zarządzania dokumentacją w Banku	Zasady zarządzania dokumentacją w Banku, obejmujące opisy zabezpieczeń, że dokumentacja jest chroniona przed nieuprawnionym dostępem, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.	Rozdział VII Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej, pkt 9 ppkt 9.2.	
71.	Informacja podmiotu nadzorowanego w sprawie przetwarzania informacji w chmurze obliczeniowej	Informacja zgodnie z załącznikiem nr 1 do Komunikatu UKNF z 23.01.2020	Rozdział VIII Zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej	Wypełniony i podpisany formularz powinien stanowić element dokumentacji Banku, stworzonej dla danej usługi chmurowej.

Załącznik nr 2

do Standardu PolishCloud 2.0

Klasyfikacja informacji

Odpowiednio przeprowadzony proces analizy klasyfikacji informacji przetwarzanej w chmurze obliczeniowej pozwoli Bankom właściwie wykonać analizę ryzyka, a w konsekwencji dobrać adekwatne mechanizmy oraz zidentyfikować narzędzia i procesy zapewniające należyty poziom bezpieczeństwa. Biorąc pod uwagę istotność procesu klasyfikacji informacji, Bank może wykorzystać poniższą listę pytań kontrolnych w ocenie dojrzałości istniejących w Banku procesów, a ewentualne braki uzupełnić, wprowadzając stosowne zmiany do procesów i polityk. Pytania poprzedzone są krótkim wyjaśnieniem.

1. **Kontekst:** zbudowanie w organizacji odpowiedniego poziomu rozumienia i właściwej identyfikacji kategorii danych, które Bank zamierza przetwarzać w chmurze, jest podstawą do doboru właściwych działań zarówno na poziomie technologicznym, jak i zgodności regulacyjnej.

   Pytanie: Jak Bank definiuje „dane prawnie chronione" oraz „dane prawnie chronione w chmurze obliczeniowej" i jak ma się to do innych kategorii danych jak np. „dane osobowe", „tajemnica bankowa"?

2. **Kontekst:** weryfikacja, czy obowiązująca w Banku polityka klasyfikacji informacji jest zorganizowana w formalny posiadający właściciela proces, czyli jest zbiorem działań faktycznych i adekwatnych, wraz z przypisanymi osobami odpowiedzialnymi za ich wykonanie i kontrolę, umożliwia Bankowi dużo prościej przechodzić z przetwarzaniem do chmury, zapewniając spełnienie jednego z podstawowych warunków regulacyjnych.

   [Istnieje konieczność potwierdzenia, że polityka klasyfikacji informacji jest zorganizowana w formalny proces, w którym stworzony został model ról i odpowiedzialności oraz określony został właściciel tego procesu. Przed przystąpieniem do adopcji usług chmurowych i rozpoczęcia procesu przetwarzania danych w chmurze należy upewnić się, że podjęto wszystkie wymagane działania umożliwiające spełnienie wymogów regulacyjnych].

   Pytanie: Czy Bank posiada udokumentowany proces klasyfikacji informacji (standard opisujący, jak realizować proces klasyfikacji oraz politykę pokazującą, kto i kiedy jest za to odpowiedzialny)? Czy w Banku realizowany jest proces klasyfikacji zgodnie z przyjętą polityką? Czy efektywność tego procesu jest mierzona?

3. **Kontekst:** Przejście do chmury może wymagać modyfikacji istniejących wytycznych dotyczących procesu, polityki i standardu klasyfikacji informacji, w ramach systemu zarządzania wewnętrznymi regulacjami w Banku.

   Pytanie: W jaki sposób Bank utrzymuje i uaktualnia proces/politykę/standard klasyfikacji informacji, a także aktualność przeprowadzonej klasyfikacji (cyklicznie oraz wraz ze zmianą wykorzystania informacji)?

4. **Kontekst:** Jeśli wiemy już, jakiego typu informacje zamierzamy przetwarzać, oraz że robimy to zgodnie z udokumentowanym i działającym procesem, przyszedł czas na zastanowienie się, czy używane obecnie rozwiązanie zadziała też u Dostawcy chmurowego dla workloadu, który chcemy tam umieścić. Może się okazać, że nasze narzędzie nie zadziała lub Dostawca ma swoje natywne mechanizmy, które będą działały w scenariuszach użycia przez odbiorców (użytkowników) rozwiązania.

   Pytanie: Jak od strony technicznej jest realizowany proces klasyfikacji informacji (czy istnieje udokumentowany opis)? Jakie dane aktualnie są objęte procesem klasyfikacji informacji? Jakie rozwiązania wspierają/automatyzują w Banku proces klasyfikacji informacji? Czy możliwa jest ich integracja z usługą proponowaną przez Dostawcę chmurowego? Czy proces można wykonać jeszcze w miejscu powstawania informacji „on-premise"? Czy możliwe będzie wykorzystywanie funkcji znaczników dla sklasyfikowanych danych w ramach chmury?

5. **Kontekst:** Niniejsze pytanie ma na celu weryfikację poprawności klasyfikacji danych w momencie ich wytworzenia. Takie weryfikacje mogą być automatyczne lub manualne. Ważne jest rozważenie, czy Bank planuje realizować taki proces, a jeżeli tak, to w jaki sposób. Potrzeba weryfikacji powinna wynikać z interpretacji przez Bank, jak i analizy ryzyka, którą Bank wykonuje w ramach przygotowania do migracji do chmury.

   Pytanie: Jakie istnieją i jak działają obecnie w Banku mechanizmy kontrolne weryfikacji klasyfikacji danych? Jakie mechanizmy kontrolne klasyfikacji danych w chmurze mogą/powinny być wdrożone?

6. **Kontekst:** Pytanie ma na celu przygotowanie Banku do realizacji skutecznego procesu kategoryzacji danych również w kontekście fizycznej lokalizacji danych w CPD (w kontekście czy jest to w ramach EOG lub też nie itp.). W praktyce Dostawców usług chmurowych może się zdarzyć przypadek, w którym dane będą znajdować się w EOG, ale inne usługi, które z tych danych korzystają w chmurze, mają już swoje CPD w innych regionach (np. w USA). Jeżeli tak jest, to należy zwrócić uwagę czy wszystkie dane są dobrze sklasyfikowane i odpowiednio zabezpieczone przez mechanizmy szyfrowania. Ponadto, Dostawca może mieć do nich potencjalny identyfikowany dostęp.

   Pytanie: Jak wygląda inwentaryzacja miejsca przechowywania danych w chmurze w zależności od ich kategorii wynikającej z klasyfikacji informacji? Kto ma do niej dostęp? Czy informacja jest szyfrowana adekwatnie do klasyfikacji? Które usługi uczestniczą w przechowywaniu i przetwarzaniu danych? Geolokalizacja przechowywania i przetwarzania danych? W jaki sposób następuje dostęp do informacji przechowywanych i jak to się ma do miejsca przechowywania danych?

7. **Kontekst:** Przeprowadzona pierwotna kwalifikacja danych składowanych i przetwarzanych w usługach chmurowych zgodnie z przyjętą polityką retencji może wymagać reklasyfikacji podczas transferu pomiędzy różnym typami usług służących do przechowywania np. pomiędzy magazynami typu WORM lub też innymi typami usług służących do przechowywania danych.

   Pytanie: Czy proponowane rozwiązanie oprócz klasyfikacji wspiera również reklasyfikację danych?

Źródła:

1. AWS – klasyfikacja danych: https:/docs.aws.amazon.com/whitepapers/latest/data-classification/welcome.html?did=wp_card&trk=wp_card
2. Klasyfikowanie danych organizacji: https:/docs.microsoft.com/pl-pl/azure/cloud-adoption-framework/innovate/best-practices/dataclassification
3. Wykorzystanie Azure Information Protection do klasyfikacji i oznaczania danych firmowych: https:/www.microsoft.com/en-us/itshowcase/using-azure-information-protection-to-classify-and-label-corporate-data
4. Identyfikowanie i klasyfikowanie danych w bazach Microsoft SQL: https:/docs.microsoft.com/en-us/sql/relational-databases/security/sql-data-discovery-and-classification?view=sql-server-ver15&tabs=t-sql
5. IBM – klasyfikacja i wykrywanie danych wrażliwych: https:/www.ibm.com/security/data-security/guardium

Załącznik nr 3

do Standardu PolishCloud 2.0

Zagrożenia i podatności w IT [1]. Wprowadzenie

Zagrożenie i podatność nie są tą samą kategorią i nie oznaczają tego samego.

Zagrożeniem jest osoba albo zdarzenie, mające potencjalny negatywny wpływ na zasoby wrażliwe.

Podatność oznacza jakość danego zasobu lub jego otoczenia, która pozwala na realizację zagrożenia.

W obszarze bezpieczeństwa systemów i sieci zagrożenia istnieją, ale są ograniczane poprzez prawidłowe użycie procedur i funkcji bezpieczeństwa. Mitygantem jest każde działanie mające na celu zabezpieczenie przed negatywnym wpływem jakiegokolwiek zagrożenia, ograniczenie szkody, w sytuacji gdy nie jest możliwa całkowita ochrona, lub usprawnienie szybkości albo efektywności wysiłków podejmowanych w celu powrotu do normalnych warunków.

Sprzęt, oprogramowanie i dane przetwarzane przez systemy mogą być wrażliwe na szereg zagrożeń. Dobór procedur i funkcji bezpieczeństwa powinien opierać się nie tylko na ogólnych celach związanych z bezpieczeństwem, ale także odnosić się do specyficznych podatności danego systemu, na które jest on narażony. Zdarza się, że systemy są zabezpieczane nadmiarowo, co stanowi jedynie marnotrawstwo zasobów i naraża użytkowników na niedogodności podczas pracy.

Czasami łatwiej jest zweryfikować każde potencjalne zagrożenie i określić, w jakim stopniu organizacja jest na nie wrażliwa (np. pożar, powódź, trzęsienie ziemi).

W innych przypadkach będzie łatwiej wyszukać potencjalne podatności bez odwoływania się do konkretnych zagrożeń (np. niewłaściwy montaż sprzętu, awaria mediów, błąd we wprowadzonych danych).

W celu dojścia do kompletnej oceny ryzyka obie perspektywy powinny być zweryfikowane.

Poniżej zaprezentowano zarówno zagrożenia, jak i podatności, które mogą razem stanowić wyzwania w zakresie bezpieczeństwa.

Poniższa lista wyzwań została podzielona na cztery kategorie.

Wyzwania w zakresie środowiska obejmują niepożądaną, specyficzną dla danego miejsca, szansę wystąpienia takich zagrożeń jak uderzenie pioruna, powódź czy trzęsienie ziemi.

1 Źródło: wiedza ekspercka członków zespołu opracowującego Standard PolishCloud 2.0 oraz informacje zawarte pod linkiem: https:/www.hq.nasa.gov/security/it_threats_vulnerabilities.htm.

Wyzwania w sferze fizycznej obejmują niepożądane, specyficzne dla danego miejsca, działania personelu, zarówno intencjonalne, jak i niezamierzone, w tym kradzież, wandalizm czy wypadek przy pracy.

Wyzwania w obszarze wsparcia obejmują podstawowe aspekty działania danego miejsca takie jak zasilanie, usługi telekomunikacyjne czy eksploatacja.

Powyższe trzy kategorie wyzwań nie są analizowane w trakcie fazy projektowania systemu czy jego utrzymania. Właściwsze jest rozpatrywanie tych zagrożeń podczas projektowania i utrzymania obiektu, w kontekście wszystkie systemów informatycznych, które w tym obiekcie się znajdują.

Ostatnią kategorią jest **kategoria wyzwań technicznych**, obejmująca podejrzane sytuacje specyficzne dla danego systemu, takie jak niewłaściwa eksploatacja systemu, złośliwe oprogramowanie czy awaria.

Wyzwania związane ze środowiskiem naturalnym (niepożądane zdarzenia specyficzne dla danego miejsca):

- pożar,
- powódź,
- tsunami,
- trzęsienie ziemi,
- erupcja wulkanu,
- uderzenie pioruna,
- zła pogoda,
- smog,
- zapylenie,
- plaga owadów,
- plaga gryzoni,
- epidemia/pandemia,
- opary chemiczne, skażenie,
- wyciek wody – np. pęknięcie rury, dziura w dachu,
- eksplozja – gazu, zakładów chemicznych, składu amunicji,
- wibracje – w pobliżu linia kolejowa, ruch lotniczy, budowa,
- interferencja elektromagnetyczna – wskazywana np. przez słaby odbiór radiowy lub drgający obraz na ekranie komputera,
- wyładowania elektrostatyczne – wskazywane np. przez iskrzenie.

Wyzwania fizyczne (niepożądane, specyficzne dla danego miejsca, działania personelu):

- nieupoważniony dostęp do obiektu,
- kradzież,
- wandalizm,
- sabotaż,
- wymuszenie,
- terroryzm/zagrożenie bombowe,
- niepokoje w pracy – pracownicy i kontraktorzy,

- wojna/zamieszki,
- niewłaściwy transport – sprzęt spadł, został zalany, wystawiony na warunki pogodowe lub został prześwietlony w czasie transportu,
- niewłaściwy montaż/składowanie – sprzęt został wystawiony na wstrząsy, uderzenia lub warunki pogodowe,
- wycieki – niebezpieczne materiały znajdują się w pobliżu np. pożywienia, napojów,
- magnesy/narzędzia magnetyczne – mogą wymazać dane lub uszkodzić czuły sprzęt,
- kolizja/zderzenie – z udziałem np. wózka widłowego, samochodów, samolotu, wózka inwalidzkiego,
- ryzyko potknięcia/upadku – sprzęt stwarza zagrożenie dla personelu,
- zagrożenie pożarowe – materiały łatwopalne składowane w pobliżu obiektu/sprzętu/miejsca pracy personelu.

Wyzwania w obszarze wsparcia:

- brak zasilania,
- ekstremalne/niestabilne temperatury,
- ekstremalna/niestabilna wilgotność,
- niebezpieczne środowisko – niezdatne do zajęcia przez ludzi,
- niedostępność obiektu – zablokowany dostęp,
- niemożliwe całkowite odcięcie zasilania – np. podczas pożaru, powodzi itp.,
- hałas elektryczny/złe uziemienie – wskazywane np. przez migające światła lub drgający ekran komputera,
- niewłaściwa eksploatacja – niewykwalifikowany personel wsparcia lub opóźniona prewencyjna konserwacja,
- niedostępność personelu – niemożliwy kontakt z personelem wsparcia lub eksploatacji,
- awaria telefonów – niemożliwy kontakt przychodzący z zewnątrz, niemożliwe wyjście telefoniczne na zewnątrz, usługa zupełnie niedostępna,
- niewłaściwe tłumienie ognia – woda, piana, halon,
- niewłaściwa utylizacja śmieci – dane wrażliwe udostępnione w nieautoryzowany sposób.

Wyzwania techniczne (sytuacje podejrzane, specyficzne dla systemu):

- niewłaściwa procedura – brak wsparcia przewidywalnych wydarzeń przez kompletną i właściwą dokumentację i szkolenia,
- niewłaściwa eksploatacja – sprzęt działający przy przekroczeniu poziomu pojemności lub niezgodnie z zaleceniami/ograniczeniami producenta,
- niewłaściwa konfiguracja sprzętu – zalecany sprzęt skonfigurowany w inny sposób niż zalecany podczas instalacji,
- niewłaściwa konfiguracja oprogramowania – zalecane oprogramowanie skonfigurowane w inny sposób niż rekomendowane podczas instalacji,
- nieautoryzowana zmiana sprzętu – dodanie innej niż zalecana lub wprowadzenie nieautoryzowanych zmian w sprzęcie,
- nieautoryzowana modyfikacja oprogramowania – dodanie innej niż zalecana lub wprowadzenie nieautoryzowanych zmian w oprogramowaniu,
- nieautoryzowane kopiowanie oprogramowania – tworzenie kopii licencjonowanego oprogramowania, nieuwzględnionych w obowiązującej umowie licencyjnej,

- nieautoryzowany dostęp logiczny – użytkowanie systemu bez autoryzowanego dostępu,
- nadużycia (przekroczenie uprawnień) – użytkowanie systemu w sposób wykraczający poza nadane upoważnienie,
- nieusankcjonowane wykorzystanie/przekroczenie praw licencyjnych – wykorzystanie dopuszczonych zasobów systemowych w nieautoryzowanym celu (wysyłanie e-maili niezwiązanych z pracą lub surfowanie w Internecie) lub przekroczenie warunków umowy licencyjnej,
- zawyżenie lub zaniżenie klasyfikacji – oznaczenie zasobów z wyższym lub niższym poziomem wrażliwości niż właściwy,
- złośliwe oprogramowanie – oprogramowanie mające na celu szkodliwe działanie w stosunku do systemu komputerowego lub jego użytkownika, obniżenie wydajności, zmiana lub uszkodzenie danych, kradzież zasobów lub naruszenie bezpieczeństwa w jakikolwiek sposób,
- błąd sprzętu/awaria (funkcjonalność) – sprzęt, który przestał działać w sposób oczekiwany przez użytkownika,
- błąd sprzętu/awaria (bezpieczeństwo) – sprzęt, który przestał działać w sposób oczekiwany przez użytkownika,
- błąd oprogramowania/awaria (funkcjonalność) – oprogramowanie, które przestało działać w sposób oczekiwany przez użytkownika,
- błąd oprogramowania/awaria (bezpieczeństwo) – oprogramowanie, które przestało działać w sposób oczekiwany przez użytkownika,
- awaria mediów – nośniki, które przestały przechowywać zachowane informacje w sposób nienaruszony oraz umożliwiający ich odczytanie,
- remanencja danych – nośniki, które przechowują informacje w sposób umożliwiający odczytanie/w sposób nienaruszony, dłużej niż zamierzono (niemożliwe całkowite usunięcie danych),
- ponowne wykorzystanie obiektu – system zapewniający użytkownikowi storage (np. pamięć lub przestrzeń dyskowa), który zawiera użyteczne informacje, należące do innego użytkownika,
- awaria komunikacji/przeciążenie – obiekt komunikacyjny, który zatrzymuje świadczenie usługi, lub który nie jest w stanie świadczyć usługi w ramach żądanej pojemności,
- błąd komunikacji – obiekt komunikacyjny, który zapewnia niedokładnie oczekiwaną usługę,
- błąd wprowadzania danych – system akceptuje błędne dane jako prawidłowe,
- przypadkowa modyfikacja oprogramowania/przypadkowe usunięcie – usunięcie lub inna niedostępność potrzebnego oprogramowania,
- przypadkowa modyfikacja danych/przypadkowe usunięcie – usunięcie lub inna niedostępność potrzebnych danych,
- przypadkowe ujawnienie danych – nieumyślne ujawnienie poufnych danych nieupoważnionemu użytkownikowi,
- zaprzeczenie – udział w procesie lub transakcji, a następnie zaprzeczanie temu udziałowi,
- podszywanie się – udział w procesie lub transakcji poprzez podszywanie się pod innego użytkownika,
- odtwarzanie wiadomości – nagrywanie prawidłowej transmisji w celu późniejszego odtworzenia dla pozyskania nieautoryzowanych informacji,
- zalew wiadomości – generowanie przesadnie dużych ilości transmisji w celu uniemożliwienia wykorzystania systemu lub usługi ze względu na przeciążenie,

- odsłuchiwanie linii – podłączenie się do obiektu komunikacji w sposób nieautoryzowany w celu zbierania użytecznej informacji,
- emanacje elektroniczne – informacje niosące fałszywe emisje związane z całym sprzętem elektronicznym,
- geolokalizacja – nieumyślne ujawnianie obecnej fizycznej lokalizacji użytkownika przez system.

Przykładowe zagrożenia i podatności[2] (inne ujęcie)

Zagrożenia:

- dostęp do sieci przez nieupoważnione osoby,
- atak bombowy,
- zagrożenie bombowe,
- naruszenie relacji kontraktowych,
- naruszenie prawa,
- skompromitowanie informacji poufnych,
- zatajenie tożsamości użytkownika,
- szkoda w wyniku działania trzeciej strony,
- szkody w wyniku testów penetracyjnych,
- zniszczenie rekordów,
- katastrofa (w wyniku działań człowieka),
- katastrofa naturalna,
- ujawnienie informacji,
- ujawnienie haseł,
- podsłuch,
- sprzeniewierzenie,
- błędy w obsłudze,
- awaria połączeń komunikacyjnych,
- fałszowanie rekordów,
- ogień,
- powódź,
- oszustwo,
- szpiegostwo przemysłowe,
- wyciek informacji,
- zakłócenie procesów biznesowych,
- utrata elektryczności,
- utrata usług wsparcia,
- awaria sprzętu,
- złośliwe oprogramowania,
- nadużywanie systemów informatycznych,
- nadużywanie narzędzi audytowych,
- skażenie,
- inżynieria społeczna.

2 Źródło: wiedza ekspercka członków zespołu opracowującego Standard PolishCloud 2.0 oraz informacje zawarte pod linkiem: https:/advisera.com/27001academy/knowledgebase/threats-vulnerabilities/.

Podatności

- skomplikowany interfejs użytkownika,
- niezmienione hasła domyślne,
- utylizacja nośników danych bez usunięcia danych,
- czułość sprzętu na zmiany napięcia,
- czułość sprzętu na wilgoć i zanieczyszczenia,
- czułość sprzętu na temperaturę,
- niewystarczające zabezpieczenie okablowania,
- niewystarczające zarządzanie pojemnością,
- niewystarczające zarządzanie zmianą,
- niewystarczająca klasyfikacja informacji,
- niewystarczająca kontrola dostępu fizycznego,
- niewystarczająca konserwacja,
- niewystarczające zarządzanie siecią,
- niewystarczający lub nieregularny backup,
- niewystarczające zarządzanie hasłami,
- niewystarczająca ochrona fizyczna,
- niewystarczająca ochrona kluczy kryptograficznych,
- niewystarczająca wymiana starego sprzętu,
- niewystarczająca świadomość bezpieczeństwa,
- niewystarczający podział obowiązków,
- niewystarczający rozdział obiektów produkcyjnych i testowych,
- niewystarczający nadzór nad pracownikami,
- niewystarczająca kontrola Dostawców,
- niewystarczające przeszkolenie pracowników,
- niekompletna specyfikacja dotycząca tworzenia oprogramowania,
- niewystarczające testy oprogramowania,
- brak polityki kontroli dostępu,
- brak polityki czystego biurka i przejrzystego ekranu,
- brak kontroli danych wejściowych i wyjściowych,
- brak dokumentacji wewnętrznej,
- brak lub słabe wdrożenie audytu wewnętrznego,
- brak polityki wykorzystania kryptografii,
- brak procedury usuwania praw dostępu po zakończeniu zatrudnienia,
- brak zabezpieczenia sprzętu przenośnego,
- brak redundancji,
- brak systemów identyfikacji i uwierzytelniania,
- brak zatwierdzenia przetwarzanych danych,
- lokalizacja narażona na zalanie,
- słaby wybór danych testowych,
- posiadanie pojedynczej kopii,
- zbyt duże umocowanie jednej osoby,
- niekontrolowane kopiowanie danych,
- niekontrolowane pobieranie z Internetu,
- niekontrolowane wykorzystanie systemów informatycznych,
- nieudokumentowane oprogramowanie,
- zdemotywowani pracownicy,

- niezabezpieczone publiczne połączenia sieciowe,
- nieweryfikowane regularnie prawa dostępu dla użytkowników.

Podsumowanie

Powyższa lista zagrożeń i podatności stanowi podpowiedź do wykorzystania przez Banki podczas procesu szacowania ryzyka. Banki powinny mieć świadomość, że opracowanie kompletnej listy pozostaje po ich stronie i mogą skorzystać z opracowanych przykładów, jednak powinny ją doprecyzować/uzupełnić samodzielnie, np. korzystając z referencyjnych norm/standardów np. ENISA, ISACA, NIST, norma ISO27017 itp.

Załączona lista zagrożeń odnosi się ogólnie do zagrożeń związanych z przygotowaniem i korzystaniem z rozwiązania teleinformatycznego, niekoniecznie chmurowego. Zagrożenia fizyczne, środowiskowe i wsparcia, są właśnie mitygowane w większości użyciem infrastruktury chmurowej, która uwalnia organizacje od konieczności dbania o własne data center i przenosi ten ciężar na Dostawcę usług chmurowych.

Wyzwania techniczne, wskazane w punktach powyżej, wydają się najbardziej dopasowane do kontekstu inicjatyw chmurowych, przykładowo:

- niewłaściwa/nierealizowana procedura szyfrowania danych przechowywanych/przetwarzanych w chmurze obliczeniowej,
- niewłaściwa konfiguracja wykorzystywanej usługi chmurowej,
- nieautoryzowany dostęp do danych po stronie Dostawcy chmurowego,
- awaria komunikacji z usługą chmurową,
- nieumyślne ujawnienie danych, usunięcie, modyfikacja danych przechowywanych w chmurze publicznej itp.
- Wydaje się, że zawsze warto rozważyć takie przykładowe wyzwania/zagrożenia jak:
- zapewnienie zgodności regulacyjnej rozwiązania opartego o chmurę publiczną/możliwości jej audytowania,
- niewłaściwy/niedoprecyzowany podział odpowiedzialności pomiędzy Bankiem a Dostawcą usługi/rozwiązania chmurowego,
- przenaszalność usługi/rozwiązania opartego o chmurę (ryzyko tzw. *vendor lock-in*) – strategicznie oraz na wypadek awarii,
- zapewnienie odpowiednich kompetencji chmurowych w organizacji,
- ograniczona świadomość/doświadczenie użytkowników w zakresie korzystania z rozwiązań chmurowych,
- retencja i kasowanie danych przechowywanych w chmurze publicznej,
- błędy i awarie w zakresie komunikacji z usługą chmurową,
- dostęp do danych przechowywanych/przetwarzanych w chmurze publicznej (pracowników – użytkowników i administratorów, kontraktorów, Dostawcy),
- podatności branego pod uwagę rozwiązania chmurowego,
- niewłaściwa konfiguracja rozwiązania/usługi chmurowej,
- złośliwe oprogramowanie ukierunkowane na rozwiązania chmurowe,
- umyślne, nieautoryzowane działanie użytkownika usługi chmurowej,
- błędne działanie rozwiązania opartego o usługi chmurowe.

Oczywiście nie jest to wyczerpująca lista, ale dotyka kluczowych aspektów związanych z prawidłowym i bezpiecznym funkcjonowaniem rozwiązania/usługi chmurowej.

Załącznik nr 4

do Standardu PolishCloud 2.0

Szablon szacowania ryzyka

Celem niniejszego dokumentu jest przykładowe usystematyzowanie wyników procesu szacowania ryzyka, związanego z uruchamianiem przez Bank usługi chmurowej.

Zebrane w arkuszu informacje odnoszą się do konkretnych zapisów, wskazanych w Komunikacie Urzędu Nadzoru Finansowego w rozdziale VI „Wytyczne do szacowania ryzyka", jak również zostały oparte o doświadczenia własne Banków, których przedstawiciele uczestniczyli w opracowaniu „Standard PolishCloud 2.0".

Ryzyko inherentne

Narażenie wynikające z konkretnego ryzyka przed podjęciem jakichkolwiek działań w celu zarządzenia tym ryzykiem; ryzyka inherentne mogą dotyczyć w szczególności:

a. zaplanowania wydatków na finansowanie realizacji projektu,
b. odpowiedniego doboru osób do zespołu projektowego,
c. dotychczasowej oceny współpracy z dostawcą zewnętrznym,
d. szczegółowości określenia wymagań funkcjonalnych systemu albo aplikacji,
e. powiązań pomiędzy projektami,
f. terminowości realizowania prac oraz zamykania projektu uwarunkowanych od czynników zewnętrznych,
g. podejmowania decyzji w zakresie struktury organizacyjnej projektu,
h. ryzyka operacyjnego.

Ryzyko rezydualne

Ryzyko, które pozostaje po podjęciu wszystkich możliwych bądź też wszelkich ekonomicznie zasadnych kroków, zmierzających do jego uniknięcia.

Zagrożenie

Zdarzenie wpływające na podwyższenie prawdopodobieństwa wystąpienia ryzyka skutkującego niedotrzymaniem parametrów projektu, dotyczących w szczególności zakresu, terminu albo budżetu projektu.

Załącznik nr 4

Szablon szacowania ryzyka

Lp.	Obszar zagrożenia	Opis ryzyka (należy wymienić poszczególne ryzyka występujące w danym obszarze zagrożenia)	**Obszar prawny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar organizacyjny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar techniczny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Ocena wpływu/ impaktu wystąpienia ryzyka inherentnego**	**Ocena prawdo-podobieństwa wystąpienia ryzyka inherentnego**	**Ocena ryzyka inherentnego** (np. wysokie, średnie, niskie, n/a)	**Czynniki ograniczające ryzyko/ mityganty** (przy poziomie ryzyka średnie, wysokie)	**Plan postępowania w przypadku wystąpienia ryzyka** (przy poziomie ryzyka średnie, wysokie)	**Ocena poziomu ryzyka rezydualnego** (np. wysokie, średnie, niskie, n/a)
1	Ogólne zagrożenia do stosowania chmury obliczeniowej: Rozproszenie geograficzne przetwarzanych informacji Ad VI.2.1) a)	Ryzyko braku zgodności procesu przetwarzania informacji z przepisami prawa, regulacjami wewnętrznymi, zobowiązaniami umownymi oraz deklaracjami i innymi uregulowaniami									
2	Ogólne zagrożenia do stosowania chmury obliczeniowej: Możliwość utraty zgodności postępowania podmiotu nadzorowanego z przepisami prawa (w tym wydanymi licencjami i/ lub zezwoleniami) Ad VI.2.1) b)	Korzystanie przez podmiot nadzorowany z usług chmury obliczeniowej w sposób niezamierzony albo inny niż zamierzony. Np. niezamierzona przez podmiot nadzorowany możliwość dostępu do przetwarzanych informacji przez pracowników i współpracowników Dostawcy usług chmurowych lub wykonywanie usług przez Dostawcę w sposób inny niż zamierzony przez Bank									
3	Ogólne zagrożenia do stosowania chmury obliczeniowej: Dostęp do przetwarzanych informacji przez osoby nieuprawnione Ad VI.2.1) c)	Dostęp do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) Dostawcy usług chmury obliczeniowej									
4	Ogólne zagrożenia do stosowania chmury obliczeniowej: Dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się fizyczne przetwarzanie (tj. kraju gdzie zlokalizowane jest centrum przetwarzania danych) Ad VI.2.1) d)	Możliwość żądania informacji lub dostępu do informacji bez wyraźnej zgody podmiotu nadzorowanego przez organy administracji krajowej, jak i międzynarodowej, właściwe dla kraju, gdzie zlokalizowane jest centrum przetwarzania danych									
5	Ogólne zagrożenia do stosowania chmury obliczeniowej: Przywiązanie do jednego Dostawcy usług chmury obliczeniowej Ad VI.2.1) 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									

Lp.	Obszar zagrożenia	Opis ryzyka (należy wymienić poszczególne ryzyka występujące w danym obszarze zagrożenia)	**Obszar prawny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar organizacyjny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar techniczny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Ocena wpływu/ impaktu wystąpienia ryzyka inherentnego**	**Ocena prawdo-podobieństwa wystąpienia ryzyka inherentnego**	**Ocena ryzyka inherentnego** (np. wysokie, średnie, niskie, n/a)	**Czynniki ograniczające ryzyko/ mityganty** (przy poziomie ryzyka średnie, wysokie)	**Plan postępowania w przypadku wystąpienia ryzyka** (przy poziomie ryzyka średnie, wysokie)	**Ocena poziomu ryzyka rezydualnego** (np. wysokie, średnie, niskie, n/a)
6	Ogólne zagrożenia do stosowania chmury obliczeniowej: Awarie i podatności elementów technologicznych chmury obliczeniowej Ad VI.2.1) f)	Awarie mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej									
7	Ogólne zagrożenia do stosowania chmury obliczeniowej: Podatność interfejsów zarządzających usługami, które są udostępniane przez Dostawcę usług chmurowych Ad VI.2.1) g)	Podatność interfejsów zarządzających usługami, które są udostępniane przez Dostawcę usług chmurowych									
8	Ogólne zagrożenia do stosowania chmury obliczeniowej: Ograniczona możliwość wpływania na zakres, kształt i zmiany usług Ad VI.2.1) h)	Ograniczona możliwość wpływania przez podmiot nadzorowany na zakres, kształt i zmiany usług, w tym w szczególności na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług przetwarzania									
9	Ogólne zagrożenia do stosowania chmury obliczeniowej: Ograniczona możliwość kontrolowania Dostawcy usług chmury obliczeniowej oraz jego poddostawców Ad VI.2.1) i)	Ograniczona możliwość podmiotu nadzorowanego na kontrolowanie Dostawcy usług chmury obliczeniowej oraz jego poddostawców, w tym na bezpośrednią weryfikację fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej									
10	Ogólne zagrożenia do stosowania chmury obliczeniowej: Podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji Ad VI.2.1) j)	Nieproporcjonalny podział odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy Dostawcę usług chmury obliczeniowej a podmiot nadzorowany									
11	Specyficzne zagrożenia do stosowanych konkretnych usług chmury obliczeniowej: Możliwości korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego Ad VI.2.2) a)	Możliwość 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)									

Lp.	Obszar zagrożenia	Opis ryzyka (należy wymienić poszczególne ryzyka występujące w danym obszarze zagrożenia)	**Obszar prawny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar organizacyjny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar techniczny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Ocena wpływu/ impaktu wystąpienia ryzyka inherentnego**	**Ocena prawdo-podobieństwa wystąpienia ryzyka inherentnego**	**Ocena ryzyka inherentnego** (np. wysokie, średnie, niskie, n/a)	**Czynniki ograniczające ryzyko/ mityganty** (przy poziomie ryzyka średnie, wysokie)	**Plan postępowania w przypadku wystąpienia ryzyka** (przy poziomie ryzyka średnie, wysokie)	**Ocena poziomu ryzyka rezydualnego** (np. wysokie, średnie, niskie, n/a)
12	Specyficzne zagrożenia do stosowanych konkretnych usług chmury obliczeniowej: Możliwości jednostronnej zmiany warunków technicznych korzystania z usługi Ad VI.2.2) b)	Możliwość jednostronnej zmiany warunków technicznych korzystania z usługi (w szczególności jej parametrów lub zasad konfiguracji)									
13	Specyficzne zagrożenia do stosowanych konkretnych usług chmury obliczeniowej: Stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług Ad VI.2.2) c)	Stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług, bez ich należytej weryfikacji i oceny adekwatności dla potrzeb podmiotu nadzorowanego									
14	Specyficzne zagrożenia do stosowanych konkretnych usług chmury obliczeniowej: Stosowane mechanizmy uwierzytelniania Ad VI.2.2) d)	Słabość stosowanych mechanizmów uwierzytelniania									
15	Specyficzne zagrożenia związane z zasobami podmiotu nadzorowanego: Zasoby, w tym zasoby ludzkie Ad VI.2.3) a)	Brak wymaganych i/lub niewystarczające posiadane zasoby, w tym zasoby ludzkie o ustalonych kompetencjach									
16	Specyficzne zagrożenia związane z zasobami podmiotu nadzorowanego: Zgodność środowiska technologicznego Ad VI.2.3) b)	Brak zgodności technologicznej, posiadanego przez podmiot nadzorowany, środowiska teleinformatycznego oraz środowiska chmury obliczeniowej, a w szczególności mechanizmów integracji									
17	Wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem Ad VI.2.4)	Oszacowana wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem									

Lp.	Obszar zagrożenia	Opis ryzyka (należy wymienić poszczególne ryzyka występujące w danym obszarze zagrożenia)	**Obszar prawny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar organizacyjny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar techniczny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Ocena wpływu/ impaktu wystąpienia ryzyka inherentnego**	**Ocena prawdo-podobieństwa wystąpienia ryzyka inherentnego**	**Ocena ryzyka inherentnego** (np. wysokie, średnie, niskie, n/a)	**Czynniki ograniczające ryzyko/ mityganty** (przy poziomie ryzyka średnie, wysokie)	**Plan postępowania w przypadku wystąpienia ryzyka** (przy poziomie ryzyka średnie, wysokie)	**Ocena poziomu ryzyka rezydualnego** (np. wysokie, średnie, niskie, n/a)
18	Szyfrowanie informacji zgodnie z wymaganiami nadzoru, zgodnie z którymi: a) Szyfrowanie informacji nie zmniejsza ważności informacji, nie zmienia też jej klasyfikacji i oceny; b) Szyfrowanie informacji oraz właściwe zarządzanie kluczami szyfrującym zapobiega ujawnieniu informacji; c) Brak jest gwarancji dla uznania danego algorytmu szyfrowania za „całkowicie bezpieczny"; d) Informacje przetwarzane w chmurze obliczeniowej powinny być szyfrowane zawsze, gdy jest to technologicznie możliwe i – w ocenie podmiotu nadzorowanego – ekonomicznie zasadne; e) Informacje prawnie chronione muszą być szyfrowane zawsze „at rest" oraz „in transit"; Dopuszcza się sytuację powierzenia Dostawcy usług chmurowych generowane lub zarządzanie kluczami szyfrującymi, które są używane do szyfrowania informacji przetwarzanej u innego Dostawcy usług chmurowych, przy czym należy uwzględnić w szacowaniu ryzyka możliwość utraty przez podmiot nadzorowany dostępu do tych kluczy; Ad VI.2.5) z podpunktami	Szyfrowanie informacji niezgodnie z wymaganiami nadzoru									

Lp.	Obszar zagrożenia	Opis ryzyka (należy wymienić poszczególne ryzyka występujące w danym obszarze zagrożenia)	**Obszar prawny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar organizacyjny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar techniczny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Ocena wpływu/ impaktu wystąpienia ryzyka inherentnego**	**Ocena prawdo-podobieństwa wystąpienia ryzyka inherentnego**	**Ocena ryzyka inherentnego** (np. wysokie, średnie, niskie, n/a)	**Czynniki ograniczające ryzyko/ mityganty** (przy poziomie ryzyka średnie, wysokie)	**Plan postępowania w przypadku wystąpienia ryzyka** (przy poziomie ryzyka średnie, wysokie)	**Ocena poziomu ryzyka rezydualnego** (np. wysokie, średnie, niskie, n/a)
19	Tworzenie „łańcucha outsourcingowego" zgodnie z wymaganiami nadzoru, zgodnie z którymi: a) Tworzenie łańcucha outsourcingowego powinno być każdorazowo oceniane przez podmiot nadzorowany z perspektywy przepisów prawa; b) Zakres odpowiedzialności Dostawcy usług chmurowych oraz jego podwyko-nawców wobec podmiotu nadzorowanego może ulegać ograniczeniu lub wyłączeniu wyłącznie w granicach przepisów prawa. Ad VI.2.6) z podpunktami	Ocena „łańcucha outsourcingowego" z perspek-tywy przepisów szczegółowych prawa, doty-czących konkretnie realizowanych czynności przetwarzania informacji									
20	Usługi chmury obliczeniowej wykorzy-stywane przez Dostawców IT podmiotu nadzorowanego. Podmiot nadzorowany powinien upewnić się, w jakim zakresie świadczona przez Dostawcę IT usługa wykorzystuje usługę chmury obliczeniowej, a w szczególności czy dochodzi do przetwarzania informacji prawnie chronionej, przetwarzanej w chmurze. W zależności od faktyczne-go wykorzystania usług chmurowych oraz zakresu przetwarzanych informacji podmiot nadzorowany powinien zapewnić zgodność z wymaganiami nadzoru. Ad VI.2.7) z podpunktami	Brak weryfikacji po stronie podmiotu nad-zorowanego, w jakim zakresie świadczona przez Dostawcę IT usługa wykorzystuje usługę chmury obliczeniowej, a w szczególności czy dochodzi do przetwarzania informacji prawnie chronionej, przetwarzanej w chmurze. Możli-wość braku zgodności z wymaganiami nadzoru w tym zakresie									

Lp.	Obszar zagrożenia	Opis ryzyka (należy wymienić poszczególne ryzyka występujące w danym obszarze zagrożenia)	**Obszar prawny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar organizacyjny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Obszar techniczny** (należy ocenić możliwość materializacji ryzyka w obszarze oraz opisać je)	**Ocena wpływu/ impaktu wystąpienia ryzyka inherentnego**	**Ocena prawdo-podobieństwa wystąpienia ryzyka inherentnego**	**Ocena ryzyka inherentnego** (np. wysokie, średnie, niskie, n/a)	**Czynniki ograniczające ryzyko/ mityganty** (przy poziomie ryzyka średnie, wysokie)	**Plan postępowania w przypadku wystąpienia ryzyka** (przy poziomie ryzyka średnie, wysokie)	**Ocena poziomu ryzyka rezydualnego** (np. wysokie, średnie, niskie, n/a)
21	Prawo właściwe umowy pomiędzy Dostawcą usług chmurowych 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, które pozwala na skuteczne wykonywanie postanowień umowy, spełnia wszystkie wymogi prawa polskiego, ciążące na podmiocie nadzorowanym, oraz wymagania organu nadzoru. b) W przypadku umowy poddanej prawu państwa trzeciego podmiot nadzorowany powinien posiadać opinię prawną, potwierdzającą spełnienie wymagań prawa obowiązującego podmiot nadzorowany oraz wymagań organu nadzoru. Ad VI.2.8) z podpunktami	Prawo właściwe dla umowy pomiędzy podmiotem nadzorowanym i Dostawcą usług chmurowych nie spełnia wymagań prawa polskiego i wymagań organu nadzoru. Brak opinii prawnej, potwierdzającej, że prawo, właściwe dla umowy pomiędzy podmiotem nadzorowanym i Dostawcą usług chmurowych spełnia wymagania prawa polskiego i wymagania organu nadzoru.									
22	Umowa z Dostawcą	Brak klauzul umownych wskazanych w Komunikacie									
23	..... (inne zidentyfikowane zagrożenia)										
...	.....										
	Podsumowanie	Ocena ogólnego/końcowego poziomu ryzyka rezydualnego dla projektu							Uzasadnienie dla ogólnego/końcowego poziomu ryzyka rezydualnego dla projektu		

Załącznik nr 5

do Standardu PolishCloud 2.0

Okresowe monitorowanie umów

Banki, powierzając czynności/usługi na zewnątrz, zobowiązane są nie tylko identyfikować, oceniać i monitorować wszelkie ryzyka wynikające z umów z Dostawcami, ale także zarządzać tymi ryzykami.

W celu zapewnienia kompleksowego procesu zarządzania ryzykiem powierzania Dostawcom wykonywania czynności należy okresowo weryfikować: zakres i skalę powierzenia, aktualność zapisów umownych oraz prawidłowość realizacji przedmiotu umowy przez Dostawcę.

Procedury w zakresie monitorowania zakresu współpracy z Dostawcami powinny określać m.in. cele procesu, założenia, podział ról, opis procesu zarządzania Dostawcami oraz uwzględniać proces raportowania. Prawidłowo zdefiniowany proces zarządzania współpracą z Dostawcami powinien umożliwić przewidywanie oraz sprawne rozwiązywanie potencjalnych problemów towarzyszących powierzeniu wykonywania procesu poza organizację, zwiększenie efektywności współpracy poprzez dostosowywanie warunków umów do rzeczywistych potrzeb Banku oraz zapewnienie realizacji przedmiotu umowy na poziomie zgodnym z oczekiwaniami Banku określonymi w umowie z Dostawcą.

Usługa przetwarzania informacji w chmurze obliczeniowej może narażać Banki na nowe kategorie zagrożeń, które w przypadku nieodpowiedniego mitygowania i zarządzania mogą wywołać negatywne konsekwencje dla Banku oraz jego klientów. Zapewnienie bezpieczeństwa przetwarzanych informacji istotnych dla procesów i działalności Banku lub stanowiących informacje prawnie chronione, jak również zgodności sposobu i zakresu przetwarzania z prawem, jest dla Banku zadaniem priorytetowym. Stosowanie nieodpowiednich mechanizmów identyfikowania, oceny i monitorowania ryzyk wynikających z zastosowania technologii chmury obliczeniowej może wpłynąć na możliwość wykonywania efektywnego nadzoru nad informacjami chronionymi, które zostały powierzone Dostawcy i są przetwarzane w chmurze obliczeniowej, a to z kolei może narazić Bank na utratę zaufania klientów. Wydaje się oczywistym, że identyfikacja i analiza ryzyk specyficznych dla technologii chmury obliczeniowej nie może kończyć się na etapie procesu zakupowego. Równie ważne jest, a z wraz z upływem czasu nawet ważniejsze, aby podobny wysiłek, który został włożony w szacowanie i mitygowanie ryzyka w momencie wdrażania projektu, został włożony w monitorowanie Dostawcy usługi chmury obliczeniowej przez cały okres trwania współpracy.

W związku z powyższym oraz w kontekście Komunikatu Urzędu Komisji Nadzoru Finansowego dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej rekomenduje się:

1. Zapobieganie wystąpieniu ryzyka związanego z wykorzystaniem technologii chmury obliczeniowej.

   W celu zaadresowania potencjalnego ryzyka przetwarzania informacji prawnie chronionych w chmurze obliczeniowej bez wiedzy i zgody Banku rekomenduje się dodanie do umów standardowej klauzuli zobowiązującej Dostawców do informowania Banku o planowanym rozpoczęciu wykorzystywania usługi chmury obliczeniowej, w celu świadczenia usług na rzecz Banku, w sytuacji gdy wiązałoby się to z przetwarzaniem informacji prawnie chronionych powierzonych Dostawcy przez Bank i zobowiązującej Dostawcę do uzyskania od Banku zgody na takie przetwarzanie.

2. Zarządzanie ryzykiem związanym z wykorzystaniem technologii chmury obliczeniowej.

   W przypadku podpisanej umowy realizowanej przy wykorzystaniu technologii chmury obliczeniowej, w celu zapewnienia, że nie uległy zmianie m.in.:

   - zakres, rodzaj, klasyfikacja oraz wartość informacji powierzonych Dostawcy i przetwarzanych w chmurze obliczeniowej,
   - wymagania prawa oraz postanowienia i zobowiązania umowne Banku, które mogłyby stanowić przeciwskazania do przetwarzania informacji w chmurze obliczeniowej, jak również,
   - że nie nastąpił wzrost ryzyka, które wiąże się z istniejącą umową powierzenia, a tym samym nie zmieniła się zdolność Banku do transferowania i akceptacji ryzyka,

   należy dokonać, nie rzadziej niż raz do roku, analizy następujących obszarów:

   a) rodzaj informacji prawnie chronionych przetwarzanych w chmurze obliczeniowej;
   b) skala przetwarzania informacji prawnie chronionych przetwarzanych w chmurze obliczeniowej;
   c) wartość przetwarzanych informacji;
   d) czy zmieniło się otoczenie prawne, regulacje, regulaminy lub postanowienia umów, których stroną jest Bank, oraz czy wpływa to albo może wpływać na zgodność postępowania Banku w kontekście przetwarzania informacji prawnie chronionych w chmurze obliczeniowej;
   e) czy zmieniło się otoczenie prawne związane z jurysdykcją kraju, w którym odbywa się fizycznie przetwarzanie informacji (lokalizacja centrum przetwarzania danych), w szczególności czy zmiany spowodowały, że dopuszczalne jest żądanie dostępu do przetwarzanych w CDP informacji podmiotu nadzorowanego dla organów administracji krajowej lub międzynarodowej bez zgody podmiotu nadzorowanego;
   f) czy nie zmienił się podmiot świadczący usługę chmury obliczeniowej lub jego poddostawcy, jak również ich dane rejestrowe;
   g) czy zmieniła się lokalizacja Centrum Przetwarzania Danych Dostawcy/poddostawcy usług chmury obliczeniowej;
   h) efektywność stosowanych mechanizmów kontrolnych i monitorujących, w szczególności:
      - czy wystąpiły nowe zagrożenia/ryzyka;
      - czy wystąpiły zmiany w wykorzystywanej usłudze chmury obliczeniowej lub trybie i zakresie jej wykorzystywania;
      - czy wystąpiły incydenty bezpieczeństwa lub nieprawidłowości w procesach dotyczących zarządzania logami, zarządzania kluczami szyfrującymi;

- czy wystąpiły zmiany w relacji z Dostawcą usług chmury obliczeniowej;
- czy wystąpiły inne problemy zidentyfikowane w trakcie trwania umowy;

i) czy Bank planuje przetwarzać nowy rodzaj informacji w chmurze obliczeniowej;

j) czy Bank planuje wykorzystać nową usługę chmury obliczeniowej.

W przypadku zidentyfikowania jakichkolwiek zmian/nieprawidłowości w zakresie wskazanym powyżej należy rozważyć zweryfikowanie nw. obszarów oraz, w razie konieczności, zaktualizowanie nw. formularzy:

a) formularz/e służące do klasyfikacji i oceny informacji oraz szacowania wartości informacji;

b) formularz/e służące do szacowania ryzyka, a dokładniej należy ocenić wpływ zmian na poszczególne ryzyka zidentyfikowane w związku z przetwarzaniem informacji prawnie chronionych w chmurze obliczeniowej;

c) plan przetwarzania informacji w chmurze obliczeniowej;

d) środki techniczne oraz zasoby organizacyjne, w szczególności zasoby ludzkie posiadające właściwe kompetencje techniczne;

e) plany ciągłości działania/strategia wyjścia;

f) inne dokumenty przygotowane przez Bank w celu zaadresowania postanowień Komunikatu UKNF w ww. obszarze.

Zidentyfikowanie zmian w wyżej wymienionych obszarach może wiązać się także z koniecznością zmiany umowy z Dostawcą usług chmurowych, przeprowadzenia ponownie procesu aktualizacji zakresu przetwarzanych informacji, szacowania ryzyka, uspójnienia pozostałej dokumentacji oraz aktualizacji zgłoszenia usług do UKNF.

Rekomenduje się, aby okresowe monitorowanie było udokumentowane oraz archiwizowane.

Załącznik nr 6

do Standardu PolishCloud 2.0

Wymagania dla Dostawców usług chmurowych zgodnie z Komunikatem

Index	Wymaganie	Opis wymagania	Wymagania po stronie Dostawcy	Produkty (odnoszą się do wymagań po stronie Dostawcy)
V.1-5	Wytyczne do klasyfikacji i oceny informacji	Podmiot nadzorowany przeprowadza w udokumentowanym procesie klasyfikację i ocenę informacji pod kątem dopuszczalności ich przetwarzania w chmurze obliczeniowej.	1. Dostawca powinien określić lokalizacje CPD, w których przetwarzane są informacje Banku (kraj, region). 2. Wszelkie zmiany obszaru przetwarzania danych wymagają uprzedniej zgody Banku.	1. Dokumentacja w zakresie lokalizacji CPD oraz obszaru przetwarzania danych (informacje o tym, jakie usługi świadczone są w poszczególnych lokalizacjach). 2. Proces informowania o zmianie obszaru przetwarzania danych.
VI.1-6	Wytyczne do szacowania ryzyka	Podmiot nadzorowany przeprowadza w udokumentowanym procesie kompleksowe szacowanie ryzyka.	Dostawca powinien dostarczyć Bankowi poniższe informacje: 1. Informacje o rozproszeniu geograficznym przetwarzanych informacji. 2. Informacje o zasadach dostępu do przetwarzanych informacji przez pracowników i współpracowników (np. poddostawców) Dostawcy usług chmurowych. 3. Dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się przetwarzanie, w szczególności odniesienie do katalogu sytuacji (lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu. 4. Informacje o mechanizmach izolacji zasobów używanych do świadczenia usług chmury obliczeniowej, w tym informacje o incydentach bezpieczeństwa związanych z naruszeniem mechanizmów izolacji. 5. Informacje o możliwości migracji usługi/danych do innych Dostawców chmurowych w celu mitygacji przywiązanie do jednego Dostawcy usług chmury obliczeniowej. 6. Informacje o interfejsach zarządzających usługami, które są udostępniane przez Dostawców usług chmurowych i ich podatnościach. 7. Informacje o możliwości wpływania na zakres, kształt i zmiany usług, w tym w szczególności na proces retencji przetwarzanych informacji oraz ich usuwania po zakończeniu realizacji usług przetwarzania. 8. Informacje o możliwości kontrolowania Dostawcy usług chmury obliczeniowej oraz jego podwykonawców, w tym bezpośredniej weryfikacji fizycznych, technicznych oraz organizacyjnych mechanizmów zabezpieczeń i kontroli świadczenia usług chmury obliczeniowej. 9. Informacje o możliwości kontrolowania jakości usług chmury obliczeniowej. 10. Informacje o podziale odpowiedzialności za bezpieczeństwo przetwarzanych informacji pomiędzy Dostawcą usług chmury obliczeniowej a podmiotem nadzorowanym. 11. Możliwości kontroli dostępu i urządzeń dostępowych użytkowników końcowych. 12. Zasady zmiany warunków umowy. 13. Informacje o wykorzystywanych poddostawcach i zakresu świadczonych przez nich usług oraz informacja o ich dostępie do danych.	1. Patrz V.1-5. 2. Patrz VII.3.2. 3. Opinie prawne w zakresie możliwości pozaumownego dostępu do przetwarzanych informacji, gwarantowanego przez jurysdykcję kraju, w którym odbywa się przetwarzanie danych. 4. Patrz VII.3.2. 5. Patrz VII.3.2. 6. Patrz VII.3.2. 7. Zasady żądania i wprowadzania żądanych zmian. 8. Zasady kontroli Dostawcy, w szczególności: a) zasady dostępu do dokumentacji certyfikacyjnej, b) zasady dostępu do wyników audytów i testów bezpieczeństwa, c) zasady prowadzenia kontroli pośredniej i bezpośredniej. 9. Docelowe SLA oraz zasady nadzoru nad jakością świadczonych usług. 10. Patrz VII.3.2. 11. Mechanizmy kontroli użytkowników i urządzeń przy dostępie do usługi chmurowej. 12. Zasady zmiany warunków usługi. 13. Lista poddostawców wraz z zakresem świadczonych przez nich zadań i inf. o dostępie do danych Banku.

Index	Wymaganie	Opis wymagania	Wymagania po stronie Dostawcy	Produkty (odnoszą się do wymagań po stronie Dostawcy)
VII.3.1	Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej	Zapewnienie kompetencji	1. Określenie wymaganych kompetencji przy korzystaniu z usługi, określenie ścieżek szkoleniowych i certyfikacyjnych.	1. Lista wymaganych i zalecanych szkoleń/certyfikatów przy korzystaniu z usługi dla poszczególnych ról oraz lista rekomendowanych przez Dostawcę ról wynikająca z podziału odpowiedzialności pomiędzy Bankiem a Dostawcą.
VII.3.2	Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej	Podział obowiązków i konsekwencje stosowania	1. Jasne określenie podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji przy korzystaniu z usługi. 2. Umożliwienie Bankowi zrozumienie konsekwencji stosowania określonej architektury środowiska chmury obliczeniowej oraz zasad jej konfiguracji.	1. Dokumentacja określająca podział odpowiedzialności za bezpieczeństwo informacji pomiędzy Bankiem a Dostawcą usług. 2. Dokumentacja określająca zasady konfiguracji usługi. 2.1. Architektura usługi. 2.2. Dokumentacja kluczowych kwestii bezpieczeństwa usługi, w szczególności: a) opis i zakres przetwarzanych informacji oraz informacja, jeżeli stosowane, o ich pseudonimizacji lub anonimizacji; b) sposób szyfrowania informacji oraz miejsce i/lub sposób przechowywania kluczy szyfrujących, zarówno „at rest", jak i „in transit"; c) potwierdzenie, że używane algorytmy szyfrowania nie są powszechnie uważane za skompromitowane; d) informacja o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany; e) dokumentacja dedykowanych i/lub zalecanych przez Dostawcę ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług, w szczególności w zakresie szyfrowania przetwarzanych informacji; f) szczegółowe i aktualne instrukcje konfiguracji usług oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji; g) opis mechanizmów logowania oraz możliwość przekazywania logów do SIEM po stronie Banku; h) Informacje o mechanizmach izolacji zasobów używanych do świadczenia usług chmury obliczeniowej; i) dokumentacja wytycznych, wzorcowych konfiguracji, opisów zasad itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji; j) Informacje o interfejsach zarządzających usługami, które są udostępniane przez Dostawców usług chmurowych i ich podatnościach (wyniki badania podatności lub testów bezpieczeństwa); k) dokumentacja potwierdzająca natywne uruchamianie nowego środowiska i/lub usługi separowanego od innych tenantów, z ustawieniami „secure-by-default". 2.3. Opis mechanizmów dostępu zdalnego Dostawcy uwzględniający poniższe wymagania: a) uwierzytelnienie dwuskładnikowe przy dostępie zdalnym do środowiska chmurowego; b) możliwość dostępu zdalnego z bezpiecznych lokalizacji sieciowych; c) możliwość nagrywania sesji administracyjnych oraz wgląd przez personel Banku w nagrania sesji.

Index	Wymaganie	Opis wymagania	Wymagania po stronie Dostawcy	Produkty (odnoszą się do wymagań po stronie Dostawcy)
VII.4	Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej	Umowa z Dostawcą usług chmury obliczeniowej	1. Podpisanie umowy outsourcingu zgodnie z Prawem bankowym. 2. Zawarcie w umowie wymagań określonych w pkt VII.4.1 Komunikatu chmurowego. 3. Informacja o prawie właściwym dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów).	1-2. Potwierdzenie zgody na zawarcie umowy zgodnej z załączonymi klauzulami umownymi. 3. Informacja o prawie właściwym dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów). 3.1 W przypadku poddania umowy prawu państwa trzeciego analiza prawna dotycząca możliwości skutecznego wykonywania postanowień umowy, wszystkich wymagań prawa polskiego ciążących na Banku oraz wytycznych organu nadzoru w zakresie Komunikatu.
VII.5	Minimalne wymagania dla przetwarzania informacji w chmurze obliczeniowej	Plan przetwarzania informacji w chmurze obliczeniowej (5.1)	1. Informacje o architekturze i konfiguracji usługi stanowiące wkład do opracowania planu przetwarzania informacji w chmurze obliczeniowej.	Patrz VII.3.2.
VII.6.1-2,5	Wymagania dla Dostawców usług chmury obliczeniowej	Zgodność Dostawcy z normami	W zakresie świadczonych usług Dostawca usług chmury obliczeniowej spełnia łącznie wymagania zapewnienia zgodności swojego działania z normami lub ich odpowiednikami w polskim lub europejskim układzie normalizacji, chyba że podmiot nadzorowany akceptuje (na podstawie wyników szacowania ryzyka) brak konieczności spełnienia tego wymagania albo jego części. 1. PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT; 2. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji; 3. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania; 4. ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej; 5. ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej. 6. 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, przy czym Bank może zaakceptować (w uzasadnionych przypadkach i na podstawie szacowania ryzyka) brak spełnienia części wymagań.	Dokumentacja potwierdzająca zgodność z normami (o ile dotyczy): 1. PN-ISO/IEC ISO 20000 dotyczące zarządzania usługami IT; 2. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji; 3. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania; 4. ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej; 5. ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej. 6. PN-EN 50600 minimum klasy 3 lub ANSI/TIA-942 minimum Tier III. Dopuszczalne dokumenty: - Certyfikaty potwierdzające zgodność z normami; - Oświadczenie Dostawcy o spełnieniu wymogów norm.
VII.6.3	Wymagania dla Dostawców usług chmury obliczeniowej	Lokalizacja CPD	1. Zaleca się, aby CPD było zlokalizowane na terenie EOG (o ile jest to uzasadnione z perspektywy kosztowej, jakościowej, ryzyka etc.) 2. Banki będące operatorami usługi kluczowej powinny preferować CPD w Polsce.	1. Patrz V.1-4.

Index	Wymaganie	Opis wymagania	Wymagania po stronie Dostawcy	Produkty (odnoszą się do wymagań po stronie Dostawcy)
VII.6.4	Wymagania dla Dostawców usług chmury obliczeniowej	Ochrona informacji i kontrola dostępu	Wymagania w zakresie ochrony informacji: 1. Domyślna zasada 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. Zasada „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 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".	Potwierdzenie spełnienia wymagań w zakresie ochrony informacji poprzez opis mechanizmów lub wskazanie zapisów umownych/proceduralnych zapewniających poniższą funkcjonalność: 1. Domyślna zasada braku dostępu do przetwarzanych informacji przez Dostawcę. 2. Brak konta administracyjnego lub użytkownika na maszynach wirtualnych podmiotu nadzorowanego i/lub w innych uruchamianych usługach. 3. Realizacja zasady „minimum koniecznego" dla uprawnień serwisowych nadawanych wyłącznie w sytuacji konieczności wykonania czynności wymaganych przez podmiot nadzorowany oraz na czas ich trwania, logowanie zdarzeń, przy czym realizacja czynności poprzedzona jest zleceniem podmiotu nadzorowanego, a cały proces obsługi i wykonania czynności jest logowany. OPCJONALNIE: Stosowny certyfikat (np. SOC 2 Type 2) wydany przez niezależną jednostkę certyfikującą akredytowaną w europejskim systemie akredytacji dla mechanizmu kontroli dostępu serwisowego.
VII.7	Wymagania dla Dostawców usług chmury obliczeniowej	Kryptografia	Informacje w chmurze obliczeniowej muszą być szyfrowane. Wymagania: 1. Dostarczenie szczegółowych i aktualnych instrukcji konfiguracji usług oraz metod weryfikacji poprawności ich konfiguracji i działania, w szczególności w zakresie szyfrowania przetwarzanych informacji. 2. Używanie dedykowanych i/lub zalecanych przez Dostawcę ustawień konfiguracyjnych podnoszących bezpieczeństwo świadczonych usług, w szczególności w zakresie szyfrowania przetwarzanych informacji. 3. Szyfrowanie zarówno „at rest", jak i „in transit" informacji prawnie chronionych przetwarzanych w chmurze obliczeniowej. 4. Informacje są szyfrowane kluczami generowanymi i/lub dostarczonymi oraz zarządzanymi przez podmiot nadzorowany. 5. Używane algorytmy szyfrowania nie są powszechnie uważane za skompromitowane. 6. 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 140-2 Level 2 lub równoważne. 7. 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, chyba że z oszacowania ryzyka wynika uzasadniony brak takiej potrzeby.	1-3. Patrz VII.3.2. 4. Możliwość szyfrowania kluczami generowanymi i/lub dostarczonymi oraz zarządzanymi przez podmiot nadzorowany, opis techniczny rozwiązania. 5. Patrz VII.3.2. 6. Możliwość wykorzystania własnego HSM lub HSM od Dostawcy – opis techniczny rozwiązania; potwierdzenie Dostawcy, że HSM spełnia wymagania FIPS 140-2 Level 2 lub równoważne. 7. W przypadku gdy klucze zostały wygenerowane lub są zarządzane przez Dostawcę usług chmury obliczeniowej, możliwość przechowywania w ramach własnej infrastruktury kopii kluczy szyfrujących w ramach infrastruktury Banku kopii kluczy szyfrujących.
VII.8	Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej	Logowanie zdarzeń	Dostawca zapewnia mechanizmy logowania zdarzeń oraz dostęp Banku do logów: 1. Logi mogą być przekazywane do Banku, w szczególności do SIEM. 2. Logi są zabezpieczone przez przed nieautoryzowanym dostępem, modyfikacją lub usunięciem.	Patrz VII.3.2.

Index	Wymaganie	Opis wymagania	Wymagania po stronie Dostawcy	Produkty (odnoszą się do wymagań po stronie Dostawcy)
VII.8.4	Monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej	Dostęp zdalny do środowiska chmurowego	Dostęp zdalny do środowiska chmurowego: 1. Jest możliwy tylko dla uprawnionego personelu Dostawcy. 2. Wymaga stosowania MFA. 3. Jest inicjowany z określonych, bezpiecznych lokalizacji sieciowych. 4. Jest realizowany pod nadzorem Banku (np. poprzez nagrywanie sesji).	Patrz VII.3.2.

Załącznik nr 7

do Standardu PolishCloud 2.0

Ankieta dla Dostawców

Celem niniejszego dokumentu jest usystematyzowanie oczekiwanych informacji od Dostawcy usług chmury obliczeniowej, związanych z uruchamianiem przez Bank usługi chmurowej.

Zebrane przykładowe pytania odnoszą się do wymagań w stosunku do Dostawcy usług chmury obliczeniowej, wskazanych w Komunikacie Urzędu Nadzoru Finansowego, jak również zostały oparte o doświadczenia własne banków, których przedstawiciele uczestniczyli w opracowaniu „Standard PolishCloud 2.0".

Opis ryzyka	Numer pytania	Pytanie do Dostawcy	Wskazówki/wymagania dla dostarczanych dowodów	Odpowiedź Dostawcy (powinna zawierać informacje zgodne ze wskazówkami umieszczonymi w sąsiedniej kolumnie)
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	1	W jakich lokalizacjach Dostawca będzie przetwarzał informacje podmiotu nadzorowanego? / Gdzie zlokalizowane jest CPD Dostawcy?	Informacja o lokalizacji powinna być udzielana przynajmniej poprzez podanie miejscowości lub regionu kraju. W uzasadnionych przypadkach można podać informację o tym, czy CDP znajduje się w Europejskim Obszarze Gospodarczym czy poza nim. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt.1	
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	2	Z jakich lokalizacji nawiązywany będzie dostęp do informacji podmiotu nadzorowanego przechowywanych w CPD Dostawcy?	Informacja o lokalizacji powinna być udzielana przynajmniej poprzez podanie miejscowości lub regionu kraju. W uzasadnionych przypadkach można podać informację o tym, czy CDP znajduje się w Europejskim Obszarze Gospodarczym czy poza nim.	
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	3	Dostawca oświadcza, że posiada wszelkie koncesje, zgody lub certyfikaty wymagane prawem lokalnym dla prowadzenia działalności w zakresie świadczenia usługi dla podmiotu nadzorowanego.	Proszę załączyć kopie/skany stosownych dokumentów.	
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	4	Czy Dostawca wdrożył proces informowania podmiotu nadzorowanego o zmianie lokalizacji?	W odpowiedzi proszę zamieścić skrócony opis. Dodatkowo należy przekazać podmiotowi nadzorowanemu stosowny dokument opisujący proces lub wyciąg z niego.	
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	5	Czy Dostawca usługi potwierdza zgodność działania z PN-ISO/IEC ISO 20000 (zarządzanie usługami IT)?	W przypadku dysponowania certyfikatem Dostawca powinien przekazać podmiotowi nadzorowanemu jego kopię lub w inny sposób umożliwić potwierdzenie certyfikacji.	
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	6	Czy Dostawca usługi potwierdza zgodność działania z PN-EN ISO/IEC 27001 (zarządzanie bezpieczeństwem informacji)?	W przypadku dysponowania certyfikatem Dostawca powinien przekazać podmiotowi nadzorowanemu jego kopię lub w inny sposób umożliwić potwierdzenie certyfikacji.	
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	7	Czy Dostawca usługi potwierdza zgodność działania zPN-EN ISO 22301 (zarządzanie ciągłością działania)?	W przypadku dysponowania certyfikatem Dostawca powinien przekazać podmiotowi nadzorowanemu jego kopię lub w inny sposób umożliwić potwierdzenie certyfikacji.	
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	8	Czy Dostawca usługi potwierdza zgodność działania z ISO/IEC 27017 (bezpieczeństwo informacji w chmurze obliczeniowej)?	W przypadku dysponowania certyfikatem Dostawca powinien przekazać podmiotowi nadzorowanemu jego kopię lub w inny sposób umożliwić potwierdzenie certyfikacji.	

Opis ryzyka	Numer pytania	Pytanie do Dostawcy	Wskazówki/wymagania dla dostarczanych dowodów	Odpowiedź Dostawcy (powinna zawierać informacje zgodne ze wskazówkami umieszczonymi w sąsiedniej kolumnie)
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	**9**	Czy Dostawca usługi potwierdza zgodność działania z ISO/IEC 27018 (zabezpieczanie danych osobowych w chmurze obliczeniowej), o ile ma to zastosowanie?	W przypadku dysponowania certyfikatem Dostawca powinien przekazać podmiotowi nadzorowanemu jego kopię lub w inny sposób umożliwić potwierdzenie certyfikacji.	
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	**10**	Czy Dostawca usługi potwierdza zgodność działania CPD z ANSI/TIA-942 minimum Tier III, PN-EN 50600 minimum klasy 3 lub innym normatywnym odpowiednikiem (proszę go wskazać)?	W przypadku dysponowania certyfikatem Dostawca powinien przekazać podmiotowi nadzorowanemu jego kopię lub w inny sposób umożliwić potwierdzenie certyfikacji.	
Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a)	**11**	Czy Dostawca oświadcza, że posiada wszelkie koncesje, zgody lub certyfikaty wymagane prawem lokalnym dla prowadzenia działalności w zakresie świadczenia usługi dla Banku?	Proszę przekazać kopię dokumentu potwierdzającego stosowne uprawnienie do prowadzenia działalności.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**12**	Czy Dostawca zapewnia realizację zasady domyślnego braku dostępu do informacji podmiotu nadzorowanego przetwarzanych w usłudze?	Proszę opisać praktyczne zastosowanie zasady domyślnego braku dostępu.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**13**	Jakie podmioty mogą mieć dostęp do informacji podmiotu nadzorowanego przetwarzanych w usłudze i jak ten dostęp jest nadawany, zarządzany, odbierany oraz kontrolowany?	Proszę wskazać listę podmiotów obejmującą nazwę, siedzibę, zakres dostępu, cel uzyskania dostępu, sposób jego przydzielania, modyfikacji, odbierania i kontroli.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**14**	Czy pracownicy Dostawcy mogą mieć dostęp do informacji podmiotu nadzorowanego przetwarzanych w usłudze? Jeśli tak, prosimy o określenie zasad przyznawania takiego dostępu.	W odpowiedzi proszę zamieścić skrócony opis. Dodatkowo należy przekazać podmiotowi nadzorowanemu stosowny dokument opisujący proces lub wyciąg z niego. Ponadto proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 2.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**15**	Czy pracownicy poddostawców mogą mieć dostęp do informacji podmiotu nadzorowanego przetwarzanych w usłudze?	Podmiot nadzorowany oczekuje, że pracownicy poddostawców nie będą mieli dostępu do danych podmiotu nadzorowanego przetwarzanych w usłudze. Dostęp pracowników poddostawców należy uzasadnić. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 2.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**16**	Czy proces Dostawcy uwzględnia uzyskanie zgody podmiotu nadzorowanego dla nadania pracownikowi Dostawcy takiego dostępu?	Proszę zamieścić skrócony opis. Należy przekazać podmiotowi nadzorowanemu stosowny dokument opisujący proces lub wyciąg z niego.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**17**	Należy przekazać Bankowi stosowną dokumentację pokazującą możliwość zapewnienia aktualizacji stosu technologicznego usługi chmury obliczeniowej bez tworzenia na maszynach wirtualnych kont administracyjnych dla Dostawcy. Taki dostęp byłby niezgodny z wymaganiami Komunikatu opisanymi w VII.6.4.b. Jeśli dostęp administracyjny w innych uruchamianych usługach chmury obliczeniowej jest niezbędny do jej świadczenia, wówczas Dostawca, zachowując zasadę minimum koniecznego dostępu, powinien przedstawić dokumentację opisującą zakresy uprawnień i sposoby aktualizacji i utrzymania usług.	Proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 12.	

Opis ryzyka	Numer pytania	Pytanie do Dostawcy	Wskazówki/wymagania dla dostarczanych dowodów	Odpowiedź Dostawcy (powinna zawierać informacje zgodne ze wskazówkami umieszczonymi w sąsiedniej kolumnie)
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**18**	Co do zasady dostęp do kont administracyjnych usług chmurowych powinien być ograniczony do osób współpracujących oraz pracowników Dostawcy. Jeśli jednak taki dostęp administracyjny dla poddostawcy jest niezbędny do jej świadczenia, wówczas Dostawca, zachowując zasadę minimum koniecznego dostępu, powinien przedstawić Bankowi dokumentację opisującą zakresy uprawnień. Dostęp pracowników poddostawców należy uzasadnić.	Proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 12.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**19**	Jak wygląda podział odpowiedzialności za bezpieczeństwo informacji pomiędzy podmiot nadzorowany a Dostawcę w ramach usługi?	W odpowiedzi proszę zamieścić skrócony opis. Dodatkowo należy przekazać podmiotowi nadzorowanemu stosowny dokument opisujący proces lub wyciąg z niego.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**20**	Czy dostęp zdalny do środowiska chmurowego odbywa się z wykorzystaniem uwierzytelnienia wieloskładnikowego?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 13.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**21**	Czy dostęp zdalny do środowiska chmurowego jest realizowany wyłącznie z bezpiecznych lokalizacji sieciowych Banku i/lub Dostawcy?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**22**	Czy Dostawca nagrywa sesje administracyjne i udostępnia nagrania personelowi podmiotu nadzorowanego?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**23**	Czy Dostawca usługi posiada mechanizmy weryfikacji przyznanych uprawnień?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**24**	Czy Dostawca usługi będzie zbierał logi zgodne z wytycznymi Banku związane z dostępem do danych podmiotu nadzorowanego przetwarzanych w usłudze chmury obliczeniowej?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 15.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**25**	Czy Dostawca będzie zabezpieczał logi związane z dostępem do informacji podmiotu nadzorowanego przetwarzanych w usłudze przed nieautoryzowanym dostępem, modyfikacją lub usunięciem?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 16.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**26**	Czy Dostawca jest w stanie dostosować okres retencji zbieranych logów do wymagań Banku w tym zakresie?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c)	**27**	Czy Dostawca usługi zapewnia przekazywanie logów do Banku i integrację z SIEM?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 17.	

Opis ryzyka	Numer pytania	Pytanie do Dostawcy	Wskazówki/wymagania dla dostarczanych dowodów	Odpowiedź Dostawcy (powinna zawierać informacje zgodne ze wskazówkami umieszczonymi w sąsiedniej kolumnie)
Dostęp do przetwarzanych informacji, gwarantowany przez jurysdykcję kraju, w którym odbywa się fizycznie przetwarzanie (lokalizacja centrum przetwarzania danych), w szczególności odniesienie do katalogu sytuacji (lub podmiotów), w której możliwe jest żądanie informacji lub dostępu do nich bez wyraźnej zgody podmiotu nadzorowanego. (VI.2.1) d)	**28**	Czy na gruncie jurysdykcji kraju, w którym zlokalizowane jest CPD Dostawcy/z którego obszaru nawiązywany jest dostęp do informacji przetwarzanych w CDP Dostawcy, dopuszczalne jest żądanie dostępu do przetwarzanych w CDP informacji podmiotu nadzorowanego dla organów administracji krajowej lub międzynarodowej bez zgody podmiotu nadzorowanego?	Wskazanie listy podmiotów administracji krajowej lub międzynarodowej wraz z wyciągiem z przepisów prawa, na podstawie których realizowane jest uprawnienie.	
Przywiązanie do jednego Dostawcy usług chmury obliczeniowej (VI.2.1.e)	**29**	Prosimy o przekazanie dokumentacji opisującej architekturę usługi.	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Przywiązanie do jednego Dostawcy usług chmury obliczeniowej (VI.2.1.e)	**30**	Prosimy o przekazanie dokumentacji określającej zasady konfiguracji usługi.	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Przywiązanie do jednego Dostawcy usług chmury obliczeniowej (VI.2.1.e)	**31**	Czy Dostawca jest w stanie zwrócić podmiotowi nadzorowanemu informacje przetwarzane w usłudze w sposób i w formacie wskazanym przez podmiot nadzorowany?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Przywiązanie do jednego Dostawcy usług chmury obliczeniowej (VI.2.1.e)	**32**	Czy Dostawca będzie wspierał podmiot nadzorowany w zakresie migracji do infrastruktury innego Dostawcy chmury obliczeniowej?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Awarie i podatności elementów technologicznych chmury obliczeniowej (VI.2.1.f)	**33**	Prosimy o podanie informacji o zastosowanych mechanizmach izolacji zasobów używanych do świadczenia usług chmury obliczeniowej.	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 3.	
Awarie i podatności elementów technologicznych chmury obliczeniowej (VI.2.1.f)	**34**	Prosimy o dostarczenie dokumentacji wytycznych, wzorcowych konfiguracji, opisów zasad itp., które w jednoznaczny sposób definiują separację przetwarzania oraz wskazują na metody weryfikacji poprawności konfiguracji.	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Awarie i podatności elementów technologicznych chmury obliczeniowej (VI.2.1.f)	**35**	Czy w ramach świadczonej usługi w ciągu ostatnich 5 lat zdarzyły się incydenty bezpieczeństwa obejmujące naruszenia mechanizmów izolacji?	Prosimy o krótki opis zaistniałych incydentów i zastosowanych w związku z ich zaistnieniem środków. Należy załączyć listę incydentów.	

Opis ryzyka	Numer pytania	Pytanie do Dostawcy	Wskazówki/wymagania dla dostarczanych dowodów	Odpowiedź Dostawcy (powinna zawierać informacje zgodne ze wskazówkami umieszczonymi w sąsiedniej kolumnie)
Awarie i podatności elementów technologicznych chmury obliczeniowej (VI.2.1.f)	**36**	Prosimy o zamieszczenie dokumentacji potwierdzającej natywne uruchamianie nowego środowiska i/lub usługi separowanego od innych tenantów, z ustawieniami „secure-by-default"?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Awarie i podatności elementów technologicznych chmury obliczeniowej (VI.2.1.f)	**37**	Proszę o dostarczenie informacji o sposobie konfiguracji usługi w zakresie mechanizmów backupu danych.	Proszę zamieścić skrócony opis procesu. Należy przekazać podmiotowi nadzorowanemu stosowny dokument opisujący proces lub wyciąg z niego. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 18.	
Podatność interfejsów zarządzających usługami, które są udostępniane przez Dostawcę usług chmurowych (VI.2.1. g)	**38**	Prosimy o informacje o interfejsach zarządzających usługami, które są udostępniane przez Dostawców usług chmurowych i ich podatnościach (wyniki badania podatności lub testów bezpieczeństwa).	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 4.	
Ograniczona możliwość wpływania na zakres, kształt i zmiany usług (VI.2.1.h)	**39**	Czy Dostawca wdrożył w organizacji proces informowania podmiotu nadzorowanego o zmianach wprowadzanych w świadczonych usługach?	Proszę zamieścić skrócony opis procesu. Należy przekazać podmiotowi nadzorowanemu stosowny dokument opisujący proces lub wyciąg z niego.	
Ograniczona możliwość wpływania na zakres, kształt i zmiany usług (VI.2.1.h)	**40**	Czy Dostawca gwarantuje prawo własności informacji podmiotu nadzorowanego przetwarzanych w usłudze zarówno w czasie korzystania z usługi, jak i po zakończeniu umowy (rozwiązaniu, w tym także nieplanowanym, wygaśnięciu) z Dostawcą?		
Ograniczona możliwość wpływania na zakres, kształt i zmiany usług (VI.2.1.h)	**41**	Jak wygląda proces retencji informacji podmiotu nadzorowanego przetwarzanych w usłudze?	Proszę zamieścić skrócony opis procesu. Należy przekazać podmiotowi nadzorowanemu stosowny dokument opisujący proces lub wyciąg z niego. Odpowiedź powinna uwzględniać także zakres dostosowania się do oczekiwań Banku w kwestii okresu retencji danych.	
Ograniczona możliwość wpływania na zakres, kształt i zmiany usług (VI.2.1.h)	**42**	Czy Dostawca usuwa informacje podmiotu nadzorowanego przetwarzane w usłudze bezpośrednio po zakończeniu umowy (rozwiązanie, w tym także nieplanowane, wygaśnięcie) wiążącej podmiot nadzorowany z Dostawcą?	Proszę zamieścić skrócony opis procesu. Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Ograniczona możliwość kontrolowania Dostawcy usług chmury obliczeniowej (VI.2.1.i)	**43**	Proszę przedstawić zasady kontroli stosowane przez Dostawcę, w szczególności: a) zasady dostępu do dokumentacji dot. usługi b) zasady dostępu do wyników audytów i testów bezpieczeństwa c) zasady prowadzenia kontroli pośredniej i bezpośredniej	Proszę zamieścić krótki opis zasad.	
Podział odpowiedzialności (VI.2.1.j)	**44**	Proszę przedstawić zasady podziału odpowiedzialności za bezpieczeństwo informacji pomiędzy podmiot nadzorowany a Dostawcę usług.	Proszę zamieścić krótki opis zasad.	

Opis ryzyka	Numer pytania	Pytanie do Dostawcy	Wskazówki/wymagania dla dostarczanych dowodów	Odpowiedź Dostawcy (powinna zawierać informacje zgodne ze wskazówkami umieszczonymi w sąsiedniej kolumnie)
Możliwość korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego (VI.2.2.a)	**45**	Prosimy wskazać używane/dostarczane przez Dostawcę mechanizmy pozwalające na kontrolę użytkowników usługi oraz urządzeń, z których nawiązywany jest dostęp do usługi.	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Możliwość jednostronnej zmiany warunków technicznych korzystania z usługi (VI.2.2.b)	**46**	Prosimy o określenie zakresu warunków technicznych korzystania z usługi (w szczególności jej parametrów lub zasad konfiguracji) podlegających jednostronnej zmianie przez Dostawcę.	Należy załączyć listę parametrów.	
Stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług (VI.2.2.c)	**47**	Czy Dostawca stosuje zasadę zmiany domyślnych lub publicznie dostępnych parametrów usługi?	Proszę zamieścić skróconą informację dot. parametrów usługi. Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Stosowane mechanizmy uwierzytelniania (VI.2.2.d)	**48**	Proszę przedstawić stosowane w usłudze mechanizmy uwierzytelnienia?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Zasoby ludzkie (VI.2.3.a)	**49**	Prosimy dostarczyć listę rekomendowanych przez Dostawcę ról wynikającą z podziału odpowiedzialności pomiędzy podmiotem nadzorowanym a Dostawcą wraz z informacją o wymaganych i zalecanych szkoleniach/certyfikatach związanych z korzystaniem z usługi w ramach poszczególnych ról.	Należy zamieścić listę ról sugerowanych przez Dostawcę.	
Zgodność środowiska technologicznego (VI.2.3.b)	**50**	Czy Dostawca deklaruje elastyczność w zakresie integracji z innymi wskazanymi przez Bank technologiami?	W miarę możliwości prosimy o wskazanie zakresu dopuszczalnej integracji lub jej ograniczenia.	
Szyfrowanie informacji (VI.2.5)	**51**	Czy Dostawca stosuje pseudonimizację lub anonimizację informacji podmiotu nadzorowanego przetwarzanych w usłudze?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	
Szyfrowanie informacji (VI.2.5)	**52**	Czy Dostawca szyfruje przetwarzane informacje podmiotu nadzorowanego w trakcie ich przechowywania („at rest")?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 9.	
Szyfrowanie informacji (VI.2.5)	**53**	Czy Dostawca szyfruje przetwarzane informacje podmiotu nadzorowanego na czas ich przesyłu („in transit")?	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 9.	
Szyfrowanie informacji (VI.2.5)	**54**	Prosimy o wskazanie sposobu szyfrowania informacji oraz miejsca i/lub sposobu przechowywania kluczy szyfrujących, zarówno dla szyfrowania informacji w spoczynku („at rest"), jak i podczas ich przesyłu („in transit").	Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 5 oraz pkt 6.	
Szyfrowanie informacji (VI.2.5)	**55**	Czy Dostawca weryfikuje stosowane algorytmy szyfrowania z zewnętrznym wiarygodnym źródłem, aby potwierdzić, że algorytmy nie są skompromitowane?	Proszę zamieścić skrócony opis procesu. Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną.	

Opis ryzyka	Numer pytania	Pytanie do Dostawcy	Wskazówki/wymagania dla dostarczanych dowodów	Odpowiedź Dostawcy (powinna zawierać informacje zgodne ze wskazówkami umieszczonymi w sąsiedniej kolumnie)
Szyfrowanie informacji (VI.2.5)	**56**	Czy Dostawca posiada sformalizowany (udokumentowany) proces zarządzania tworzeniem, wykorzystaniem (w tym zasadami dostępu), ochroną, niszczeniem kluczy szyfrujących oraz, gdy to zasadne, przechowywaniem kopii zapasowych kluczy w infrastrukturze podmiotu nadzorowanego?	Proszę zamieścić skrócony opis procesu. Należy przekazać podmiotowi nadzorowanemu stosowną dokumentację techniczną. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 10.	
Szyfrowanie informacji (VI.2.5)	**57**	Kto zarządza kluczami szyfrującymi stosowanymi do szyfrowania danych przechowywanych w/przesyłanych do usługi?	Proszę o wskazanie podmiotów. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 7.	
Szyfrowanie informacji (VI.2.5)	**58**	Kto posiada dostęp do kluczy szyfrujących stosowanych do szyfrowania danych przechowywanych w/przesyłanych do usługi?	Proszę o wskazanie podmiotów. Dodatkowo proszę umieścić dowody w formie zrzutów ekranu/logów w pliku Ankieta dla Dostawców – udokumentowanie konfiguracji usługi pkt 8., 11.	
Szyfrowanie informacji (VI.2.5)	**59**	Czy Dostawca udostępnia urządzenia HSM dla celów utrzymywania i zarządzania kluczami szyfrującymi?	Proszę krótko opisać zasady, na jakich udostępniane są urządzenia.	
Szyfrowanie informacji (VI.2.5)	**60**	Czy urządzenia HSM udostępniane przez Dostawcę spełniają wymagania minimum FIPS 140-2 Level 2 lub równoważne?	W przypadku dysponowania certyfikatem Dostawca powinien przekazać podmiotowi nadzorowanemu jego kopię.	
Kontrola „łańcucha outsourcingowego" (VI.2.6)	**61**	Proszę wskazać wszystkich podwykonawców Dostawcy usługi wraz z zakresem świadczonych przez nich zadań i informacją o dostępie do danych podmiotu nadzorowanego.	W przypadku dysponowania certyfikatem Dostawca powinien przekazać podmiotowi nadzorowanemu jego kopię.	
Kontrola „łańcucha outsourcingowego" (VI.2.6)	**62**	Proszę wskazać okres, na jaki Dostawca zawarł z poddostawcami umowę w zakresie świadczonych przez nich usług?	Należy dostarczyć listę podmiotów, powierzonych im czynności wraz z okresem, na jaki została zawarta umowa.	
Kontrola „łańcucha outsourcingowego" (VI.2.6)	**63**	Czy Dostawca jest w stanie nałożyć na swoich podwykonawców takie same zobowiązania, jakim podlegałby na gruncie umowy z podmiotem nadzorowanym?	Należy przekazać listę podmiotów ze wskazaniem ew. ograniczeń w zakresie nałożenia zobowiązań na podwykonawców.	
Prawo właściwe umowy z Dostawcą (VI.2.8)	**64**	Czy Dostawca przewiduje poddanie umowy z podmiotem nadzorowanym prawu polskiemu lub prawu innego państwa członkowskiego EOG?	Proszę wymienić konkretny kraj.	
Prawo właściwe umowy z Dostawcą (VI.2.8)	**65**	Czy Dostawca przewiduje poddanie umowy prawu państwa trzeciego poza EOG?	Proszę wymienić konkretny kraj.	

Załącznik nr 8

do Standardu PolishCloud 2.0

Ankieta dla Dostawców usług opartych o chmurę obliczeniową

Cel:

Celem uzupełnienia ankiety jest udokumentowanie konfiguracji usługi udostępnianej Bankowi przez Dostawcę, w ramach której wykorzystywana jest zewnętrzna infrastruktura chmury obliczeniowej, zgodnie z postanowieniami „Komunikatu UKNF dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej".

1. Udokumentowanie w formie zrzutów ekranu/logów w zakresie lokalizacji CPD oraz obszaru przetwarzania danych (informacje o tym, jakie usługi świadczone są w poszczególnych lokalizacjach) – patrz Ankieta dla Dostawców pyt. 1.

   Udokumentowanie:

2. Udokumentowanie w formie zrzutów ekranu/logów, czy dostęp do przetwarzanych informacji mają wyłącznie pracownicy Dostawcy lub poddostawców – patrz Ankieta dla Dostawców pyt. 14, 15.

   Udokumentowanie:

3. Udokumentowanie w formie zrzutów ekranu/logów stosowanych mechanizmów izolacji zasobów używanych do świadczenia usług chmury obliczeniowej – patrz Ankieta dla Dostawców pyt. 33.

   Udokumentowanie:

4. Udokumentowanie w formie zrzutów ekranu/logów interfejsów zarządzających usługami chmury obliczeniowej oraz informacji o zabezpieczeniach interfejsów – patrz Ankieta dla Dostawców pyt. 38.

Udokumentowanie:

5. Udokumentowanie w formie zrzutów ekranu/logów, jakie klucze szyfrujące, jakie algorytmy szyfrowania są wykorzystywane do szyfrowania danych – patrz Ankieta dla Dostawców pyt. 54.

Udokumentowanie:

6. Udokumentowanie w formie zrzutów ekranu/logów, gdzie przechowywane są klucze szyfrujące – patrz Ankieta dla Dostawców pyt. 54.

Udokumentowanie:

7. Udokumentowanie w formie zrzutów ekranu/logów, kto zarządza kluczami szyfrującymi – patrz Ankieta dla Dostawców pyt. 57.

Udokumentowanie:

8. Udokumentowanie w formie zrzutów ekranu/logów, kto ma dostęp do kluczy szyfrujących – patrz Ankieta dla Dostawców pyt. 58.

Udokumentowanie:

9. Udokumentowanie w formie zrzutów ekranu/logów, czy informacje przetwarzane w chmurze obliczeniowej są zawsze szyfrowane. Prosimy o potwierdzenie szyfrowania danych „at rest" oraz „in transit" – patrz Ankieta dla Dostawców pyt. 52, 53.

Udokumentowanie:

10. Udokumentowanie w formie zrzutów ekranu/logów, gdzie są przechowywane kopie kluczy szyfrujących – patrz Ankieta dla Dostawców pyt. 56.

Udokumentowanie:

11. Udokumentowanie w formie zrzutów ekranu/logów, czy możliwość rozszyfrowania danych mają wyłącznie administratorzy Dostawcy – patrz Ankieta dla Dostawców pyt. 58.

Udokumentowanie:

12. Udokumentowanie w formie zrzutów ekranu/logów dostępu administracyjnego dla Dostawcy i poddostawców, jeśli jest on niezbędny do świadczenia usługi chmurowej. Dostawca, zachowując zasadę minimum koniecznego dostępu, powinien przedstawić Bankowi dokumentację opisującą zakresy uprawnień poszczególnych pracowników. Dostęp pracowników poddostawców należy uzasadnić – patrz Ankieta dla Dostawców pyt. 18.

Udokumentowanie:

13. Udokumentowanie w formie zrzutów ekranu/logów, z jakich sposobów uwierzytelniania korzystają pracownicy posiadający konta administracyjne. Czy jest to uwierzytelnianie MFA? – patrz Ankieta dla Dostawców pyt. 20.

Udokumentowanie:

14. Udokumentowanie w formie zrzutów ekranu/logów, czy sesje pracowników, administratorów Dostawcy są monitorowane i nagrywane – patrz Ankieta dla Dostawców pyt. 22.

Udokumentowanie:

15. Udokumentowanie w formie zrzutów ekranu/logów zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej – patrz Ankieta dla Dostawców pyt. 24.

Udokumentowanie:

16. Udokumentowanie w formie zrzutów ekranu/logów sposobu zabezpieczenia logów przed nieautoryzowanym dostępem, modyfikacją lub usunięciem – patrz Ankieta dla Dostawców pyt. 25.

Udokumentowanie:

17. Udokumentowanie w formie zrzutów ekranu/logów, czy jest wykorzystywane narzędzie do korelacji logów (SIEM) – patrz Ankieta dla Dostawców pyt. 27.

Udokumentowanie:

18. Udokumentowanie w formie zrzutów ekranu/logów sposobu konfiguracji, (polityki backupu) mechanizmów backupu danych – patrz Ankieta dla Dostawców pyt. 37.

Udokumentowanie:

Załącznik nr 9

do Standardu PolishCloud 2.0

Fazy projektu wdrożenia usługi przetwarzania danych w chmurze obliczeniowej – metoda kaskadowa

Wstęp

Niniejszy dokument jest uzupełnioną wersją dokumentu „Plan wdrożenia chmury", stanowiącego załącznik nr 7 Standardu PolishCloud 1.0, opublikowanego na początku 2020 roku.

Obecna wersja opisuje etapy projektu wdrożenia usługi przetwarzania danych w chmurze obliczeniowej dla projektów realizowanych metodą kaskadową. Przyjęto modelowe fazy projektu według metodyki PMBOK (ang. *Project Management Body of Knowledge*).

Opisane etapy i czynności mogą stanowić uzupełnienie/odniesienie do standardowych procesów projektowych funkcjonujących w bankach, w tym do zasad prowadzenia prac zgodnie z innymi metodykami, np. metodyką zwinną.

1. Inicjowanie projektu

Zazwyczaj efektem tego etapu jest wstępna koncepcja projektu. Koncepcja ta, w wielu przypadkach, służy temu, żeby wewnętrzni decydenci mogli ocenić szansę projektu i dać zielone światło do dalszych prac, ewentualnie odesłać założenia do korekty lub wstrzymać dalsze działania projektowe.

Na tym etapie projektu wykonywane są następujące czynności:

- Ustalenie ogólnego celu – pomysłu na projekt,
- Ustalenie wykonalności projektu (analiza ograniczeń),
- Wykonanie wstępnej analizy finansowej,
- Ustalenie sponsora/źródeł finansowania projektu.

Zwykle w ramach prowadzonych prac otwierany jest formalny projekt lub inna inicjatywa, która pozwala na alokację działań związanych z wykonywanymi czynnościami.

2. Wstępna ocena pod kątem możliwości realizacji potrzeby w usłudze chmurowej

Na tym etapie projektu rekomendowane jest dokonywanie wstępnej oceny („*pre-assessment*") potrzeby pod kątem realizacji w chmurze obliczeniowej, obejmującej np.:

- Przeprowadzenie porównania rozwiązania w usłudze chmurowej vs. wdrożenie on-premise (jeśli jest to zasadne), obejmującego wstępną ocenę możliwości realizacji wyma-

gań biznesowych, wstępne porównanie analizy finansowej dla rozwiązania chmurowego vs. wdrożenie on-premise, analizę potencjalnych Dostawców usług chmurowych;
- Wykonanie wstępnej analizy wpływu rozwiązania chmurowego na architekturę aplikacji, ocena możliwości integracji rozwiązania z innymi systemami, przybliżenie docelowej konfiguracji rozwiązania;
- Przeprowadzenie *proof of concept* rozwiązania, jeśli planowane jest wykorzystanie całkowicie nowych dla Banku technologii;
- Inwentaryzację i klasyfikację danych, klasyfikację istotności usługi – w zależności od wyników oceny podejmowana jest wstępna decyzja pod kątem outsourcingu w kontekście wytycznych EBA oraz przepisów Prawa bankowego, outsourcingu szczególnego chmury obliczeniowej oraz wymagań stosowania wytycznych Komunikatu UKNF;
- Wykonanie wstępnej oceny wymagań szyfrowania w przypadku realizacji inicjatywy w chmurze obliczeniowej;
- Zbadanie posiadanych w Banku kompetencji w zakresie usług chmurowych i on-premise oraz wykonanie analizy możliwości pozyskania brakujących kompetencji (szkolenia, kontraktorzy, rekrutacja);
- Potwierdzenie zgodności planowanej inicjatywy ze strategią Banku oraz innymi regulacjami wewnętrznymi.

3. Punkt decyzyjny/decyzja o dopuszczalności wdrożenia rozwiązania chmurowego

Na tym etapie projektu podejmowana jest decyzja o:

- Braku możliwości/zasadności wykorzystania rozwiązania chmurowego i o realizacji projektu on-premise;
- Realizacji projektu w oparciu o rozwiązania chmurowe;
- Wstrzymaniu realizacji inicjatywy.

4. Planowanie projektu (w przypadku decyzji o realizacji projektu w oparciu o rozwiązania chmurowe)

Na tym etapie projektu realizowane są następujące czynności:

- Zdefiniowanie głównego celu projektu oraz określenie celów pośrednich (cele projektu często określa się według kryteriów dobrze określonego celu SMART, które powodują, że możliwa jest ocena wykonalności projektu);
- Określenie oczekiwanych efektów projektu, produktów końcowych;
- Estymacja czasu realizacji zadań i określenie wymaganych zasobów;
- Opracowanie harmonogramu projektu;
- Opracowanie formalnego planu jakości;
- Opracowanie formalnego planu komunikacji;
- Opracowanie planu zarządzania ryzykiem.

5. Definicja wymagań

Podczas etapu definicji wymagań zespół projektowy, wspierany odpowiednio dla zakresu danego zadania przez jednostki Banku odpowiedzialne za bezpieczeństwo, infrastrukturę techniczną, architekturę, zarządzanie ryzykiem, zgodność:

- Opracowuje koncepcję rozwiązania i określa jej wpływ na obecną architekturę Banku;
- Przygotowuje dokument specyfikacji wymagań funkcjonalnych i pozafunkcjonalnych;
- Spisuje wymagania w zakresie infrastruktury technicznej;
- Dokumentuje wymagania w zakresie cyberbezpieczeństwa.

6. Opracowanie i dystrybucja zapytania ofertowego

Po udokumentowaniu wymagań biznesowych, technicznych, w obszarze cyberbezpieczeństwa, zgodności z prawem i przepisami zespół projektowy przygotowuje zapytanie ofertowe, które zostanie wysłane do wybranych Dostawców usług chmury obliczeniowej. Przy tworzeniu wymagań zawartych w zapytaniu ofertowym należy uwzględnić:

1) Czy istnieją na rynku rozwiązania chmurowe posiadające referencje w branży finansowej?
2) Czy potencjalni oferenci mogą zapewnić Centrum Przetwarzania Danych (CPD) na terenie Europejskiego Obszaru Gospodarczego (EOG)?
3) Czy potencjalni oferenci spełniają wymagania dla Dostawców usług chmurowych wskazane w Komunikacie UKNF?
4) W przypadku gdy Bank jest operatorem usługi kluczowej (zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa) – czy potencjalni oferenci mogą zapewnić CPD na terenie Rzeczpospolitej Polskiej?
5) Czy możliwe jest zapewnienie odpowiednich kompetencji po stronie Banku? Czy są wymagane dodatkowe szkolenia dla pracowników? Jakie są możliwości pozyskania kompetencji na rynku? Z jakimi kosztami należy się liczyć?
6) Czy została potwierdzona zgodność ze standardami wewnętrznymi i przepisami (rozdział VII pkt 4.1 ppkt d Komunikatu UKNF)?
7) Czy rozwiązanie chmurowe będzie w stanie zapewnić wymaganą dla projektu pojemność i wydajność?
8) Jakie będą wymagane zasady przekazywania informacji odnośnie do zdarzeń naruszenia bezpieczeństwa informacji, rozumianego jako poufność, integralność i dostępność przetwarzanych informacji i zasobów, ze szczególnym uwzględnieniem informacji poufnych w rozumieniu umowy zawartej przez Bank z Dostawcą usługi chmurowej?
9) Jakie będą wymagane zasady bezpiecznego i trwałego niszczenia danych w chmurze?
10) W jaki sposób będą monitorowane parametry działania usługi chmurowej?
11) Jakie będą zasady zakończenia współpracy z Dostawcą usługi chmurowej?

Przed uruchomieniem procesowania zapytania ofertowego należy zweryfikować, czy Bank posiada już umowy z Dostawcami usług chmury obliczeniowej, które mogą być wykorzystane dla tej inicjatywy.

Odpowiedzi na zapytanie ofertowe powinny zawierać m.in. informacje o spełnieniu wymagań określonych w Komunikacie UKNF, rozdział VII, pkt 6 Wymagania dla Dostawców usług chmury obliczeniowej. Przykładowa ankieta wymagań dla Dostawców usług chmury obliczeniowej wraz z wymaganiami w zakresie konfiguracji usługi znajduje się w Załącznikach nr 7 oraz 8 do opracowania Standard PolishCloud 2.0.

7. Ocena inicjatywy pod kątem wytycznych EBA (European Banking Authority) w sprawie outsourcingu

Na tym etapie prac sugerowana jest ocena nowej inicjatywy pod kątem wytycznych EBA w sprawie outsourcingu.

8. Ocena inicjatywy pod kątem przepisów o powierzaniu czynności podmiotom zewnętrznym

Na tym etapie prac sugerowana jest ocena nowej inicjatywy pod kątem zgodności z przepisami Prawa bankowego o powierzaniu czynności podmiotom zewnętrznym.

9. Ocena inicjatywy pod kątem przepisów o outsourcingu szczególnym chmury obliczeniowej

Na tym etapie prac sugerowane jest potwierdzenie, czy w ramach usługi będą przetwarzane informacje prawnie chronione i czy usługa będzie definiowana jako outsourcing szczególny chmury obliczeniowej.

10. Ocena ofert, w tym ocena ryzyka związanego z usługą chmurową

Na podstawie odpowiedzi Dostawców na zapytanie ofertowe, w szczególności udzielonych odpowiedzi na wymagania wynikające z Komunikatu UKNF, zdefiniowane w ankiecie dla Dostawców usług chmurowych oraz zgodnie z obowiązującymi przepisami wewnętrznymi, Bank dokonuje oceny otrzymanych ofert.

W ramach procesu oceny ofert powinno być przeprowadzone szacowanie ryzyka dla każdego z oferowanych rozwiązań.

Szacowanie ryzyka może być przeprowadzone przy wykorzystaniu szablonu formularza szacowania ryzyka, który stanowi Załącznik nr 4 do opracowania Standard PolishCloud 2.0.

Wstępny wynik analizy ryzyka, łącznie z wymaganiami funkcjonalnymi, aspektami finansowymi etc., jest podstawą do podjęcia decyzji o wyborze Dostawcy usług chmurowych dla danego przedsięwzięcia.

11. Akceptacja oferty i negocjacje umowy z Dostawcą usługi chmury obliczeniowej

Na tym etapie prac, biorąc pod uwagę kwestie biznesowe, aspekt finansowy, jak również wynik szacowania ryzyka dla proponowanego rozwiązania, dokonywany jest wybór oferty najlepiej spełniającej wymagania Banku.

Bank, zgodnie z obowiązującymi przepisami wewnętrznymi, prowadzi negocjacje z wybranym Dostawcą usług chmurowych. Podczas negocjacji wskazane jest uzgodnienie z Dostawcą metod postępowania z ewentualnymi ryzykami zidentyfikowanymi przy ocenie oferty. Na podstawie uzgodnień Bank opracowuje ostateczny plan postępowania ze zidentyfikowanymi ryzykami.

12. Podpisanie umowy z Dostawcą usług chmurowych

Na tym etapie prac, zgodnie z obowiązującymi w Banku przepisami, następuje podpisanie umowy między Bankiem i Dostawcą usługi chmurowej. Umowa powinna być zgodna z wymaganiami Komunikatu UKNF.

Ewentualne zidentyfikowane ryzyka, ocena łańcucha outsourcingowego (jeśli dotyczy) powinny być zaadresowane poprzez wprowadzenie odpowiednich zapisów umownych zabezpieczających Bank w tym zakresie.

Na podstawie uzgodnionego harmonogramu prac można wskazać najlepszy moment do poinformowania UKNF o przetwarzaniu informacji w chmurze obliczeniowej, zabezpieczając spełnienie wszystkich wymagań Komunikatu, w tym wymogu poinformowania UKNF 14 dni przed produkcyjnym uruchomieniem usługi.

13. Realizacja projektu – analiza szczegółowa

Podczas realizacji tego etapu projektu przeprowadzana jest analiza szczegółowa rozwiązania m.in. pod kątem wpływu na architekturę, w zakresie wymagań funkcjonalnych i pozafunkcjonalnych, infrastruktury technicznej, cyberbezpieczeństwa.

14. Realizacja projektu – projektowanie i budowa

Ten etap prac projektowych obejmuje:

- opracowanie projektu technicznego,
- przygotowanie infrastruktury technicznej,
- development,
- przeprowadzenie testów (jednostkowych, systemowych, integracyjnych) na podstawie scenariuszy testowych, udokumentowanie wyników testów,
- przeprowadzenie testów bezpieczeństwa na podstawie udokumentowanych założeń, udokumentowanie wyników testów bezpieczeństwa,
- przeprowadzenie testów wydajnościowych na podstawie udokumentowanych założeń, udokumentowanie wyników testów wydajnościowych.

15. Realizacja projektu – testy odbiorcze

W ramach tego etapu prac przeprowadzane są testy akceptacyjne rozwiązania na podstawie przygotowanych scenariuszy testowych. Zgodnie z wymaganiami Komunikatu zarówno warunki scenariuszy testowych, jak i wyniki testów odbiorczych powinny zostać udokumentowane.

16. Realizacja projektu – uzupełnienie dokumentacji wymaganej dla usługi chmurowej

Ten etap prac obejmuje m.in.:

- przeprowadzenie ostatecznego szacowania ryzyka dla wdrażanej usługi chmurowej, bazując na informacjach pozyskanych podczas prowadzonych prac projektowych, wyników testów, audytów itp., oraz formalne zatwierdzenie jego wyników,

- przeprowadzenie i udokumentowanie testów wyjścia z usługi (scenariusze testowe, założenia, wyniki testów),
- wprowadzenie odpowiednich aktualizacji w planie ciągłości działania Banku,
- udokumentowanie stosowanych dla usługi mechanizmów szyfrujących,
- opisanie procedury zarządzania kluczami szyfrującymi,
- potwierdzenie, że informacje przetwarzane w ramach usługi chmurowej są szyfrowane zgodnie z wymaganiami Komunikatu UKNF,
- udokumentowanie zasad zbierania logów,
- przygotowanie dokumentu potwierdzającego zgodność usługi z wymaganiami UKNF,
- podjęcie przez Bank formalnej decyzji o wykorzystaniu usługi chmurowej.

Kompletność przygotowanej dokumentacji projektowej dla danej inicjatywy chmurowej powinna być zweryfikowana z listą produktów do opracowania po stronie Banku, znajdującą się w Załączniku nr 1 do niniejszego Standardu.

Dla przypomnienia, sposób zatwierdzania wyników szacowania ryzyka dla usługi chmurowej powinien być wskazany w „Polityce zarządzania ryzykiem bezpieczeństwa teleinformatycznego" obowiązującej w Banku.

Dokument „Wyniki szacowania ryzyka" powinien zawierać oświadczenie mówiące, że świadczenie usługi chmury obliczeniowej będzie realizowane zgodnie z wymaganiami prawa obowiązującymi Bank, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez Bank standardami.

Formalne zatwierdzenie „wyników szacowania ryzyka" następuje w sposób właściwy dla akceptacji procesów ze względu na ich istotność lub znaczenie opisanych w odpowiednich dokumentach wewnętrznych danej organizacji. Dla procesów krytycznych lub istotnych przetwarzanych w usłudze chmury obliczeniowej może okazać się konieczna uchwała zarządu Banku.

17. Wdrożenie przedprodukcyjne – konfiguracja usługi

Uwaga: na tym etapie nie jest jeszcze dokonywana migracja danych produkcyjnych.

Po zakończeniu wdrożenia przedprodukcyjnego dokonywana jest aktualizacja statusu planów naprawczych i oceny ryzyka w celu potwierdzenia, że zidentyfikowane uprzednio ryzyka zostały zaadresowane zgodnie z założeniami.

Określany jest też termin migracji danych i uruchomienia produkcyjnego.

18. Zgłoszenie do UKNF

Najpóźniej na tym etapie prac powinno nastąpić zgłoszenie inicjatywy do UKNF, zgodnie z wymaganiami Komunikatu chmurowego.

19. Migracja danych produkcyjnych do usługi chmurowej

Po co najmniej 14 dniach od momentu zgłoszenia do UKNF możliwe jest rozpoczęcie przetwarzania danych w usłudze chmurowej, a zatem rozpoczęcie migracji danych produkcyjnych.

20.Uruchomienie produkcyjne

Po zakończeniu i przetestowaniu migracji danych możliwe jest formalne uruchomienie produkcyjne, poprzedzone formalną decyzją w tym zakresie i komunikacją do użytkowników i innych interesariuszy, zgodnie z obowiązującymi w Banku przepisami.

21. Zamknięcie projektu

Ten etap prac obejmuje ocenę efektów projektu i zwykle kończy się zamknięciem administracyjnym i prawnym projektu.

Definicje wybranych pojęć związanych z kwestiami projektowymi.

Analitycy biznesowi Członkowie zespołu realizującego projekt po stronie zamawiającego, odpowiedzialni za przygotowanie wymagań biznesowych oraz nadzorowanie zgodności koncepcji rozwiązania z wymaganiami biznesowymi.

Analitycy IT Członkowie zespołu realizującego projekt po stronie realizującego, odpowiedzialni za opracowanie wymagań funkcjonalnych oraz wspieranie analityków biznesowych w opracowywaniu wymagań biznesowych.

Architekci IT Członkowie zespołu realizującego projekt po stronie realizującego, odpowiedzialni za opracowanie koncepcji architektury rozwiązania oraz za zapewnienie spójności rozwiązania.

Dokumentacja eksploatacyjna Dokumentacja zawierająca procedury i instrukcje z zakresu instalacji i konfiguracji, instrukcje operatorskie, instrukcje eksploatacyjno-utrzymaniowe.

Dokumentacja techniczna Dokumentacja techniczna (batche, słowniki, dane, procedury, interfejsy, raporty, logi, transakcje, programy, serwisy, komunikaty, błędy); opis architektury systemu (architektura fizyczna systemu, architektura logiczna aplikacji, wykaz niezbędnych systemów współdziałających, wykaz niezbędnych narzędzi systemowych, opis wymagań sprzętowych).

Etap projektowania i budowy Celem etapu jest zaprojektowanie i zbudowanie aplikacji lub zmian w aplikacjach oraz przygotowanie do przeprowadzenia testów akceptacyjnych.

Etap testowania akceptacyjnego Celem etapu jest uzyskanie potwierdzenia, iż aplikacja lub zmiany w aplikacji są zgodne z zaakceptowanymi szczegółowymi wymaganiami funkcjonalnymi i pozafunkcjonalnymi.

Etap wdrożenia i stabilizacji Produkcyjne uruchomienie aplikacji lub zmian w aplikacjach oraz kontrola poprawności ich działania.

Plan testów Dokument zawierający informacje nt. planów w zakresie rodzajów testów, zespołu wykonawców, harmonogramu, narzędzi, środowisk testowych.

Plan wdrożenia Dokument mający na celu sformułowanie planu wdrożenia aplikacji, a w szczególności opisujący weryfikacje wymagań wdrożeniowych i eksploatacyjnych, harmonogram wdrożenia, role i odpowiedzialności, plan migracji danych, procedurę wdrożenia, kryteria oceny powodzenia wdrożenia, plan awaryjny, plan etapu stabilizacji, kryteria zakończenia okresu stabilizacji, ryzyka.

Produkt projektu Rezultat projektu zdefiniowany pod względem cech funkcjonalnych i jakościowych.

Projekt Jednorazowe przedsięwzięcie o sprecyzowanym celu, zakresie, budżecie i czasie trwania, zmierzające do osiągnięcia określonych efektów finansowych lub niefinansowych.

Rejestr ryzyk w projekcie Udokumentowanie zidentyfikowanych ryzyk dotyczących danego projektu wraz z ich statusem i historią.

Ryzyko projektu Możliwość poniesienia negatywnych konsekwencji przyszłych i niepewnych, choć przewidywalnych zdarzeń, których skutki mogą dotyczyć samego projektu, a w szczególności harmonogramu projektu (przekroczenie terminu), budżetu projektu (przekroczenie puli przeznaczonych na ten cel środków finansowych) lub wartości produktów projektu (np. obniżenie jakości produktów projektu czy korzyści projektu).

Scenariusze testowe Dokument do testowania zakresu biznesowego systemu; scenariusz zawiera opis zdarzeń, sprawdza procesy biznesowe lub ciąg wykonywanych po sobie funkcji biznesowych zaimplementowanych w systemie; biznesowy scenariusz testowy może przebiegać przez wiele aplikacji lub modułów aplikacji.

Zakres projektu Wszystko, co w ramach projektu zostanie wykonane lub wytworzone.

Załącznik nr 10

do Standardu PolishCloud 2.0

Nadzór (governance)

Governance, czyli nadzór, pomaga uzyskać pewność, że wdrożone w chmurze obliczeniowej rozwiązania skutecznie adresują potrzeby biznesowe interesariuszy, zapewniając jednocześnie zgodność regulacyjną. Efektywny nadzór pomaga uzyskać równowagę między realizacją celów i minimalizacją ryzyka operacyjnego. W ocenie skuteczności prowadzonego przez Bank nadzoru pomocna może się okazać analiza odpowiedzi na poniższe pytania, dotyczące uwzględnienia w nadzorze aspektów przetwarzania chmurowego:

1. Czy polityka bezpieczeństwa Banku obejmuje aspekty bezpieczeństwa przetwarzania chmurowego? Czy zaktualizowana polityka jest znana i stosowana w Banku?
2. Czy procedury bezpieczeństwa Banku zostały rozszerzone o aspekty związane z bezpieczeństwem przetwarzania chmurowego (w szczególności związane z zarządzaniem użytkownikami, kontrolą dostępu, szyfrowaniem, zarządzaniem kluczami szyfrującymi, monitorowaniem bezpieczeństwa, zarządzaniem incydentami, zarządzaniem danymi, zarządzaniem konfiguracją, zarządzaniem rozwojem oprogramowania)? Czy zaktualizowane procedury są znane i stosowane w Banku?
3. Czy zdefiniowane i wdrożone zostały mierniki/kontrole/audyty z zakresu bezpieczeństwa przetwarzania chmurowego?
4. Czy źródła identyfikacji ryzyk bezpieczeństwa zostały rozszerzone o aspekty przetwarzania chmurowego? Czy proces zarządzania ryzykiem uwzględnia nowe formy przetwarzania danych w chmurze, w tym aspekty związane m.in. z lokalizacją i retencją danych?
5. Czy Bank posiada odpowiednie kompetencje w zakresie zarządzania, tworzenia, korzystania oraz utrzymania rozwiązań chmurowych?
6. Czy programy rozwoju kompetencji pracowników zostały rozszerzone o aspekty przetwarzania i bezpieczeństwa chmurowego (ścieżki szkoleniowe i certyfikacji)?
7. Czy programy budowania świadomości kierowane do pracowników i ewentualnie klientów zostały rozszerzone o aspekty przetwarzania i bezpieczeństwa chmurowego?
8. Czy w ramach umowy z Dostawcą zdefiniowano klarowny podział odpowiedzialności za bezpieczeństwo usług chmurowych (*shared responsibility model*)?
9. Czy zdefiniowano i wdrożono proces inicjalnej i cyklicznej oceny Dostawców chmurowych w zakresie ustalonych wymagań i standardów bezpieczeństwa Banku?
10. Czy są określone procedury tworzenia kopii zapasowych i przywracania z tych kopii danych (backup) w zakresie rozwiązań chmurowych?

11. Czy są określone wymagania dla dostępności danych na potrzeby przeprowadzenia audytu (*audit trail*)?

12. Czy plany ciągłości działania (ang. *Business Continuity Planning*) uwzględniają możliwość utraty dostępu do wybranych usług w chmurze, środowisk chmurowych lub przetwarzanych w chmurze danych?

Źródła:

1. Polityki i zarządzanie bezpieczeństwem w chmurze IBM: https:/www.ibm.com/cloud/architecture/architectures/securityArchitecture/security-policy-governance-risk-compliance
2. IBM Cloud compliance programs: https:/www.ibm.com/cloud/compliance
3. GCP security foundation guide: https:/services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf
4. GCP Cloud compliance documents:
   a. https:/cloud.google.com/security/compliance
   b. https:/cloud.google.com/security/compliance/compliance-reports-manager
5. Microsoft Well-Architected Framework: https:/docs.microsoft.com/en-us/azure/architecture/framework/
6. Microsoft Cloud Adoption Framework: https:/docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/security-baseline/azure-security-guidance
7. Przewodnik budowy zaufanych usług chmurowych na platformie Microsoft Azure: https:/azure.microsoft.com/en-us/overview/trusted-cloud/
8. Microsoft Trust Center: https:/www.microsoft.com/en-us/trust-center

Załącznik nr 11

do Standardu PolishCloud 2.0

Wybrane definicje i pojęcia związane z bezpieczeństwem informacji

Anonimizacja – proces nieodwracalnego pozbawienia zbioru danych cech informacji chronionej przez jej usunięcie lub pozbawienie możliwości powiązania z danymi chronionymi. Przykładowa technika anonimizacji danych to zastąpienie ciągu znaków chronionych stałym lub losowym symbolem. Proces anonimizacji powinien odbywać się na poziomie logicznego wpisu, przykładowo w przypadku wielu pól identyfikujących osobę należy anonimizować zarówno pojedyncze pola, jak i zależności pomiędzy polami. Zanonimizowany zbiór danych zazwyczaj przestaje podlegać ochronie.

Pseudonimizacja – proces zamiany wartości rzeczywistej na fikcyjną (pseudonimizowaną) w zbiorze danych. Jeżeli ciągle istnieje powiązanie między wartością rzeczywistą a fikcyjną, to mówimy o pseudonimizacji odwracalnej. W przypadku usunięcia relacji między wartością fikcyjną a rzeczywistą mówimy o pseudonimizacji nieodwracalnej, co jest szczególnym przypadkiem anonimizacji. Najczęstszymi technikami pseudonimizacji są: szyfrowanie z użyciem klucza tajnego, tokenizacja, używanie funkcji skrótu („hash"). Pseudonimizacja umożliwia redukcję wrażliwości przetwarzanych danych. Dane pseudonimizowane mogą być traktowane jako dane anonimizowane, jeżeli nastąpiła pseudonimizacja nieodwracalna (anonimizacja) lub jeśli metoda pseudonimizacji pozwala na wyodrębnienie systemu pseudonimizacji (przykładowo system szyfrujący dane i klucz jest traktowany jako podlegający ochronie, natomiast sam pseudonimizowany zbiór danych nie podlega ochronie).

Szyfrowanie a anonimizacja – anonimizacja jest procesem trwałego i nieodwracalnego pozbawienia zbioru danych cech informacji chronionej. Szyfrowanie jest procesem zabezpieczenia dostępu do danych chronionych poprzez odwracalny proces pozbawienia cech informacji chronionej, wymagający zachowania środków ochrony względem klucza tajnego zastosowanego w procesie szyfrowania.

Kryptografia – dziedzina wiedzy zajmująca się przekazywaniem informacji w sposób zabezpieczony przed niepowołanym dostępem.

Klucze (MEK, KEK, TEK etc.) – klucze to podstawowe parametry używane w procesie szyfrowania oraz deszyfrowania danych. Podstawowy podział kluczy to klucze symetryczne oraz asymetryczne. W przypadku kluczy symetrycznych ten sam klucz jest użyty do zaszyfrowania i odszyfrowania wiadomości. Kryptografię asymetryczną nazywa się także kryptografią z użyciem klucza publicznego. W kryptografii asymetrycznej używa się klucza publicznego i prywatnego powiązanych ze sobą za pomocą relacji matematycznej. W typowym użyciu do szyfrowania używa się klucza publicznego, a do odszyfrowania wiadomości klucza prywatnego. Ochronie podlega klucz prywatny. Można wyróżnić następujące typy kluczy: *Master Encryption Key* (MEK) – klucz użyty do generowania następnych kluczy; *Key Encryption Key* (KEK) – klucz służący do szyfrowania innych kluczy; *Data Encryption Key* (DEK) – klucz służący do szyfrowania danych; *Traffic Encryption Key* (TEK) – klucz używany do szyfrowania ruchu sieciowego.

Systemy do zarządzania kluczami – systemy zapewniające zarządzanie cyklem życia kluczy. Można wydzielić wyspecjalizowane moduły HSM (*Hardware Security Module*) oraz KMS (*Key Management System*). HSM to systemy typowo sprzętowe, które spełniają kryteria opisane standardem FIPS 140-2 Level 3. KMS to usługi wprowadzone przez Dostawców chmurowych, które dodają zazwyczaj możliwość zarządzania kluczami jako usługę.

Bring Your Own Key – termin ten odnosi się do funkcjonalności KMS udostępnionego przez Dostawcę chmurowego umożliwiającej wykorzystanie własnego, lokalnego klucza. Lokalne klucze powinny być zarządzane w systemie HSM lub innym KMS spełniającym wymagania regulatora.

Rotacja kluczy – proces cyklicznej wymiany kluczy wykorzystywanych do dostępu do usług lub danych. Proces ten ma na celu minimalizację ryzyka związanego ze złamaniem klucza lub jego wyciekiem. Im szerszy dostęp do klucza, tym istotniejsza jest jego cykliczna wymiana.

Szyfrowanie – jedna z technik pseudonimizacji. Proces zamiany informacji jawnej w szyfrogram z użyciem klucza oraz algorytmu szyfrującego. Do realizacji procesu odwrotnego niezbędna jest znajomość algorytmu oraz klucza (parametrów szyfrowania).

Tokenizacja – jedna z technik pseudonimizacji wykorzystująca jednokierunkowy mechanizm szyfrujący oparty na przypisaniu identyfikatora (indeksu, sekwencji lub losowo wygenerowanej liczby) niepowiązanego z informacją chronioną. Do odszyfrowania zabezpieczonej informacji niezbędna jest wiedza na temat powiązania identyfikatora z informacją chronioną. Powiązanie to podlega ochronie przed niepowołanym dostępem.

WORM – (ang. *Write Once Read Many*) – technologia przechowywania danych, w której informacja raz zapisana może być wielokrotnie odczytywana, jednak nie może być już w żaden sposób modyfikowana. Ochrona przed modyfikacją danych w urządzeniach tej klasy daje pewność, że dane nie mogą zostać zmodyfikowane po inicjalnym zapisaniu ich na zasobach WORM. Takie podejście zapewnia wysoki poziom integralności i bezpieczeństwa danych, eliminując jednocześnie ryzyko ich usunięcia lub modyfikacji.

Załącznik nr 12

do Standardu PolishCloud 2.0

Objaśnienia i lista wybranych klauzul wraz z przykładami

Zgodnie z pkt VII. 4.1. Komunikatu umowa z Dostawcą powinna zawierać co najmniej postanowienia regulujące:

a. klarowny podział odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji, z uwzględnieniem modelu świadczenia usług, ciągłości działania usług (z uwzględnieniem parametrów RTO i RPO tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;

Objaśnienie:

1. Należy zwrócić uwagę na to, by definicje „RTO", „RPO" oraz „SLA" zawarte w umowie były zgodne z definicjami zawartymi w Komunikacie. Parametry RTO, RPO powinny być w szczególności wzięte pod uwagę, gdy odtworzenie danych lub np. restart usługi w innym CPD jest w zakresie obowiązków Dostawcy (i powinien być objęty takimi parametrami). Taka sytuacja może w szczególności występować, gdy usługa chmury obliczeniowej jest świadczona w modelu pośrednim, tj. gdy bezpośredni Dostawca Banku wykorzystuje chmurę do świadczenia usług na rzecz Banku. Parametry takie powinny występować również zgodnie z wymaganiami Banku (np. w zależności od oczekiwanej biznesowo dostępności usługi).
2. Model odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji wynika z praktyki rynkowej – ważne, by umowa jednoznacznie określała podział odpowiedzialności.

b. klarowną definicję i wskazanie lokalizacji przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;

Objaśnienie:

1. VIII.1.4. Komunikatu: podmiot nadzorowany informuje o lokalizacji (kraj, region albo inne równoważne) centrum przetwarzania danych (CPD) świadczącym usługę chmury obliczeniowej;

   Przypis nr 5 Komunikatu: 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 Do-

stawca 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.

2. Zatem Komunikat nie nakłada wymogu podawania adresu CPD (precyzyjne wskazanie lokalizacji) w notyfikacji zgodnie z Załącznikiem nr 1 Komunikatu. Wskazanie takiej informacji może rodzić zagrożenie dla bezpieczeństwa fizycznego przetwarzanych informacji, dlatego jako minimum wystarczy wskazanie w notyfikacji zgodnie z Załącznikiem nr 1 Komunikatu np.: „strefy dostępu" lub „regionu", przy czym wskazanie takie powinno obejmować co najmniej kraj i przybliżoną lokalizację CPD (np. miasto lub region geograficzny). Bank powinien mieć jak najdalej idącą wiedzę, gdzie jego dane mogą być przetwarzane, jednak UKNF nie wymaga tak dokładnego notyfikowania w tym zakresie.

3. Umowa powinna umożliwiać Bankowi precyzyjne określenie lokalizacji przetwarzania danych oraz lokalizacji CPD (np. przekazanie takiej informacji na żądanie Banku) z uwzględnieniem polityk wewnętrznych Banku dotyczących lokalizacji danych. Przy czym nie jest to równoznaczne z informacją notyfikowaną UKNF, która może być na poziomie „strefa dostępu", „region" lub innymi równoważnymi.

4. Zwracamy uwagę, że zgodnie z Komunikatem Banki, które zostały uznane stosowną decyzją za operatorów usług kluczowych lub są operatorami infrastruktury krytycznej, powinny w pierwszej kolejności wykorzystywać CPD położone w Polsce o ile – w ocenie Banku – oferowane warunki umowne, ekonomiczne, operacyjne, SLA czy funkcjonalne są nie gorsze od CPD znajdujących się poza terytorium Rzeczypospolitej Polskiej. Bank, dokonując analizy, powinien brać pod uwagę nie tylko bieżące zapotrzebowanie i zakres wykorzystywanych usług, ale także potencjalny rozwój i możliwość świadczenia usług przez Dostawcę chmurowego, np. niektóre usługi chmury obliczeniowej mogą być dostępne w (realizowane z) niektórych CPD Dostawcy chmurowego.

5. W obowiązującym prawie brak definicji „przetwarzania informacji". W związku z tym przy stworzeniu przykładowej definicji przetwarzania informacji wykorzystana została definicja przetwarzania danych zawarta w art. 4 pkt 2) RODO.

6. Z zastrzeżeniem pkt. 4) powyżej, CPD powinno, ale nie musi, znajdować się w kraju należącym do EOG, jednak korzystanie z CPD znajdującego się poza EOG wiąże się z koniecznością uzyskania zezwolenia KNF zgodnie z przepisem art. 6d Prawa bankowego.

Przykładowe klauzule:

1. [*Definicje*] „**Przetwarzanie informacji**": operacja lub zestaw operacji na informacjach, lub zestawach informacji dokonywanych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, przesyłanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

c. prawo właściwe umowy (w tym sąd właściwy i zasady rozstrzygania sporów);

Przykładowe klauzule:

PRAWO WŁAŚCIWE, JURYSDYKCJA

1. Niniejsza Umowa oraz wszelkie zobowiązania pozaumowne z niej wynikające lub powstające w związku z nią podlegają prawu polskiemu.
2. Każda ze Stron nieodwołalnie wyraża zgodę, chyba że ustawa stanowi o wyłącznej jurysdykcji, aby wszelkie spory, które mogą powstać w związku z niniejszą Umową lub które są związane z jej naruszeniem, wypowiedzeniem lub nieważnością, były rozstrzygane przez sąd powszechny, właściwy dla [*np. Miasta Stołecznego Warszawy (Warszawa Śródmieście).*]

lub w przypadku poddania umowy prawu innemu niż polskie:

1. Niniejsza Umowa oraz wszelkie zobowiązanie pozaumowne z niej wynikające lub powstające z nią podlegają prawu [_____] [*prawo państwa innego niż polskie*].
2. Z uwagi na okoliczność, iż Zamawiający [*Bank*] jest podmiotem nadzorowanym w rozumieniu polskiej Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. 2019.298) i korzystanie przez Zamawiającego z usług, które są świadczone przez Dostawcę na podstawie niniejszej Umowy, jest ściśle regulowane, Dostawca niniejszym oświadcza, iż prawo państwa, któremu poddana została Umowa, pozwala na skuteczne wykonywanie postanowień niniejszej Umowy, wymogów prawa polskiego ciążących na Zamawiającym oraz wytycznych polskiego organu nadzoru, w tym Komunikatu. Szczegółowy opis wymogów prawa polskiego oraz wytycznych wraz z analizą prawną dotyczącą możliwości ich skutecznego wykonywania pod prawem [_____] stanowi Załącznik nr [__] do Umowy.
3. Każda ze Stron nieodwołalnie wyraża zgodę, chyba że ustawa stanowi o wyłącznej jurysdykcji, aby wszelkie spory, które mogą powstać w związku z niniejszą Umową lub które są związane z jej naruszeniem, wypowiedzeniem lub nieważnością, były rozstrzygane przez sąd powszechny, właściwy dla [_____].

d. potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;

Objaśnienie:

1. W obecnym stanie prawnym chodzi o zgodność z RODO. Dla jasności przez zwrot „o ile ma zastosowanie" rozumiemy sytuację, gdy na podstawie umowy outsourcingu w chmurze obliczeniowej przetwarzane są dane osobowe.

e. własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu (wygaśnięciu, rozwiązaniu), także w sposób nieplanowany

Objaśnienie:

1. Rekomenduje się, aby Bank określił w umowie z Dostawcą chmurowym lub Dostawcą IT, który wykorzystuje chmurę obliczeniową, sposób zwrotu danych Banku, a także w miarę możliwości zwrot danych/informacji wytworzonych w oparciu o dane dostarczone przez Bank, np. profile behawioralne klienta.

f. gwarancje, rękojmie, ubezpieczenia (polisy ubezpieczeniowe Dostawcy usług chmury obliczeniowej), kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej oraz zasad postępowania w takich sytuacjach, o ile ma to zastosowanie;

g. określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie), zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;

Objaśnienie:

1. W przypadku outsourcingu bankowego zastosowanie ma zakaz ograniczania odpowiedzialności w relacji Bank – klient, Dostawca – Bank. Dla jasności przez zwrot „o ile ma zastosowanie" rozumie się sytuację, gdy na podstawie umowy na usługi chmurowe przetwarzane są informacje, których utrata lub ujawnienie może spowodować szkodę po stronie klientów Banków.

Przykładowe klauzule:

Ograniczenia odpowiedzialności Dostawcy zawarte w Umowie nie dotyczą odpowiedzialności Dostawcy wobec Banku zgodnie z brzmieniem przepisu art. 6b ustawy Prawo bankowe.

h. klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) Dostawcy usług chmury obliczeniowej oraz warunki nadawania praw dostępu do informacji przetwarzanych przez podmiot nadzorowany

Objaśnienie:

1. Rekomendowanym mechanizmem zmiany listy poddostawców jest wymóg każdorazowej zgody Banku dla takiej zmiany. Dopuszczalna jest również sytuacja, w której Dostawca za uprzednim poinformowaniem Banku jednostronnie podejmuje decyzje o zmianie poddostawców i aktualizuje listę poddostawców. W takim przypadku Umowa musi opisywać pre-

cyzyjnie zasady uprzedniego powiadamiania o zmianie listy poddostawców, a także dawać podstawę do wypowiedzenia umowy przez Bank, w razie zmiany poddostawców z naruszeniem Umowy lub w razie sprzeciwu Banku dla zaangażowania określonego poddostawcy.

2. Sugerowane jest, aby lista poddostawców została załączona do Umowy w formie załącznika. Listy dostępne on-line mogą zostać zaakceptowane przy uregulowaniu w Umowie zasad powiadamiania o ich aktualizacji i uwzględnieniu monitorowania tej listy w organizacji Banku.
3. Celem tego wymogu jest jednoznaczne wskazanie w umowie:
    - kanałów komunikacji służących do informowania o planowanych zmianach w standardach świadczonych usług, np. poprzez wskazanie dedykowanego adresu strony www lub
    - zapewnienie efektywnej wymiany informacji o zmianach w standardach świadczonych usług chmury obliczeniowej (w tym zmianach o charakterze technicznym), np. adresu e-mail upoważnionego pracownika Dostawcy i pracownika Banku do komunikacji.

i. klarowne wskazanie zasad, zgodnie z którymi 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;

Przykładowe klauzule:

4. [*W formie oświadczenia w sekcji „Oświadczenia i zapewnienia”*] Dostawca oświadcza i zapewnia, że zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań wszystkich poddostawców są transparentne i zostały opisane w [*odesłanie do właściwych postanowień umowy lub dokumentacji*].

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

Objaśnienie:

1. Celem tego wymogu jest wskazanie w umowie:
    - kanałów komunikacji służących do informowania o planowanych zmianach w standardach świadczonych usług, np. poprzez wskazanie dedykowanego adresu strony www lub
    - zapewnienie efektywnej wymiany informacji o zmianach w standardach świadczonych usług chmury obliczeniowej (w tym zmianach o charakterze technicznym), np. adresu e-mail upoważnionego pracownika Dostawcy i pracownika Banku.

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

Objaśnienie:

1. Celem niniejszego postanowienia jest jednoznaczne wskazanie w umowie kanałów komunikacji służących do przesyłania dokumentacji technicznej, deklaracji zgodności i instrukcji konfiguracji usług, np. poprzez wskazanie dedykowanego adresu strony www lub adresu e-mail upoważnionego pracownika Dostawcy i pracownika Banku do komunikacji.

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

Objaśnienie:

1. Brzmienie postanowienia będzie każdorazowo uzależnione od rodzaju świadczonych usług i ustaleń stron (np. zapewnienie w umowie przekazywania określonych informacji poprzez dedykowanego e-maila, adres strony).

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);

Objaśnienie:

1. Zgodnie z RODO administrator w umowie powierzenia zawartej z podmiotem przetwarzającym musi zawrzeć postanowienie dotyczące umożliwienia przeprowadzenia administratorowi lub audytorowi upoważnionemu przez administratora audytów, w tym inspekcji. Konieczne jest zatem zawarcie w umowie na usługę chmurową możliwości i zasad przeprowadzenia inspekcji oraz taka możliwość nie powinna zostać wyłączona, niezależnie od wyników szacowania ryzyka. Jednakże, w zależności od jego wyników, można natomiast uzależnić prawo do przeprowadzenia audytu/inspekcji przez Bank (wysokie ryzyko) lub podmiot trzeci (średnie i niskie ryzyko). Prawo do inspekcji może jednak zostać umownie ograniczone, np. poprzez wskazanie, że będzie środkiem stosowanym dopiero wówczas, gdy inne środki kontroli zawiodą, są niemożliwe do przeprowadzenia lub byłyby niewystarczające w określonym stanie faktycznym.
2. Dopuszcza się, z uwzględnieniem zastrzeżeń wskazanych w Komunikacie, możliwość wykorzystania przez Bank (a także przez Dostawcę innego niż Dostawca usług chmurowych) audytu drugiej lub trzeciej strony, tylko i wyłącznie pod warunkiem, że druga lub trzecia strona

zagwarantuje w umowie, że audyt zostanie przeprowadzony na podstawie fizycznych inspekcji w lokalizacjach przetwarzania informacji, a także gdy Dostawca chmurowy zapewni w umowie pełną współpracę przy wykonaniu audytu. Rekomendowane jest, aby w przypadku korzystania z audytu drugiej i trzeciej strony Bank zagwarantował sobie prawo do audytu realizowanego wyłącznie na jego rzecz, a nie wyłącznie w ramach audytu połączonego.

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;

Objaśnienie:

1. Bank zapewnia w umowie z Dostawcą chmurowym prawo nadzoru bankowego (UKNF) do wykonania obowiązków kontrolnych.

o. 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;

Objaśnienie:

1. Bank powinien się upewnić, czy posiadane licencje wykorzystywanego oprogramowania uprawniają do korzystania z niej w lokalizacji danego CPD (lub w chmurze obliczeniowej w ogóle).
2. Bank powinien zweryfikować, jaki jest zakres praw udzielanych Dostawcy w związku z przetwarzaniem informacji w usłudze chmury obliczeniowej.

p. zasady zmiany treści umowy, w tym parametrów technicznych używanych usług chmury obliczeniowej;

Objaśnienie:

1. W zakresie zmian dotyczących parametrów technicznych związanych z wykonaniem umowy w umowie powinny zostać wskazane:
   - kanały komunikacji służące do informowania o planowanych zmianach w standardach świadczonych usług, np. poprzez wskazanie dedykowanego adresu strony www lub
   - zapewnienie efektywnej wymiany informacji o zmianach w standardach świadczonych

usług chmury obliczeniowej (w tym zmianach o charakterze technicznym), np. adresu e-mail upoważnionego pracownika Dostawcy i pracownika Banku.

2. W umowie należy uregulować, jaki zakres dokumentów składających się na Umowę wymaga aneksowania Umowy, a jaki może podlegać ewentualnym jednostronnym zmianom przez Dostawcę (np. dokumentacja udostępniana on-line), a także na jakich zasadach przekazywane są informacje o takich zmianach (zob. objaśnienia dotyczące wymogów wymiany informacji).

q. zasady rozwiązywania umowy, w tym zasady i terminy zwrotu i/lub usunięcia przetwarzanych informacji;

Objaśnienie:

1. Umowa powinna regulować termin realizacji tych obowiązków, a także sposób potwierdzenia trwałego usunięcia z infrastruktury Dostawcy i Dostawcy chmurowego przetwarzanych informacji, zarówno tych dostarczonych przez Bank, jak informacji wytworzonych w oparciu o dane dostarczone przez Bank, np. danych obejmujących profile behawioralne.

r. zasady wsparcia, w tym zakres i okna czasowe (z uwzględnieniem stref czasowych), tryb i sposób zgłaszania problemów z usługami chmury obliczeniowej;

Objaśnienie:

1. Bank powinien zwrócić uwagę na czas realizacji czynności serwisowych względem czasu roboczego wykorzystywania usługi chmurowej (np. czy w związku z inną strefą czasową Dostawcy nie są to godziny robocze funkcjonowania Banku).

s. zasady wymiany informacji, w tym w szczególności w zakresie bezpieczeństwa oraz zarządzania bieżącymi incydentami, obejmujące zarówno pracowników podmiotu nadzorowanego, jak i Dostawcę usług chmury obliczeniowej, a w przypadku istotnego narażenia na skutki danego incydentu – również inne strony (np. klientów, poddostawców itp.), w celu zapewnienia adekwatności postępowania do poziomu istotności incydentu.

n/d.

Załącznik nr 13

do Standardu PolishCloud 2.0

Plan przetwarzania informacji w chmurze obliczeniowej

1. Informacje o realizowanych zadaniach i przetwarzanych informacjach

Nazwa systemu/aplikacji, której informacje są przetwarzane	...
Opis zadania realizowanego za pomocą usługi	...
Rodzaj przetwarzanych informacji	☐ Chronione (tajemnica bankowa) ☐ Inne chronione (z innych przepisów prawa) ☐ Niechronione
Klasa przetwarzanych informacji[1]	☐ Publiczne ☐ Wewnętrzne ☐ Poufne
Typ informacji	☐ Produkcyjne ☐ Testowe
Outsourcing szczególny	☐ Tak ☐ Nie
Opis formatu i struktury informacji	... *(może być referencja do szczegółowej dokumentacji)*

2. Ochrona informacji

Mechanizmy zabezpieczenia informacji	☐ Maskowanie ☐ Pseudonimizacja ☐ Anonimizacja ☐ Inne
Opis mechanizmów zabezpieczenia informacji	... *Należy opisać, jakie pola i w jaki sposób są poddawane poniższym procesom zabezpieczenia*
Opis mechanizmów szyfrowania informacji	... *(może być referencja do szczegółowej dokumentacji)*
Zarządzanie i przechowywanie kluczy szyfrujących	☐ Dostawca ☐ Bank
Opis kontroli dostępu do przetwarzanych informacji	... *informacja o tym, kto ma dostęp do przetwarzanych informacji oraz jak ten dostęp jest nadawany, zarządzany, odbierany i kontrolowany*

3. Umowa z Dostawcą

Dostawca	
Nr umowy	
Prawo właściwe dla umowy	
Data zawarcia umowy, a w przypadku gdy umowa nie jest jeszcze zawarta – przewidywana data jej zawarcia	
Okres obowiązywania umowy	
Data ostatniego przedłużenia lub zmiany w umowie	
Data rozpoczęcia korzystania z usługi	

4. Inne

Data kolejnej weryfikacji planu	
Data ostatniej aktualizacji planu	
Zakres ostatniej aktualizacji	

Załącznik nr 14

do Standardu PolishCloud 2.0

Scenariusz wyjścia z relacji z Dostawcą

1. Opis usługi

Identyfikator umowy	
Usługa (przedmiot umowy)	
Dostawca (nazwa/firma przedsiębiorcy)	
Planowana data zakończenia przetwarzania danych w chmurze:	
Okres wypowiedzenia umowy: przez Bank przez Dostawcę	

2. Sposób postępowania w związku z wygaśnięciem umowy

Założona strategia	**Przedłużenie relacji z dotychczasowym Dostawcą:** ☐ Zawarcie/przedłużenie umowy z dotychczasowym Dostawcą **Realizacja usługi przez inny podmiot:** ☐ Wybór nowego Dostawcy **Realizacja usługi przez pozostałych, dotychczasowych Dostawców:** ☐ Kontynuacja z dotychczasowymi Dostawcami **Powrót działalności do Banku:** ☐ Przejęcie działalności przez jednostkę Banku **Zaprzestanie działalności:** ☐ Brak kontynuowania działalności po wygaśnięciu umowy **Inne:** ☐ ..... ☐ .....
	Wskaż wariant preferowany spośród wymienionych powyżej:

3. Kluczowe działania umożliwiające realizację scenariusza wyjścia

Przedłużenie relacji	
Realizacja usługi przez inny podmiot	
Realizacja usługi przez Bank (powrót do Banku)	
Zaprzestanie działalności będącej przedmiotem umowy	
Inne	przykłady:

4. Zaangażowane jednostki Banku realizujące scenariusz wyjścia

Jednostki realizujące scenariusz	
Jednostki wspierające	
Jednostki informowane o wdrożeniu scenariusza	

5. Historia dokumentu

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

Załącznik nr 15

do Standardu PolishCloud 2.0

Wyjście z chmury – główne zagadnienia

Rozdział I. Plan wycofania usługi

1. **Scenariusze wycofania**
    1. Należy określić przewidywane scenariusze wycofania dla usługi, np. migracja on-premise, zmiana dostawcy etc.
    2. Dopuszczalne jest określenie alternatywnych scenariuszy w zależnie od sytuacji – np. nagłe zaprzestanie świadczenia usługi, rezygnacja z usługi po zakończeniu kontraktu etc.
2. **Wpływ zmiany na organizację**
    1. Należy opisać wpływ zmiany na organizację, tj. zmiany w procesach krytycznych, wpływ na zasoby ludzkie i strukturę organizacyjną, wymagania szkoleniowe etc.
3. **Opis transferu usługi oraz danych**
    1. Wysokopoziomowy opis procesu migracji usługi oraz danych, wymaganych narzędzi etc.
    2. Transfer usług to całokształt działań (w tym czynności prawnych) prowadzących do zwrotu Klientowi sprzętu Klienta, oprogramowania Klienta, całości przetwarzanych na zlecenie Klienta danych Klienta oraz w zależności od okoliczności prawnych przeniesienia na Klienta umów z osobami trzecimi wymaganych do realizacji usług zdefiniowanych w umowie w sposób gwarantujący nieprzerwaną realizację usług.
4. **Scenariusze testowe wycofania i kryteria akceptacji**
    1. Scenariusze testowe dla procesów migracji.
    2. Klient wraz z Dostawcą jest zobowiązany do wykonywania cyklicznych testów planu wyjścia o rekomendowanej częstotliwości nie rzadszej niż raz na 12 miesięcy.
5. **Backup danych i czasy migracji**
    1. Określenie czasu potrzebnego na przygotowanie projektu przełączenia, uruchomienie prac operacyjnych, uzyskanie odpowiednich zgód i poinformowanie użytkowników usługi o planowanym przełączeniu.
    2. Określenie czasu pobrania danych do migracji od Dostawcy. Czas musi uwzględniać zapisy umowne z Dostawcą na wyodrębnienie danych i fizyczne ich przekazanie (w tym warunki sieciowe i czas na zamontowanie danych).
    3. Określenie czasu dla procesu przełączenia usługi w wymiarze inicjalnym i docelowym migracji danych, a także uruchomieniu usługi na odtworzonych danych. Czas ten nie może naruszać przyjętego RTO i RPO dla usługi.
    4. Dla usług o znaczeniu krytycznym dla ciągłości działania Banku należy przechowywać backup lokalny danych przekazanych do chmury celem minimalizacji czasu przełączenia

usługi. Zakres backupu i czas retencji danych powinien zostać zdefiniowany z punktu widzenia ryzyka dla ciągłości działania. Backup ma na celu jedynie minimalizację czasu inicjalnego przełączenia najbardziej krytycznych danych. Całkowity czas migracji zakłada pozyskanie wszystkich danych od Dostawcy.

6. **Harmonogram migracji**

   1. Szacunkowy harmonogram migracji na „on-premise" lub do innej usługi. Powinien być to harmonogram projektowy, zawierać wymagane zasoby, zadania i kamienie milowe.

7. **Role i odpowiedzialności**

   1. Określenie ról i odpowiedzialności w procesie migracji.
   2. Obowiązki Dostawcy.
   3. W razie wypowiedzenia lub rozwiązania umowy, niezależnie od przyczyny, Dostawca usług chmurowych zapewni Klientowi, niezwłocznie po wygaśnięciu lub rozwiązaniu umowy, możliwość transferu danych Klienta poprzez:
      1) umożliwienie Klientowi pobrania danych Klienta ze swojej infrastruktury w terminie ustalonym przez Klienta i Dostawcę usług chmurowych;
      2) wydanie loginów i haseł zgodnie z umową;
      3) zapewnienie właściwej ochrony danych klienta znajdujących się w logach systemów współdzielonych;
      4) zwrot sprzętu Klienta wniesionego do infrastruktury Dostawcy, jeśli taka sytuacja miała miejsce;
      5) zwrot dokumentacji w wersji papierowej (o ile taka istniała).
   4. Dostawca usług chmurowych zapewni, w zależności od okoliczności prawnych, Klientowi możliwość ciągłego, nieprzerwanego korzystania z licencji niezbędnych do podtrzymania ciągłości działania usług, w tym możliwość przeniesienia, w zależności od okoliczności prawnych, na Klienta licencji, o których mowa w punkcie powyżej.
   5. Dostawca usług chmurowych jest zobowiązany do:
      1) usunięcia w sposób nieodwracalny danych Klienta oraz oprogramowania Klienta z zasobów Dostawcy oraz podwykonawców współpracujących;
      2) w szczególności usunięcia w sposób nieodwracalny danych Klienta z zasobów Dostawcy oraz podwykonawców współpracujących mających charakter danych osobowych oraz danych objętych tajemnicą bankową lub zawodową;
      3) współpracy z Klientem w zakresie transferu danych do Klienta lub innego podmiotu wskazanego przez Klienta;
      4) zapewnienia współpracy jego podwykonawców w zakresie realizacji planu wyjścia;
      5) określenia wspólnie z Klientem: a) szczegółowego harmonogramu planu wyjścia, b) szczegółowego zakresu prowadzonych czynności, c) szczegółowego sposobu realizacji planu wyjścia, d) odpowiedzialności Stron, e) środków technicznych niezbędnych do realizacji planu wyjścia, jeśli są potrzebne.

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

   8.1. Scenariusz 1. Migracja „on-premise"

   1. Należy zdefiniować parametry środowiska lokalnego w zakresie dostępności, wydajności i pojemności w celu przejęcia usługi chmurowej, w której się znajdują.

2. Plan wyjścia powinien w szczególności obejmować także:
   1) wyznaczenie dedykowanych managerów odpowiedzialnych za przeprowadzenie procesu transferu usług chmurowych;
   2) przygotowanie, w uzgodniony przez Strony sposób, do transportu całości sprzętu Klienta, jeżeli taki był elementem świadczenia usług;
   3) wydanie Klientowi haseł i loginów pozwalających na dalsze korzystanie z danych klienta, w tym haseł i loginów do baz danych oraz wszystkich systemów objętych usługami;
   4) przekazanie przez Dostawcę usług chmurowych wszystkich informacji dotyczących sposobu dostarczania i obsługi świadczonych usług istotnych z punktu widzenia przeniesienia usług i przekazania kompetencji utrzymaniowych innemu podmiotowi;
   5) zapewnienie po stronie Dostawcy usług chmurowych bezpiecznego połączenia teleinformatycznego platformy wykorzystywanej do świadczenia usług chmurowych do systemu informatycznego wskazanego przez Klienta, z wykorzystaniem bezpiecznej sieci teleinformatycznej, w celu przeprowadzenia transferu danych klienta;
   6) zapewnienie przez Klienta środków technicznych po stronie systemu informatycznego Klienta umożliwiających zestawienie połączenia teleinformatycznego;
   7) zapewnienie transferu do systemu teleinformatycznego wskazanego przez Klienta całości danych klienta w sposób zapewniający ich pełne bezpieczeństwo i integralność oraz poziom transferu umożliwiający sprawne przeniesienie wszystkich danych klienta w czasie uzgodnionym przez Strony, a także wydania wszystkich kopii zapasowych danych klienta (o ile były sporządzane zgodnie z umową),
   8) przekazanie przez Dostawcę usług chmurowych wiedzy specyficznej dla realizowanych usług chmurowych, w takim zakresie, w jakim będzie to niezbędne do dalszej realizacji usług przez Klienta lub podmiot trzeci wskazany przez Klienta;
   9) niezwłocznie po zakończeniu świadczenia usług chmurowych usunięcie przez Dostawcę oraz podwykonawców Dostawcy usług chmurowych, w sposób trwały oraz zgodny z najlepszymi praktykami w tym zakresie, całości ewentualnie posiadanych kopii danych klienta (po uprzednim transferze takich danych do Klienta lub podmiotu wskazanego przez Klienta) oraz wszystkich danych i informacji (np. plików konfiguracyjnych specyficznie wykorzystywanych dla danego Klienta a niestanowiących części usług chmurowych Dostawcy) wykorzystywanych do konfiguracji, obsługi, backupu i archiwizacji systemu lub poszczególnych jego elementów.
3. Wymagania uwzględniają:
   1) odpowiednią ilość serwerów wraz z określeniem ich lokalizacji w centrach danych;
   2) wolne miejsce w centrach danych wraz z zapewnieniem fizycznej możliwości wpięcia w infrastrukturę;
   3) odpowiednią konfigurację serwerów, zapewniającą odpowiednią wydajność (odpowiednia ilość procesorów, odpowiednia ilość pamięci RAM, odpowiednie połączenia sieciowe, odpowiednie zasoby dyskowe);
   4) odpowiednią ilość przestrzeni dyskowej, która jest niezbędna do przejęcia danych przechowywanych w usłudze chmurowej; przestrzeń ta musi zostać przewidziana na okres jednego roku i aktualizowana raz do roku w planie przełączenia.
4. Zdefiniowane środowisko jest dostępne w jednym z poniższych podejść:
   1) fizycznie zakupione i skonfigurowane na potrzeby migracji;
   2) niezakupione, ale dostępne u producenta w podanej konfiguracji; taka dostępność

potwierdzona jest listem intencyjnym lub umową z Dostawcą, w której określono czas pozyskania i dostarczenia infrastruktury;

3) posiadana jest infrastruktura wykorzystywana do innych celów, która może zostać w razie uruchomienia planu zwolniona i w okresie przejściowym do zakupu może zostać użyta celem wykonania przełączenia.

8.2. Scenariusz 2. Migracja do innego dostawcy usług

1. Alternatywne usługi chmurowe wraz z Dostawcami, czasem uruchomienia i kosztem.

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

2. Określenie minimalnych wymagań bezpieczeństwa dla wycofania usługi:
   1) wymagania bezpieczeństwa dla docelowego rozwiązania po wycofaniu,
   2) wymagania bezpieczeństwa dla procesu migracji.
3. Proces migracji danych i przełączenia usługi.
4. Proces musi uwzględniać poniższe punkty wraz z ich operacyjnym rozwinięciem i technicznym uszczegółowieniem. Na potrzeby opisu procesu powinny zostać opracowane instrukcje wykonawcze dla wszystkich ról zdefiniowanych w procesie.
   1) Formalna decyzja o wycofaniu lub przełączeniu, określenie zasad wydania takiej decyzji i jej trybu;
   2) poinformowanie użytkowników o uruchomieniu planu przełączenia wraz z podaniem przewidywanych czasów i skutków dla użytkowników;
   3) pozyskanie i skonfigurowanie infrastruktury;
   4) wyodrębnienie danych od Dostawcy i fizyczne ich przekazanie;
   5) zamontowanie danych z backupu w środowisku Banku i poinformowanie o inicjalnym uruchomieniu usługi;
   6) zamontowanie danych od Dostawcy i poinformowanie o pełnym przełączeniu usługi.
5. Klient może podjąć decyzję o wyłączeniu realizacji niektórych zobowiązań wynikających z planu wyjścia. W przypadku podjęcia takiej decyzji przez Klienta Strony dostosowują plan wyjścia do zmian wprowadzonych przez Klienta – w szczególności w związku z rezygnacją z określonych zadań Klient może żądać skrócenia harmonogramu realizacji planu wyjścia.
6. Strony w czasie realizacji planu wyjścia zapewnią personel techniczny o kompetencjach i wiedzy umożliwiającej realizację uzgodnionego przez Strony planu wyjścia w uzgodnionym terminie.
7. Strony zapewnią dostęp do informacji niezbędnych do wykonania powierzonych zadań w ramach planu wyjścia, w tym szczegóły dotyczące odpowiedniego systemu informatycznego.
8. Strony w trakcie trwania umowy przygotowują szczegółowe plany wyjścia dla poszczególnych usług oraz zobowiązują się do ich częściowego lub całościowego przetestowania w trakcie trwania umowy.

9. Cały proces wyjścia powinien zakończyć się podpisaniem protokołu, w którym jedna strona potwierdza przejęcie sprzętu, licencji, oprogramowania itp., a druga strona potwierdza usunięcie danych klienta.
10. Strony w trakcie trwania umowy dokonają przybliżonej oceny kosztów planu wyjścia.

Rozdział II. Plan nagłego zaprzestania świadczenia usługi

1. W przypadku nagłego i długotrwałego braku dostępu do usługi z powodu problemów po stronie Dostawcy usługi (dłuższe niż zakłada SLA), przewidując przywrócenie usługi w przeciągu [ ] godzin, należy wykonać plan znajdujący się w tym punkcie.
2. Wymagania techniczne zbieżne z rozdziałem I, przy założeniu powrotu do wykorzystywanej usługi chmurowej.
   1) Określenie, jakie konta i jakie uprawnienia zostaną użyte do przełączenia.
   2) Przełączenie usługi zakłada dostęp tylko do wybranego zakresu danych w trybie nagłym. Należy podać zakres i typ danych, jaki będzie dostępny i jak zostanie pozyskany. Przyjmuje się zatem ryzyko nieposiadania dostępu do całości danych i uruchomienia funkcjonalności przesyłania wiadomości bieżących.
   3) Udokumentowane instrukcje dla Administratorów Systemów wraz z przygotowanymi zgłoszeniami serwisowymi (RFC) dla wszystkich zadań przełączenia.
   4) W przypadku problemów na poziomie CRITICAL powiadamiany jest odpowiedni dział w ramach struktury IT Banku oraz uruchamiany jest Dostawca w ramach wykupionej usługi wsparcia. Równolegle rejestrowany jest problem, którego obsługa realizowana jest w ramach oddzielnego procesu (problem management Banku).
   5) Jeżeli Bank nie ma zdefiniowanego procesu problem management, należy opracować także dedykowaną instrukcję, role i zadania dla koordynatora przełączenia usługi. Instrukcja taka zawiera przede wszystkim zasady poinformowania użytkowników o przełączeniu usługi.
   6) Powrót do usługi chmurowej jest opisany powyżej poprzez instrukcje dla administratorów i rozpisane zadania.

Załącznik nr 16

do Standardu PolishCloud 2.0

Szablon dokumentacji kontroli ISO27001

ISO27001 – opis kontroli po stronie Dostawcy

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.5.1.1	Polityki bezpieczeństwa informacji	Zabezpieczenie Zbiór polityk bezpieczeństwa informacji powinien być opracowany, zatwierdzony przez kierownictwo, opublikowany i zakomunikowany pracownikom i właściwym stronom zewnętrznym.		Przykładowy opis	Przykładowy opis		
A.5.1.2	Przegląd polityk bezpieczeństwa informacji	Zabezpieczenie Polityki bezpieczeństwa informacji należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne.					
A.6.1.1	Role i odpowiedzialność za bezpieczeństwo informacji	Zabezpieczenie Odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana.					
A.6.1.2	Rozdzielanie obowiązków	Zabezpieczenie Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić, celem ograniczenia okazji do nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia organów organizacji.					
A.6.1.3	Kontakty z organami władzy	Zabezpieczenie Należy utrzymywać stosowne kontakty z właściwymi organami władzy.					
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów	Zabezpieczenie Należy utrzymywać stosowne kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa.					
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Zabezpieczenie Bezpieczeństwo informacji należy uwzględnić w zarządzaniu projektami, niezależnie od rodzaju projektu.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.6.2.1	Polityka stosowania urządzeń mobilnych	Zabezpieczenie Należy wprowadzić politykę oraz wspierające ją zabezpieczenia w celu zarządzania ryzykami, wynikającymi z użytkowania urządzeń mobilnych.					
A.6.2.2	Telepraca	Zabezpieczenie Należy wdrożyć politykę oraz wspierające ją zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania telepracy.					
A.7.1.1	Postępowanie sprawdzające	Zabezpieczenie Historię wszystkich kandydatów do pracy należy zweryfikować zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp oraz dostrzeżonych ryzyk.					
A.7.1.2	Warunki zatrudnienia	Zabezpieczenie Umowy z pracownikami i kontrahentami powinny określać odpowiedzialność stron w obszarze bezpieczeństwa informacji.					
A.7.2.1	Odpowiedzialność kierownictwa	Zabezpieczenie Kierownictwo powinno wymagać, aby wszyscy pracownicy i kontrahenci stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami.					
A.7.2.2	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Zabezpieczenie Wszyscy pracownicy organizacji oraz, w stosownych wypadkach, kontrahenci powinni przejść stosowne kształcenie i szkolenie uświadamiające oraz regularnie otrzymywać aktualizacje polityk i procedur związanych z ich stanowiskiem pracy.					
A.7.2.3	Postępowanie dyscyplinarne	Zabezpieczenie Postępowanie dyscyplinarne wobec pracowników naruszających zasady bezpieczeństwa informacji należy prowadzić na podstawie ustalonych i przedstawionych im zasad.					
A.7.3.1	Zakończenie zatrudnienia lub zmian zakresu obowiązków	Zabezpieczenie Należy określić i przedstawić pracownikowi lub kontrahentowi, które odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, a następnie egzekwować je.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.8.1.1	Inwentaryzacja aktywów	Zabezpieczenie Należy identyfikować aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów.					
A.8.1.2	Własność aktywów	Zabezpieczenie Aktywa znajdujące się w ewidencji należy przypisać ich właścicielom.					
A.8.1.3	Akceptowalne użycie aktywów	Zabezpieczenie Należy zidentyfikować, udokumentować i wdrożyć zasady akceptowalnego użycia informacji oraz aktywów związanych z informacjami i środkami przetwarzania informacji.					
A.8.1.4	Zwrot aktywów	Zabezpieczenie Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa organizacji.					
A.8.2.1	Klasyfikowanie informacji	Zabezpieczenie: Informacje powinny być sklasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.					
A.8.2.2	Oznaczanie informacji	Zabezpieczenie Należy opracować i wdrożyć odpowiedni zbiór procedur oznaczania informacji, zgodnych z przyjętym w organizacji schematem klasyfikacji informacji.					
A.8.2.3	Postępowanie z aktywami	Zabezpieczenie Należy opracować i wdrożyć procedury postępowania z aktywami, zgodnie z przyjętym przez organizację schematem klasyfikacji informacji.					
A.8.3.1	Zarządzanie nośnikami wymiennymi	Zabezpieczenie Organizacja powinna wdrożyć procedury zarządzania nośnikami wymiennymi, zgodnie ze schematem klasyfikacji przyjętym w organizacji.					
A.8.3.2	Wycofywanie nośników	Zabezpieczenie Nośniki, które nie będą dłużej wykorzystywane, należy bezpiecznie wycofać, zgodnie z formalnymi procedurami.					
A.8.3.3	Przekazywanie nośników	Zabezpieczenie Nośniki zawierające informacje należy chronić przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.9.1.1	Polityka kontroli dostępu	Zabezpieczenie Politykę kontroli dostępu należy ustanowić, udokumentować i poddawać przeglądom zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji.					
A.9.1.2	Dostęp do sieci i usług sieciowych	Zabezpieczenie Użytkownicy powinni mieć dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia.					
A.9.2.1	Rejestrowanie i wyrejestrowanie użytkowników	Zabezpieczenie W celu umożliwienia przydzielania praw dostępu należy wdrożyć formalny proces rejestrowania i wyrejestrowywania użytkowników.					
A.9.2.2	Przydzielanie dostępu użytkownikom	Zabezpieczenie Należy wdrożyć formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników.					
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	Zabezpieczenie Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować.					
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	Zabezpieczenie Przydzielanie poufnych informacji uwierzytelniających powinno podlegać formalnemu procesowi zarządzania.					
A.9.2.5	Przegląd praw dostępu użytkowników	Zabezpieczenie Właściciele aktywów powinni przeglądać prawa dostępu użytkowników w regularnych odstępach czasu.					
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	Zabezpieczenie Przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji należy odbierać po zakończeniu zatrudnienia, umowy lub porozumienia, lub dostosowywać do zaistniałych zmian.					
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	Zabezpieczenie Użytkownicy powinni mieć obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.9.4.1	Ograniczenie dostępy do informacji	Zabezpieczenie Dostęp do informacji oraz funkcji systemu aplikacyjnego należy ograniczać zgodnie z polityką kontroli dostępu.					
A.9.4.2	Procedury bezpiecznego logowania	Zabezpieczenie Tam, gdzie polityka kontroli dostępu tego wymaga, dostęp do systemów i aplikacji powinien być kontrolowany przez procedurę bezpiecznego logowania.					
A.9.4.3	System zarządzania hasłami	Zabezpieczenie Systemy zarządzania hasłami powinny być interaktywne i zapewniać wybór haseł dobrej jakości.					
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych	Zabezpieczenie Wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, powinno podlegać ograniczeniom i ścisłemu nadzorowi.					
A.9.4.5	Kontrola dostępu do kodów źródłowych programów	Zabezpieczenie Dostęp do kodu źródłowego programów powinien być ograniczony.					
A.10.1.1	Polityka stosowania zabezpieczeń kryptograficznych	Zabezpieczenie Należy opracować i wdrożyć politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji.					
A.10.1.2	Zarządzanie kluczami	Zabezpieczenie Należy opracować politykę dotyczącą korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożyć ją na wszystkich etapach cyklu życia kluczy.					
A.11.1.1	Fizyczna granica obszaru bezpiecznego	Zabezpieczenie Należy określić granice bezpieczeństwa i wykorzystać je do zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji.					
A.11.1.2	Fizyczne zabezpieczenie wejść	Zabezpieczenie Bezpieczne strefy należy chronić odpowiednimi zabezpieczeniami wejść zapewniającymi dostęp wyłącznie osobom uprawnionym.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.11.1.3	Zabezpieczenie biur, pomieszczeń i obiektów	Zabezpieczenie Należy zaprojektować i stosować fizyczne zabezpieczenia biur, pomieszczeń i obiektów.					
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Zabezpieczenie Należy zaprojektować i stosować fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami.					
A.11.1.5	Praca w obszarach bezpiecznych	Zabezpieczenie Należy zaprojektować i stosować procedury pracy w obszarach bezpiecznych.					
A.11.1.6	Obszary dostaw i załadunku	Zabezpieczenie Należy sprawować nadzór nad punktami dostępu takimi jak obszary dostaw i załadunku oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń i, jeśli to możliwe, odizolować je od środków przetwarzania informacji, aby zapobiec nieuprawnionemu dostępowi.					
A.11.2.1	Lokalizacja i ochrona sprzętu	Zabezpieczenie Sprzęt należy umieścić i chronić w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.					
A.11.2.2	Systemy wspomagające	Zabezpieczenia Sprzęt należy chronić przed awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających.					
A.11.2.3	Bezpieczeństwo okablowania	Zabezpieczenie Okablowanie zasilające oraz telekomunikacyjne przenoszące dane lub wspomagające usługi informacyjne należy chronić przez przechwyceniem, zakłóceniem lub uszkodzeniem.					
A.11.2.4	Konserwacja sprzętu	Zabezpieczenie Sprzęt należy prawidłowo konserwować w celu zapewnienia jego ciągłej dostępności i integralności.					
A.11.2.5	Wynoszenie aktywów	Zabezpieczenie Sprzętu, informacji i programów nie należy wynosić poza siedzibę organizacji bez uzyskania wcześniejszego zezwolenia.					
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Zabezpieczenie Aktywa wynoszone poza siedzibę organizacji należy zabezpieczyć przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Zabezpieczenie Przed zbyciem lub przekazaniem sprzętu do ponownego użycia należy sprawdzić wszystkie jego składniki zawierające nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.					
A.11.2.8	Pozostawianie sprzętu użytkownika bez opieki	Zabezpieczenie Użytkownicy powinni zapewnić odpowiednią ochronę sprzętu pozostawianego bez opieki.					
A.11.2.9	Polityka czystego biurka i ekranu	Zabezpieczenie Należy wprowadzić politykę czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania informacji.					
A.12.1.1	Dokumentowanie procedur eksploatacyjnych	Zabezpieczenie Procedury eksploatacyjne powinny być udokumentowane i udostępniane wszystkim potrzebującym ich użytkownikom.					
A.12.1.2	Zarządzanie zmianami	Zabezpieczenie Zmiany w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji, powinny być nadzorowane.					
A.12.1.3	Zarządzanie pojemnością	Zabezpieczenie Należy monitorować i dostosowywać wykorzystanie zasobów oraz przewidywać wymaganą pojemność w przyszłości dla zapewnienia właściwej wydajności systemu.					
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Zabezpieczenie Należy oddzielić środowiska rozwojowe, testowe i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.					
A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem	Zabezpieczenie Należy wdrożyć zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.					
A.12.3.1	Zapasowe kopie informacji	Zabezpieczenie Zapasowe kopie informacji, oprogramowania i obrazów systemów należy regularnie wykonywać i testować zgodnie z ustaloną polityką kopii zapasowych.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.12.4.1	Rejestrowanie zdarzeń	Zabezpieczenie Należy tworzyć, przechowywać i systematycznie przeglądać dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji.					
A.12.4.2	Ochrona informacji w dziennikach zdarzeń	Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń należy chronić przed manipulacją i nieuprawnionym dostępem.					
A.12.4.3	Rejestrowanie działań administratorów i operatorów	Zabezpieczenie Działania administratorów i operatorów systemów należy rejestrować, a dzienniki chronić i systematycznie przeglądać.					
A.12.4.4	Synchronizacja zegarów	Zabezpieczenie Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa należy zsynchronizować z jednym wzorcowym źródłem czasu.					
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	Zabezpieczenie Należy wdrożyć procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych.					
A.12.6.1	Zarządzanie podatnościami technicznymi	Zabezpieczenie Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych należy niezwłocznie pozyskiwać, oceniać stopień narażenia organizacji na te podatności i podejmować odpowiednie środki w celu przeciwdziałania związanemu z nimi ryzyku.					
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	Zabezpieczenie Należy ustanowić i wdrożyć zasady instalowania oprogramowania przez użytkowników.					
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	Zabezpieczenie Należy starannie zaplanować i uzgodnić wymagania audytu oraz działania obejmujące weryfikację systemów produkcyjnych, w celu zminimalizowania zakłóceń w procesach biznesowych.					
A.13.1.1	Zabezpieczenia sieci	Zabezpieczenie Sieci powinny być zarządzane i nadzorowane w celu ochrony informacji w systemach i aplikacjach.					
A.13.1.2	Bezpieczeństwo usług sieciowych	Zabezpieczenie Umowy dotyczące wszystkich usług sieciowych, świadczonych wewnętrznie lub zlecanych na zewnątrz, powinny zawierać zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.13.1.3	Rozdzielanie sieci	Zabezpieczenie Grupy usług informacyjnych, użytkowników i systemów informacyjnych powinny być rozdzielone w strukturze sieci.					
A.13.2.1	Polityki i procedury przesyłania informacji	Zabezpieczenie Należy wdrożyć formalne polityki przesyłania informacji, procedury i zabezpieczenia w celu ochrony informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności.					
A.13.2.2	Porozumienia dotyczące przesyłania informacji	Zabezpieczenie Porozumienia powinny uwzględniać bezpieczne przesyłanie informacji biznesowych między organizacją i podmiotami zewnętrznymi.					
1.13.2.3	Wiadomości elektroniczne	Zabezpieczenie Informacje przekazywane w formie wiadomości elektronicznych powinny być odpowiednio chronione.					
A.13.2.4	Umowy o zachowaniu poufności	Zabezpieczenie Należy zidentyfikować, regularnie przeglądać i dokumentować wymagania odnoszące się do umów o zachowaniu poufności lub nieujawnianiu informacji w sposób odzwierciedlający potrzeby organizacji w zakresie ochrony informacji.					
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji	Zabezpieczenie Wymagania dotyczące bezpieczeństwa informacji należy włączyć do wymagań stawianych nowym systemom informacyjnym lub rozbudowie systemów istniejących.					
A.14.1.2	Zabezpieczenie usług aplikacyjnych w sieciach publicznych	Zabezpieczenie Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, należy chronić przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnieniem i zmianami.					
A.14.1.3	Ochrona transakcji usług aplikacyjnych	Zabezpieczenie Informacje związanie z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje należy chronić, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, nieuprawnionemu powieleniu lub odtworzeniu.					
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	Zabezpieczenie Należy ustanowić zasady prac nad rozwojem oprogramowania i systemów oraz stosować je w pracach rozwojowych prowadzonych wewnątrz organizacji.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.14.2.2	Procedury kontroli zmian w systemach	Zabezpieczenie Należy nadzorować zmiany w systemach podczas ich cyklu rozwojowego, przy użyciu formalnych procedur kontroli zmian.					
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	Zabezpieczenie Po dokonaniu zmian w platformach produkcyjnych należy przeprowadzić przegląd krytycznych aplikacji biznesowych lub przetestować je, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo.					
A.14.2.4	Ograniczenia dotyczące zmian w systemach oprogramowania	Zabezpieczenie Modyfikacji w pakietach oprogramowania należy dokonywać z rozwagą i ograniczać się do zmian niezbędnych, a wszystkie takie zmiany ściśle nadzorować.					
A.14.2.5	Zasady projektowania bezpiecznych systemów	Zabezpieczenie Należy ustanowić, udokumentować i utrzymywać zasady projektowania bezpiecznych systemów oraz stosować je do wszystkich prac implementacyjnych nad systemami informacyjnymi.					
A.14.2.6	Bezpieczne środowisko rozwojowe	Zabezpieczenie Organizacje powinny ustanowić i odpowiednio chronić bezpieczne środowiska rozwojowe przeznaczone do rozwoju systemów oraz prac integracyjnych obejmujących całość cyklu rozwojowego procesów.					
A.14.2.7	Prace rozwojowe zlecane podmiotom zewnętrznym	Zabezpieczenie Organizacja powinna nadzorować i monitorować prace rozwojowe nad systemami zlecone podmiotom zewnętrznym.					
A.14.2.8	Testowanie bezpieczeństwa systemów	Zabezpieczenie Funkcje bezpieczeństwa należy testować w czasie prac rozwojowych.					
A.14.2.9	Testy akceptacyjne systemów	Zabezpieczenie Dla nowych systemów informacyjnych, ich modernizacji i nowych wersji systemów należy ustanowić programy testów akceptacyjnych i kryteria z nimi związane.					
A.14.3.1	Ochrona danych testowych	Zabezpieczenie Dane testowe należy starannie wybierać, chronić i nadzorować.					
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z Dostawcami	Zabezpieczenie Należy uzgodnić z Dostawcą i udokumentować wymagania bezpieczeństwa informacji celem zmniejszenia ryzyk związanych z dostępem Dostawcy do aktywów organizacji.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z Dostawcami	Zabezpieczenie Należy ustanowić wszystkie istotne wymagania dotyczące bezpieczeństwa informacji i uzgodnić je z każdym Dostawcą, który może uzyskać dostęp, przetwarzać, przechowywać, przesyłać lub dostarczać elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do organizacji.					
A.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	Zabezpieczenie Porozumienia z Dostawcami powinny uwzględniać wymagania odnoszące się do ryzyk w bezpieczeństwie informacji, związanych z usługami technologii informacyjnych i telekomunikacyjnych oraz łańcuchem dostaw produktów.					
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez Dostawców	Zabezpieczenie Organizacje powinny regularnie monitorować, przeglądać i audytować dostarczanie usług zewnętrznych.					
A.15.2.2	Zarządzanie zmianami w usługach świadczonych przez Dostawców	Zabezpieczenie Należy zarządzać zmianami w zakresie świadczenia usług przez Dostawców, w tym utrzymaniem i doskonaleniem istniejących polityk bezpieczeństwa informacji, procedur i zabezpieczeń, z uwzględnieniem krytyczności informacji, systemów i procesów biznesowych, których dotyczą, oraz ponownego szacowania ryzyka.					
A.16.1.1	Odpowiedzialność i procedury	Zabezpieczenie Należy ustanowić odpowiedzialność kierownictwa oraz procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem informacji.					
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zabezpieczenie Zdarzenie związane z bezpieczeństwem informacji należy zgłaszać odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe.					
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji	Zabezpieczenie Należy zobowiązać pracowników oraz kontrahentów korzystających z systemów usług informacyjnych organizacji do odnotowania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w systemach lub usługach.					
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	Zabezpieczenie Zdarzenia związane z bezpieczeństwem informacji należy ocenić i podjąć decyzję w sprawie zakwalifikowania ich jako incydentów związanych z bezpieczeństwem informacji.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji	Zabezpieczenie Reakcja na incydenty związane z bezpieczeństwem informacji powinna być zgodna z udokumentowanymi procedurami.					
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Zabezpieczenie Wiedzę zdobytą podczas analizy i rozwiązywania incydentów związanych z bezpieczeństwem informacji należy wykorzystać do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów.					
A.16.1.7	Gromadzenie materiału dowodowego	Zabezpieczenie Organizacja powinna określić i stosować procedury identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy.					
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji	Zabezpieczenie Organizacja powinna określić wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach, np. w czasie kryzysu czy katastrofy.					
A.17.1.2	Wdrożenie ciągłości bezpieczeństwa informacji	Zabezpieczenie Organizacja powinna ustanowić, udokumentować, wdrożyć i utrzymywać procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji.					
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	Zabezpieczenie Organizacja powinna weryfikować ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu celem zapewnienia ich aktualności i skuteczności w niekorzystnych sytuacjach.					
A.17.2.1	Dostępność środków przetwarzania informacji	Zabezpieczenie Środki przetwarzania informacji należy wdrażać z nadmiarem wystarczającym do spełnienia wymagań dostępności.					
A.18.1.1	Określenie stosownych wymagań prawnych i umownych	Zabezpieczenie Wszystkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania należy zidentyfikować, udokumentować i aktualizować dla każdego systemu informacyjnego oraz całości organizacji.					
A.18.1.2	Prawa własności intelektualnej	Należy wdrożyć odpowiednie procedury zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.					

ID zabezpieczenia (zał. A)	Cel stosowania zabezpieczeń	Zabezpieczenie	Zgodność z ISO 27001 Tak/Nie/ Częściowo/ Nie dotyczy	Opis implementacji zabezpieczenia	Testowanie i audytowanie zabezpieczeń	Zasady testowania Samoocena/ Niezależne testowanie	Plany naprawcze (przy braku zgodności lub zgodności częściowej)
A.18.1.3	Ochrona zapisów	Zabezpieczenie Zapisy należy chronić przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem, stosownie do wymagań prawnych, regulacyjnych, umownych i biznesowych.					
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę	Zabezpieczenie Należy zapewnić prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji.					
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	Zabezpieczenie Zabezpieczenia kryptograficzne należy stosować zgodnie z odpowiednimi umowami, przepisami i regulacjami.					
A.18.2.1	Niezależny przegląd bezpieczeństwa informacji	Zabezpieczenie Podejście organizacji do zarządzania bezpieczeństwem informacji oraz jego wdrożenie (tzn. cele stosowania zabezpieczeń, zabezpieczenia, polityki, procesy i procedury dotyczące bezpieczeństwa informacji) należy poddawać niezależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy nastąpią istotne zmiany.					
A.18.2.2	Zgodność z politykami bezpieczeństwa i standardami	Zabezpieczenie Kierownicy powinni regularnie dokonywać przeglądu zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa, standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności.					
A.18.2.3	Sprawdzania zgodności technicznej	Zabezpieczenie Należy regularnie przeglądać systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa informacji i standardami obowiązującymi w organizacji.					

Załącznik nr 17

do Standardu PolishCloud 2.0

Lista zagadnień dla wyboru Dostawców związanych z bezpieczeństwem

Mając na względzie, że finalnie analizie zgodności z Komunikatem Regulatora podlega całe rozwiązanie realizujące określoną funkcjonalność biznesową, a nie usługa przetwarzania w chmurze jako taka (która zazwyczaj ma możliwość elastycznej konfiguracji), należy z wnikliwością podejść do rozważań i oczekiwań stawianych w stosunku do Dostawcy usług przetwarzania w chmurze oraz dostawcy rozwiązania biznesowego działającego w chmurze (które w szczególności może mieć architekturę hybrydową). Aby w kompletny sposób podejść do oceny dostawcy rozwiązania bazującego na usłudze chmurowej w kontekście wymagań Komunikatu chmurowego KNF, proponujemy poniższą listę pytań, które należy omówić z planowanym dostawcą rozwiązania, aby potwierdzić gotowość proponowanego rozwiązania/usługi w kontekście wspomnianych wymagań, a z którymi zgodność m.in. będzie musiał wykazać Bank przed Regulatorem w celu uruchomienia przetwarzania chmurowego w ramach tego rozwiązania/usługi.

Jakie zagadnienia w kontekście oceny Dostawcy rozwiązania bazującego na usłudze chmurowej powinien rozważyć Bank (zgodnie z Komunikatem chmurowym)?

1. Kompetencje chmurowe i doświadczenia dostawcy rozwiązania, w tym posiadane certyfikaty dla osób i usług/rozwiązań.
2. Jakie szkolenia z zakresu usługi/rozwiązania chmurowego oferuje dostawca rozwiązania oraz Dostawca usług przetwarzania w chmurze?
3. Jakie wsparcie dla Banku i dla dostawcy rozwiązania oferuje Dostawca usługi chmurowej?
4. Czy dostawca rozwiązania jest w stanie zaproponować rozwiązanie w formule *proof of concept* lub MVP dla zróżnicowanych przez Bank scenariuszy/przypadków użycia?
5. Jakie są możliwości skalowania rozwiązania działającego w chmurze? Czy istnieją jakieś ograniczenia w skalowaniu wertykalnym bądź horyzontalnym?
6. Jakie możliwości wyjścia z usługi chmurowej zapewnia dostawca rozwiązania działającego w chmurze publicznej? Czy możliwe jest przeniesienie rozwiązania do infrastruktury on-premise lub do innego Dostawcy usług chmurowych?
7. W jakim zakresie dostawca rozwiązania wspiera zapewnienie ciągłości działania rozwiązania chmurowego? Jaka jest rola i w jaki sposób Dostawca usług przetwarzania w chmurze wspiera zapewnienie ciągłości działania usługi?
8. Czy Dostawca rozwiązania w ramach oferowanego rozwiązania/usługi chmurowej wykorzystuje standardy i działa zgodnie z normami zarządzania bezpieczeństwem informacji i ciągłości działania? Czy i w jakim zakresie podlegał certyfikacji ISO27001-18 oraz ISO22301?

9. Czy lokalizacje CPD, jakie będą wykorzystywane do świadczenia usługi chmurowej dla Banku, spełniają wymagania norm wskazanych w Komunikacie (PN-EN 50600, ANSI/TIA-942)?

10. Z jakich mechanizmów kontroli dostępu i separacji danych korzysta dostawca rozwiązania w ramach oferowanego rozwiązania opartego o usługę chmurową? Czy proces ten jest udokumentowany i poddawany cyklicznym przeglądom? Czy możliwy jest niezależny audyt tego obszaru u Dostawcy?

11. Z jakich mechanizmów szyfrowania korzysta dostawca rozwiązania zarówno dla danych „at rest", jak i „in transit" w ramach oferowanego rozwiązania opartego o usługę chmurową? Jakie podejście do zarządzania kluczami stosuje/rekomenduje Dostawca w ramach oferowanej usługi chmurowej (patrz: pytania o kryptografię w Załączniku nr 18)?

12. Z jakich mechanizmów monitorowania korzysta dostawca w ramach oferowanego rozwiązania opartego o usługę chmurową? Jakie podejście do logowania stosuje/rekomenduje dostawca w ramach oferowanej usługi chmurowej (patrz: pytania o monitorowanie w Załączniku nr 19)?

Bibliografia:

1. GCP foundation guide: https:/services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf
2. Microsoft Cloud Adoption Framework: https:/azure.microsoft.com/en-us/cloud-adoption-framework/
3. Microsoft Well-Architected Framework: https:/docs.microsoft.com/en-us/azure/architecture/framework/
4. IBM cloud adoption and transformation: https:/www.ibm.com/cloud/architecture/adoption
5. IBM Cloud Adoption and Transformation Framework: https:/www.ibm.com/cloud/architecture/adoption/dimensions

Załącznik nr 18

do Standardu PolishCloud 2.0

Kryptografia

Jednym z wymagań Komunikatu KNF, które rodzi wiele wątpliwości Podmiotów Nadzorowanych, jest kwestia kryptografii i zarządzania kluczami kryptograficznymi. Aby ułatwić Bankom i Dostawcom usług chmurowych odpowiednie przygotowanie tego obszaru, przygotowaliśmy listę pytań, jakie podmiot powinien zadać sobie w celu oceny kompletności/gotowości tego aspektu bezpieczeństwa dla planowanego/realizowanego przetwarzania chmurowego w ramach usługi.

Lista pytań dla banku w kontekście szyfrowania:

Czy w kontekście usługi chmurowej, której wykorzystanie planuje Bank, zostało przeanalizowane i udokumentowane podejście do szyfrowania i zarządzania kluczami kryptograficznymi, w szczególności:

1. Czy Bank dysponuje dokumentacją szyfrowania „at rest" od Dostawcy usługi chmurowej i dokumentuje, w jaki sposób wykorzystuje te mechanizmy w ramach usługi chmurowej?
2. Czy Bank dysponuje dokumentacją szyfrowania „in transit" od Dostawcy usługi chmurowej i dokumentuje, w jaki sposób wykorzystuje te mechanizmy w ramach usługi chmurowej?
3. Czy Bank prowadzi rejestr odstępstw dla usług chmurowych, gdzie szyfrowanie własnym kluczem nie jest możliwe (wykorzystanie kluczy generowanych oraz/lub zarządzanych przez Dostawcę usługi chmurowej, zgodnie z przeprowadzonym szacowaniem ryzyka)?
4. Czy Bank prowadzi rejestr odstępstw dla usług chmurowych, w zakresie braku przechowywania kopii kluczy szyfrujących, które zostały wygenerowane lub są zarządzane przez Dostawcę usługi chmurowej (np. ze względu na brak technicznej możliwości pobrania klucza Dostawcy, uwzględniając wyniki szacowania ryzyka dla danej usługi chmurowej)?
5. W jaki sposób realizowane jest szyfrowanie kluczami generowanymi oraz zarządzanymi przez Bank? Czy Bank posiada udokumentowany proces zarządzania tworzeniem, wykorzystaniem, ochroną, niszczeniem kluczy szyfrujących oraz kontrolą tego procesu wraz z zarządzaniem uprawnieniami dostępu do kluczy?
6. Czy Bank opracował standard stosowania dostępnych w chmurach publicznych metod szyfrowania z wykorzystaniem własnego klucza (np. dla Customer Managed/Supplied Encryption Key; Bring/Hold Your Own Key)?
7. Czy Bank zamierza powierzać swojemu Dostawcy usług (w tym Dostawcy usług chmury obliczeniowej) generowanie oraz/lub zarządzanie kluczami szyfrującymi, które są używane do szyfrowania informacji przetwarzanej w usługach chmury obliczeniowej innego Dostawcy

usług chmury obliczeniowej? Jeśli tak, to czy mechanizm ten jest udokumentowany? Czy przeprowadzono analizę ryzyka dla wykorzystania takiego mechanizmu, w szczególności w kontekście możliwości utraty dostępu podmiotu nadzorowanego do kluczy szyfrujących?

8. Z jakich rozwiązań HSM i/lub KMS (Key Management System) będzie korzystał Bank do generowania kluczy kryptograficznych do szyfrowania danych w chmurze? Czy istnieje dokumentacja w zakresie korzystania z tych rozwiązań? Czy stosowany HSM spełnia wymagania minimum FIPS 140-2 Level 2 lub równoważne?

9. W jaki sposób zapewnione będą kompetencje w zakresie szyfrowania w Banku? Kto odpowiadać będzie w Banku za wdrożenie i utrzymanie rozwiązań w zakresie szyfrowania? Czy zapewnione zostało wsparcie Dostawcy w tym zakresie wraz z podziałem odpowiedzialności pomiędzy Dostawcę a Bank?

10. Czy Bank będzie miał możliwość monitorowania, czy i w jaki sposób są szyfrowane zasoby w chmurach publicznych, z których korzysta?

11. Czy proces przekazywania kluczy kryptograficznych pomiędzy środowiskiem Banku a usługami HSM w chmurze jest monitorowany, rozliczany i wykorzystuje wielowarstwowe mechanizmy ochrony na poziomie kanału komunikacyjnego, jak i procesu wymiany bezpiecznej przesyłki?

Lista pytań dla Dostawcy usług chmurowych w kontekście szyfrowania:

Czy i w jaki sposób rozwiązanie chmurowe proponowane przez Dostawcę (i jego podwykonawców) do świadczenia usługi chmurowej dla Banku adresuje kwestie szyfrowania i zarządzania kluczami kryptograficznymi wynikające z Komunikatu chmurowego UKNF i wewnętrznych standardów Banku, w szczególności w jaki udokumentowany sposób zapewnia (w przypadku negatywnej odpowiedzi na któreś z poniższych pytań, Dostawca potrafi wskazać, opisać i zapewnić alternatywne rozwiązanie adresujące to wymaganie lub uargumentować brak zgodności):

1. Szyfrowanie informacji w spoczynku „at rest”? Czy proces ten jest udokumentowany i może być przekazany do informacji Banku/Regulatora? Czy można zweryfikować działanie tego procesu?

2. Szyfrowanie informacji w trakcie transmisji „in transit” (również w chmurze pomiędzy innymi usługami/komponentami chmurowymi)? Czy proces ten jest udokumentowany i może być przekazany do informacji Banku/Regulatora? Czy można zweryfikować działanie tego procesu?

3. Zarządzanie kluczami szyfrującymi przez Dostawcę i przechowywanie ich m.in. w HSM, do którego dostęp jest kontrolowany (uwierzytelnianie, autoryzacja, logowanie i monitorowanie dostępu)? Czy proces ten jest udokumentowany i może być przekazany do informacji Banku/Regulatora?

4. Wewnętrzne mechanizmy kontroli dostępu do infrastruktury i urządzeń przechowujących klucze szyfrujące? Czy proces ten jest udokumentowany, kontrolowany, a wynik lub zapewnienie o weryfikacji może być przekazany do wiadomości Banku/Regulatora?

5. Usługę chmurową pozwalającą na szyfrowanie informacji przy pomocy klucza szyfrującego wygenerowanego, dostarczonego i/lub zarządzanego przez Bank? Czy też szyfrowanie informacji możliwe jest tylko kluczem generowanym i/lub zarządzanym przez Dostawcę?
6. Usługę chmurową pozwalającą na używanie i przechowywanie kluczy szyfrujących lokalnie w infrastrukturze Banku (możliwość pobrania i przechowywania przez Bank kopii kluczy szyfrujących)? Czy też możliwe jest przechowywanie kluczy szyfrujących tylko w infrastrukturze Dostawcy?
7. Usługę chmurową pozwalającą na używanie i przechowywanie kluczy szyfrujących innego Dostawcy?
8. Wykorzystanie rozwiązania HSM w chmurze, które spełnia wymagania minimum FIPS 140-2 Level 2 lub równoważne?
9. Nadrzędny klucz pozwalający na odszyfrowanie informacji np. na potrzeby procedury *Break Glass*? Jeśli tak, w jakich sytuacjach może on być wykorzystywany? Jak jest monitorowany dostęp do niego?
10. Kompetencje w zakresie szyfrowania? W jakim zakresie Dostawca zakłada wsparcie nimi Banku (np. szkolenia, doradztwo, wsparcie, utrzymanie)?
11. Wdrożone mechanizmy kontroli, monitorowania, rozliczania dostępu oraz wykorzystania kluczy kryptograficznych w procesie szyfrowania/deszyfrowania danych Banku (dostępność wewnętrznych mechanizmów Usługodawcy zapewniających monitorowanie i rozliczalność realizowanych procesów kryptograficznych oraz dostępu do zasobów Banku)?
12. Mechanizmy i algorytmy kryptograficzne usługi chmurowej spełniające wymagania zdefiniowane w standardzie kryptografii Banku (o ile istnieje taki wewnętrzny dokument i został on udostępniony Dostawcy)?
13. Możliwość przeprowadzenia audytu na wypadek, gdyby była potrzeba? Czy proces ten jest udokumentowany?

Źródła:

1. Wprowadzenie do mechanizmów szyfrowania danych na platformie Microsoft Azure: https:/docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview
2. Przegląd rozwiązań bezpieczeństwa baz danych Azure SQL: https:/docs.microsoft.com/en-us/azure/azure-sql/database/security-overview
3. Najlepsze praktyki szyfrowania danych na platformie Microsoft Azure: https:/docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices
4. Azure Key Vault: https:/docs.microsoft.com/pl-pl/azure/key-vault/general/basic-concepts
5. Azure Key Vault Managed HSM: https:/docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview
6. AWS Key Management Service (KMS): https:/aws.amazon.com/kms/
7. GCP Encryption: https:/cloud.google.com/storage/docs/encryption
8. GCP Key Management: https:/cloud.google.com/security/key-management-deep-dive
9. IBM przegląd aspektów bezpieczeństwa na platformie IBM Cloud https:/www.ibm.com/cloud/architecture/architectures/securityArchitecture/security-for-data
10. IBM Cloud Hyper Protect Services: https:/ibm-hyper-protect.github.io/

Załącznik nr 19

do Standardu PolishCloud 2.0

Monitorowanie

Monitorowanie poprawności działania systemów i aplikacji działających w chmurze publicznej jest istotnym elementem zapewnienia ciągłości ich działania. Monitorowanie może odbywać się na różnych poziomach stosu technologicznego, przy czym istotne jest spojrzenie na ten aspekt w dwóch perspektywach – platformowej oraz aplikacyjnej, które mogą różnić się zakresem odpowiedzialności realizowanych działań przez zaangażowane podmioty (podmiot nadzorowany, dostawca rozwiązania, Dostawca usług przetwarzania w chmurze) oraz zakresem informacji logowanych przez narzędzia do monitorowania. Ze względu na fakt, iż logi mogą również zawierać informacje będące tajemnicą bankową, w ramach analizy wymagań związanych z systemem monitorowania pomocne może być uwzględnienie poniższych pytań.

Lista pytań, jakie Bank powinien sobie zadać w kontekście monitorowania:

1. Jak wyglądać będzie proces zbierania logów związanych z przetwarzaniem informacji w chmurze obliczeniowej?
2. Czy zidentyfikowane zostały wszystkie źródła logów związane z zapewnieniem rozliczalności operacji wykonywanych w chmurze oraz czy została przeprowadzona analiza zakresu logowania, w szczególności w kontekście logowania danych osobowych/danych objętych tajemnicą bankową itp.?
3. Czy zdefiniowano zasady retencji dla logowanych danych oraz ich usuwania?
4. W jaki sposób Bank planuje zabezpieczać logi związane z przetwarzaniem informacji w chmurze obliczeniowej przed nieautoryzowanym dostępem, modyfikacją lub usunięciem, w szczególności logi obejmujące szczególne kategorie danych, jak np. dane osobowe/dane objęte tajemnicą bankową itp.?
5. Czy zostało przeanalizowane i jest planowane wykorzystanie SIEM? Jeśli tak, to jakiego typu (aktualnie stosowany w Banku/on-premise, chmurowy, hybryda)?
6. Czy istnieje możliwość integracji rozwiązania chmurowego z systemem SIEM wykorzystywanym aktualnie przez podmiot nadzorowany?
7. Czy istnieje możliwość monitorowania dostępu użytkowników uprzywilejowanych w ramach usługi chmurowej?
8. Czy proces zarządzania incydentami uwzględnia aspekty chmurowe? Czy zdefiniowano i wdrożono scenariusze monitorowania w oparciu o zdarzenia chmurowe?
9. Jakie zastosowano mierniki (KPI) w zakresie wykrywania i reagowania na incydenty w chmurze?

10. Czy Dostawca chmurowy ma udokumentowany i dostępny dla klienta proces monitorowania dostępności, integralności i poufności w ramach oferowanych usług chmurowych wraz z opisem udostępnianych klientowi metryk?

11. Jaki jest rekomendowany przez Dostawcę model podziału odpowiedzialności w zakresie monitorowania bezpieczeństwa usługi chmurowej?

12. W jaki sposób Dostawca zapewnia rozliczalność operacji wykonywanych przez poszczególnych użytkowników w ramach usług chmurowych, gdzie są one logowane oraz czy istnieje możliwość ich integracji z systemami SIEM klienta?

Źródła:

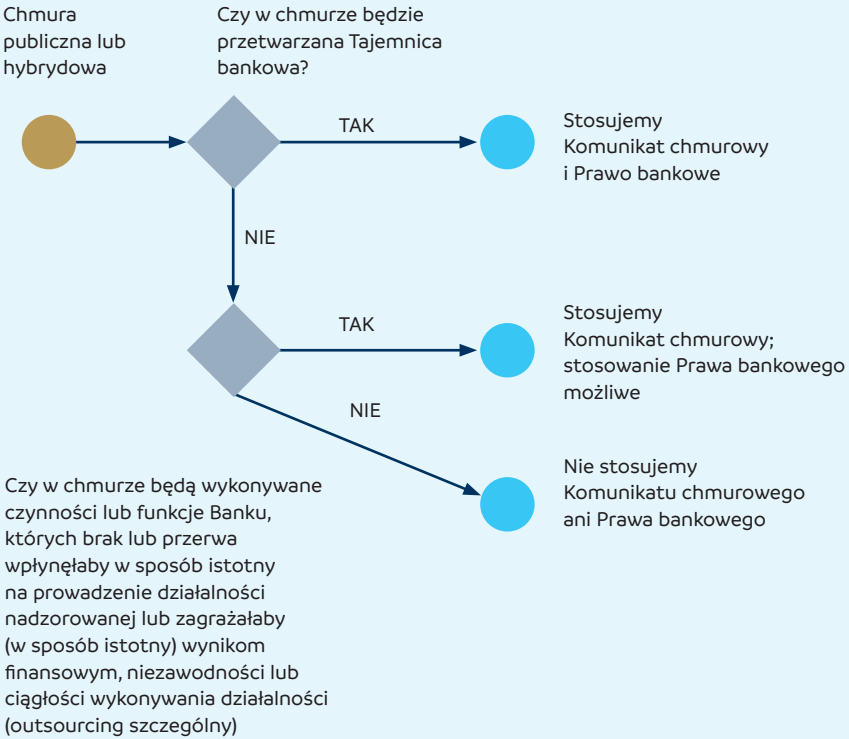
1. Przegląd aspektów monitorowania infrastruktury, danych i aplikacji na platformie IBM Cloud: https:/www.ibm.com/cloud/architecture/architectures/securityArchitecture/security-monitoring-and-intelligence
2. Logowanie zdarzeń na platformie IBM Cloud https:/cloud.ibm.com/docs/Log-Analysis-with-LogDNA?topic=Log-Analysis-with-LogDNA-getting-started
3. Monitorowanie wydajności i stanu aplikacji i usług na platformie IBM Cloud: https:/cloud.ibm.com/docs/Monitoring-with-Sysdig?topic=Monitoring-with-Sysdig-getting-started
4. Wprowadzenie do monitorowania usług na platformie Microsoft Azure: https:/docs.microsoft.com/pl-pl/azure/azure-monitor/overview
5. Analiza logów za pomocą Azure Log Analytics: https:/docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-analytics-overview
6. Monitorowanie bezpieczeństwa infrastruktury w środowisku Microsoft Azure: https:/docs.microsoft.com/en-us/azure/security-center/
7. Azure Sentinel – zaawansowana analiza zdarzeń i logów za pomocą usług SIEM/SOAR w chmurze: https:/docs.microsoft.com/en-us/azure/sentinel/overview
8. Wdrażanie dedykowanych modeli uczenia maszynowego w analizie zdarzeń bezpieczeństwa – Microsoft Sentinel: https:/docs.microsoft.com/en-us/azure/sentinel/bring-your-own-ml

Załącznik nr 20

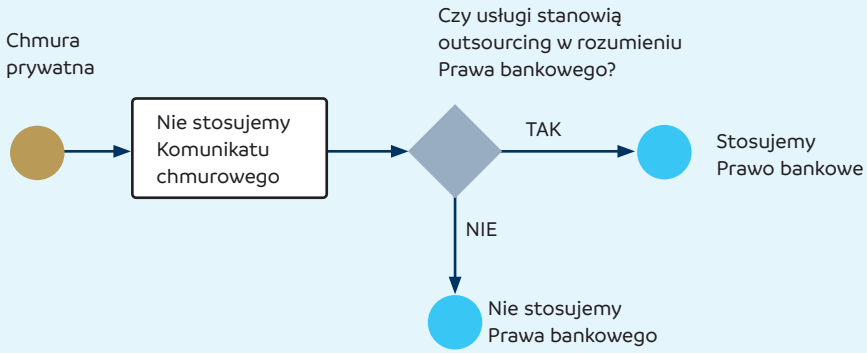
do Standardu PolishCloud 2.0

Graficzny schemat stosowania Komunikatu chmurowego i Prawa bankowego

Graficzny schemat stosowania Komunikatu chmurowego i Prawa bankowego



Publiczna czy prywatna?



Załącznik nr 21

do Standardu PolishCloud 2.0

Propozycja wypełnienia notyfikacji zgodnie z Załącznikiem nr 1 Komunikatu chmurowego

Zamieszone poniżej komentarze należy traktować jako propozycję dodatkowych wyjaśnień, jak informować UKNF o zamiarze przetwarzania w chmurze obliczeniowej publicznej lub hybrydowej.

Oznaczenie podmiotu nadzorowanego (nazwa, adres, NIP, REGON)	BANK S.A., ul. Polska 11/11, 00–001 Warszawa, NIP: 1234567890, REGON: 987654321 **Komentarz:** *W przypadku oddziałów instytucji finansowych rekomendowane jest wskazanie oznaczenia oddziału w Polsce obejmujące dane wskazane powyżej lub ich odpowiednika np. w zakresie NIP lub 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:	Informacje o reklamacjach klientów Banku: dane osobowe klientów, nagrania rozmów na infolinii, decyzje w procesie reklamacyjnym, pisma reklamacyjne i odpowiedzi na nie. **Komentarz:** *Zgodnie z definicjami Komunikatu w I.1.2 rodzaj informacji chronionych można powiązać z ogólnym określeniem, np. tajemnica bankowa, tajemnica ubezpieczeniowa lub agencyjna, bez konieczności szczegółowego wskazywania konkretnych informacji takich jak imię, nazwisko, PESEL, nr karty kredytowej, nr polisy, lub ograniczyć się tylko do przykładowego podania informacji bez ich enumeratywnego wyliczenia.* *W zakresie notyfikowania outsourcingu szczególnego wystarczające jest podanie, że chodzi o outsourcing szczególny z ewentualnym uzupełnieniem, o jakie przykładowo informacje chodzi.* *W przypadku gdy notyfikacja wskazuje na zamiar przetwarzania tajemnicy bankowej lub outsourcing szczególny (rodzaj informacji) i np. dotychczas stokenizowana/animizowana informacja (np. nr karty kredytowej) nie jest już tak zabezpieczona, nie ma potrzeby zgłaszania zmiany notyfikacji, informacje te bowiem zawierają się w pojęciu np. tajemnicy bankowej (rodzaj informacji).*
Nazwa i adres Dostawcy usług chmury obliczeniowej:	Dostawca Chmury S.A., ul. Chmurowa 90, 00-001 Warszawa **Komentarz:** *W przypadku usługi SaaS obejmującej hosting aplikacji na zewnętrznej chmurze obliczeniowej wskazuje się dostawcę usługi SaaS, przy czym z uwagi na sektorowe ryzyko koncentracji należy również podać nazwy głównych dostawców hostingu chmury obliczeniowej (zapewniających przechowywanie danych Banku).*
Nazwy usług chmury obliczeniowej lub ich rodzaj:	Serwery wirtualne, storage, sieci wirtualne, aplikacja CRM **Komentarz:** *Zaproponowany opis usług można uzupełnić o ich nazwy handlowe. Można również wskazać, w jakim modelu są realizowane usługi (np. Aplikacja CRM w modelu SaaS). W przypadku usługi SaaS obejmującej hosting aplikacji na zewnętrznej chmurze obliczeniowej wskazuje się nazwę aplikacji w modelu SaaS.*

Lokalizacje CPD przetwarzanych informacji (państwo, region):	Warszawa, Wrocław, Frankfurt (Niemcy), Dublin (Irlandia) **Komentarz:** *O ile to możliwe, rekomendowane jest podanie w miarę precyzyjnych lokalizacji CPD. Komunikat pozwala na wskazanie w notyfikacji „EOG" jako określenia lokalizacji CPD, przy czym nie wpływa to na wymóg określenia lokalizacji w umowie w sposób bardziej precyzyjny (np. region).*
Data podpisania umowy z Dostawcą usług chmury obliczeniowej lub przewidywany termin jej zawarcia:	10.2020 – przewidywany termin zawarcia umowy **Komentarz:** *Należy wskazać datę umowy, której podpisanie wiąże się dla Banku z korzystaniem z chmury obliczeniowej. Nie wskazuje się daty podpisania umowy pomiędzy dostawcą aplikacji w modelu SaaS a jego poddostawcą w zakresie hostingu.*
Okres, na jaki została zawarta umowa z Dostawcą usług chmury obliczeniowej:	Na okres 3 lat od daty zawarcia umowy. **Komentarz:** *Odpowiednio stosujemy uwagi jak powyżej.*
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 **Komentarz:** *Tam, gdzie jest to możliwe, podajemy służbowy 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.

Warszawa, 01.08.2020	Członek Zarządu Banku	Prokurent Banku
_____	_____	_____
Miejscowość, data	Podpisy osób reprezentujących podmiot nadzorowany	

kochański & partners Business Law Firm

DODATEK

Opinia w przedmiocie kwalifikacji prawnej korzystania z chmury obliczeniowej przez partnerów Banku

8 września 2021 r.

DO:

Związek Banków Polskich

OD:

Kochański & Partners Spółka Komandytowa

r.pr. Szymon Ciach
s.ciach@kochanski.pl

1. ZAKRES I CELE OPINII

1.1. Niniejsza opinia prawna („**Opinia**") została przygotowana przez kancelarię prawną Kochański & Partners sp.k. z siedzibą w Warszawie („**Kancelaria**") na zlecenie Związku Banków Polskich z siedzibą w Warszawie („**Klient**" lub „**ZBP**").

1.2. Klient zlecił Kancelarii przeprowadzenie analizy prawnej w przedmiocie istnienia obowiązku stosowania Komunikatu Chmurowego w sytuacji, gdy bank krajowy, który podlega obowiązkowi stosowania Komunikatu Chmurowego („**Bank**"), korzysta z usług podmiotu zewnętrznego (np. pośrednika kredytu hipotecznego, biura tłumaczeń, agencji marketingowej, firmy windykacyjnej, biegłego audytora – „**Partner**"), który to podmiot:

a) w swojej działalności wykorzystuje chmurę obliczeniową, jednakże nie jest ona wykorzystywana do realizacji głównego przedmiotu powierzenia (usługi świadczonej dla Banku)[1],

b) realizuje usługi na rzecz Banku w jednym z dwóch wariantów: w charakterze outsourcingu uregulowanego w rozumieniu art. 6a–6d Prawa bankowego („**outsourcing regulowany**"), jak i w sposób nie kwalifikujący się jako outsourcing regulowany.

1.3. W ramach współpracy z Partnerem (w obu wariantach) może dochodzić do sytuacji, gdy Partner ma dostęp do informacji objętych tajemnicą bankową w rozumieniu art. 104 ust. 1 Prawa bankowego, a także przetwarza tego typu informacje w ramach usług chmury obliczeniowej, z której korzysta.

1.4. Opinia obejmuje w szczególności analizę przepisów Prawa bankowego oraz postanowień Komunikatu Chmurowego (w tym uzupełnień w ramach opublikowanych Q&A), a także pomocniczo innych aktów prawnych, w odniesieniu do powyższego zagadnienia. Opinia ma na celu udzielenie odpowiedzi na poniższe pytania:

a) Pytanie 1. Czy Bank ma obowiązek weryfikować spełnienie wymogów Komunikatu Chmurowego w sytuacji, gdy współpracuje z Partnerem w ramach outsourcingu regulowanego, który korzysta z usługi chmury obliczeniowej?

b) Pytanie 2. Czy Bank ma obowiązek weryfikować spełnienie wymogów Komunikatu Chmurowego w sytuacji, gdy współpracuje z Partnerem poza outsourcingiem regulowanym, który korzysta z usługi chmury obliczeniowej?

c) Pytanie 3. Czy kwestia dostępu do danych objętych tajemnicą bankową przez Dostawcę usługi chmury obliczeniowej ma wpływ na obowiązek stosowania Komunikatu Chmurowego w określonych wyżej sytuacjach?

d) Pytanie 4. Jaka jest podstawa prawna obowiązku samodzielnego stosowania Komunikatu Chmurowego w przypadku pośredników kredytu hipotecznego jako podmiotów nadzorowanych w rozumieniu Ustawy o nadzorze?

1.5. Opinia swoim zakresem obejmuje następujące akty prawne i stanowiska organów nadzoru:

a) Ustawa z 29 sierpnia 1997 r. Prawo bankowe („**Prawo bankowe**") (Dz. U. z 2020 r. poz. 1898 z późń. zm.);

1 Przykładem może być usługa chmury obliczeniowej o funkcjonalności poczty e-mail, w modelu SaaS lub też usługa przechowywania danych w chmurze (np. wirtualny dysk w modelu SaaS).

b) Ustawa z 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2020 r. poz. 2059 z późn. zm.). („**Ustawa o nadzorze**");

c) Ustawa z 23 marca 2017 r. o kredycie hipotecznym oraz o nadzorze nad pośrednikami kredytu hipotecznego i agentami (Dz. U. z 2020 r. poz. 1027 z późn. zm.) („**Ustawa o kredycie hipotecznym**");

d) Rekomendacja D Komisji Nadzoru Finansowego dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach ze stycznia 2013 r. („**Rekomendacja D**");

e) Rekomendacja M Komisji Nadzoru Finansowego dotycząca zarządzania ryzykiem operacyjnym w bankach ze stycznia 2013 r. („**Rekomendacja M**");

f) Wytyczne EBA w sprawie outsourcingu z 25 lutego 2019 r. („**Wytyczne EBA**");

g) Stanowisko UKNF z 16 września 2019 r. dotyczące wybranych zagadnień związanych z wejściem w życie Wytycznych EBA w sprawie outsourcingu i ich uwzględnianiem w działalności banków („**Stanowisko ws. Wytycznych EBA**");

h) Komunikat Urzędu Komisji Nadzoru Finansowego z 23 stycznia 2020 r., ze zmianami, dotyczącym przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej („**Komunikat Chmurowy**");

i) Pytania i odpowiedzi (Q&A) UKNF w zakresie stosowania Komunikatu UKNF z 23 stycznia 2020 r. dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z dnia 17.12.2020 r. oraz z dnia 25.03.2021 r. („**Q&A**").

1.6. Opinia nie obejmuje szczegółowej analizy regulacji w zakresie banków spółdzielczych, SKOK, banków zagranicznych, instytucji kredytowych, agentów ubezpieczeniowych, a także innych przepisów sektorowych w zakresie informacji prawnie chronionych (tajemnic prawnie chronionych innych niż określone w prawie bankowym, w tym w zakresie tajemnicy ubezpieczeniowej przetwarzanej przez banki). Na potrzeby Opinii poprzez „informacje prawnie chronione" rozumie się wyłącznie tajemnicę bankową opisaną art. 104 ust. 1 Prawa bankowego, chyba że wyraźnie wskazano inaczej.

2. WPROWADZENIE DO ZAGADNIENIA

2.1. Na tle wytycznych stosowania Komunikatu Chmurowego, opisanych w pkt. IV Komunikatu Chmurowego oraz rozwiniętych w ramach Q&A, powstała istotna wątpliwość, czy Bank ma obowiązek stosować postanowienia Komunikatu Chmurowego za każdym razem, gdy poweźmie wiadomość, że jego Partner wykorzystuje lub zamierza wykorzystywać usługi chmury obliczeniowej w swej działalności. W szczególności wątpliwość dotyczy tego, czy sama okoliczność przetwarzania informacji prawnie chronionych w usłudze chmury obliczeniowej (nawet jeśli na własne potrzeby Partnera) stanowi już o obowiązku stosowania Komunikatu Chmurowego, a jeśli tak, to który z podmiotów powinien weryfikować zgodność przetwarzania z wymogami Komunikatu Chmurowego.

2.2. Jak wspominano powyżej, typowym przykładem takiej sytuacji może być wykorzystanie usług poczty lub przechowywania dokumentów „w chmurze" przez Partnera. Usługa poczty w modelu SaaS (Software as a Service) różni się od tradycyjnej poczty (on-premise) przede wszystkim tym, że poczta elektroniczna hosto-

wana jest w chmurze obliczeniowej, co oznacza, że obsługa ruchu wiadomości, a także przetwarzanie i przechowywanie ich treści, odbywa się typowo na serwerach dostawcy oprogramowania poczty. Funkcjonalność poczty jest najczęściej zintegrowana z pozostałymi usługami pakietu biurowego (np. edycją dokumentów). Pozwala to korzystać z usług za pośrednictwem przeglądarki internetowej w połączeniu z możliwością zdalnej wymiany i edycji dokumentów w trybie on-line.

2.3. Wątpliwości pojawiły się przede wszystkim w związku z matrycą stosowania zawartą w pkt. IV.4. Komunikatu Chmurowego:

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.	

2.4. Znalazły one swój wyraz również w pytaniach kierowanych do UKNF, na które UKNF odpowiedział w ramach Q&A:

Nb. 1 [2] Stosowanie Komunikatu w relacji pomiędzy zakładem ubezpieczeń a agentami ubezpieczeniowymi, zakładami reasekuracji, brokerami ubezpieczeniowymi.

Zakład ubezpieczeń stosuje Komunikat w relacjach z multiagentami oraz agentami wyłącznymi w zakresie, w jakim podmioty te wykonują na rzecz zakładu ubezpieczeń proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez zakład ubezpieczeń oraz:

1. przetwarzanie informacji w chmurze obliczeniowej publicznej lub hybrydowej ma charakter outsourcingu szczególnego, lub
2. przetwarzanie w chmurze obliczeniowej publicznej lub hybrydowej dotyczy informacji prawnie chronionych (outsourcing chmury obliczeniowej inny niż szczególny).

Podmioty te, jako podmioty nadzorowane, stosują Komunikat, gdy korzystają z chmury obliczeniowej publicznej lub hybrydowej, a przetwarzanie informacji, w ramach tych chmur obliczeniowych, ma charakter outsourcingu szczególnego lub dotyczy informacji prawnie chronionych.

Zakład ubezpieczeń nie stosuje Komunikatu w relacjach z zakładami reasekuracji i brokerami ubezpieczeniowymi, ponieważ wskazane podmioty samodzielnie realizują czynności w ramach prowadzonej przez siebie działalności gospodarczej. Podmioty te, jako podmioty nadzorowane, stosują Komunikat, gdy korzystają z chmury obliczeniowej publicznej lub hybrydowej, a przetwarzanie informacji, w ramach tych chmur obliczeniowych, ma charakter outsourcingu szczególnego lub dotyczy informacji prawnie chronionych.

2 Numery boczne nadane przez autora.

Nb.2 Czy podmiot nadzorowany powinien notyfikować zamierzone przetwarzanie danych w chmurze obliczeniowej jeżeli korzysta z chmury obliczeniowej za pośrednictwem innego podmiotu nadzorowanego? Notyfikacja w przypadku relacji podmiot nadzorowany – podmiot nadzorowany.	W przypadku współpracy podmiotu nadzorowanego z innym podmiotem nadzorowanym, podmiot ten nie ma obowiązku dokonywania oddzielnych notyfikacji uwzględniających korzystanie z chmury przez podmiot nadzorowany, któremu powierzono przetwarzanie, jeżeli korzystanie z chmury jest jego autonomiczną decyzją. Przykładowo w relacji zakład ubezpieczeń – agent ubezpieczeniowy, jeżeli ten drugi autonomicznie korzysta z usług chmurowych (niedostarczonych przez zakład ubezpieczeń), to zakład ubezpieczeń nie ma obowiązku notyfikowania korzystania z chmury i tylko agent ubezpieczeniowy notyfikuje UKNF korzystanie z chmury. Jeżeli natomiast podmiot nadzorowany korzysta z usługi chmurowej dostarczonej przez inny podmiot nadzorowany i wykorzystuje ją do wykonywania czynności na rzecz tego podmiotu, to obydwa podmioty dokonują oddzielnych notyfikacji. Przykładowo w relacji zakład ubezpieczeń – agent ubezpieczeniowy, jeżeli ten drugi korzysta z usługi chmurowej dostarczanej przez zakład ubezpieczeń, to zarówno zakład (niezależnie od tego, z iloma agentami współpracuje), jak i agent dokonują oddzielnych notyfikacji we własnym zakresie wykorzystywania chmury. Każdy podmiot nadzorowany prowadzi ewidencję umów outsourcingu, której obowiązek prowadzenia dotyczy również umów z dostawcą usługi chmury obliczeniowej. Ewidencja ta jest prowadzona zgodnie z obowiązującymi dany podmiot przepisami. UKNF zaleca, aby ewidencja w zakresie usług chmury obliczeniowej uwzględniała również informacje wymienione w Załączniku Nr 1 do Komunikatu.

2.5. Powyższe stanowiska wyrażone w Q&A odnoszą się wyłącznie do relacji zakład ubezpieczeń – broker/agent ubezpieczeniowy, w sytuacji gdy oba podmioty są podmiotami nadzorowanymi. Podobne wątpliwości, jak te wyrażone w zadanym pytaniu, można mieć jednakże również do współpracy banków z Partnerami w charakterze pośredników kredytu hipotecznego, którzy też są „podmiotami nadzorowanymi" w rozumieniu Ustawy o nadzorze. Q&A nie rozwiewają istniejących na tym tle wątpliwości, dają jednakże pewne kierunkowe wskazówki. W szczególności, jako istotna dla obowiązku notyfikacji zgodnie z Komunikatem Chmurowym, wskazana została okoliczność, czy korzystanie z chmury odbywa się w sposób autonomiczny, czy też funkcjonalnie związany z usługą powierzoną przez podmiot nadzorowany, a równolegle czy dochodzi do przetwarzania informacji prawnie chronionych w chmurze. Wydaje się, że w zaprezentowanym w Q&A stanowisku nieco rozdzielono obowiązek notyfikacji od samego obowiązku stosowania Komunikatu Chmurowego, gdy w istocie pierwszy obowiązek wynika z drugiego. Konieczna jest więc analiza rzeczywistej matrycy stosowania Komunikatu. O ile szczegółowe wnioski dla danej sytuacji wymagają analizy konkretnej grupy przypadków, na potrzeby Opinii analizowane są zagadnienia o charakterze zasadniczym. Z podjętej w Opinii analizy prawnej wynika, że możliwe są różne scenariusze działania banków, natomiast fundamentalna kwestia dotyczy raczej nie tego, czy rozwiązania chmury obliczeniowej są bezpieczne, lecz czy dopuścić można (jeśli tak, to w jakim zakresie) do sytuacji, gdy dostawcy chmury obliczeniowej dla Partnerów mają dostęp do danych przetwarzanych przez Partnerów, w tym danych objętych tajemnicą bankową. Z tego względu pominięto szczegółową analizę prawną w odniesieniu do poszczególnych grup Partnerów (np. agenci ubezpieczeniowi, pośrednicy, brokerzy ubezpieczeniowi), skupiając się na podstawnym rozróżnieniu Partnerów współpracujących z bankiem: Partnerów w ramach outsourcingu regulowanego i Partnerów spoza outsourcingu regulowanego. Całościowy obraz analizowanych zagadnień prawnych ukazany został w formie graficznej w Schemacie stanowiącym ZAŁĄCZNIK NR 1 – SCHEMAT do Opinii.

3. ANALIZA PRAWNA

Nadzór KNF

3.1. Zgodnie z podstawową dla działania organów administracji publicznej zasadą legalizmu organy władzy publicznej działają na podstawie i w granicach prawa (art. 7 Konstytucji RP). Nadzór nad sektorem bankowym sprawowany jest przez Komisję Nadzoru Finansowego („**KNF**") zgodnie z Ustawą o nadzorze, która w swoim art. 1. ust. 2. pkt. 1 stanowi, że nadzór nad rynkiem finansowym obejmuje nadzór bankowy, sprawowany zgodnie z przepisami Prawa bankowego, ustawy z 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz. U. z 2020 r. poz. 2027 z późn. zm.), ustawy z dnia 7 grudnia 2000 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających (Dz. U. z 2021 r. poz. 102 z późn. zm.) oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniającego rozporządzenie (UE) nr 648/2012 (Dz. Urz. UE L 176 z 27.06.2013, str. 1, z późn. zm.).

3.2. Celem przytoczenia powyższych przepisów jest wskazanie, że zakres nadzoru w zakresie outsourcingu, a co za tym idzie, wymagania nakładane na podmioty nadzorowane, powinien znajdować swoje źródło w przepisach powszechnie obowiązującego prawa.

Podstawy prawne aktów regulacyjnych nadzoru (*soft law* outsourcingu)

3.3. Prawo bankowe reguluje obszar outsourcingu jako czynności powierzone przez banki podmiotom zewnętrznym – są to czynności bankowe (określone w art. 5 i art. 6 Prawa bankowego) oraz czynności faktyczne związane z działalnością bankową. Czynności faktyczne nie są wymienione wprost w Prawie bankowym, jednak do kwalifikacji poszczególnych czynności faktycznych jako podlegających outsourcingowi bankowemu w praktyce bankowej, w ślad za stanowiskiem Generalnego Inspektoratu Nadzoru Bankowego („**GINB**") z 2004 r.[3], przyjmuje się najczęściej następujące kryteria:

a) dostęp Partnera do tajemnicy bankowej;

b) związek powierzonej czynności z działalnością bankową, rozumiany w szczególności jako istotny element procesu realizowanego przez Bank w obszarze działalności nadzorowanej;

c) znaczenie czynności powierzonych Partnerowi dla krytycznych procesów bankowych.

3.4. Outsourcing jest zatem zagadnieniem uregulowanym odpowiednimi przepisami Prawa bankowego. UKNF jako organ nadzoru, a także Europejski Urząd Nadzoru Bankowego („**EBA**") jako unijny organ nadzoru, niejednokrotnie przedstawiały swoją interpretację oraz oczekiwania w zakresie stosowania przepisów outsourcingu w celu ograniczenia ryzyk wynikających z outsourcingu wykorzystywanego przez podmioty nadzorowane.

3.5. W kontekście outsourcingu funkcji IT regulacje tzw. *soft law*, czyli aktów organu nadzoru, pojawiały się już w Rekomendacji D, która w pkt. 10 wymaga od Banku, aby posiadał sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych, zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego, uwzględniające również usługi świadczone przez podmioty należące do grupy kapitałowej Banku.

3 Pismo z dnia 21 grudnia 2004 r. Narodowy Bank Polski NB-BPN-I-022-70/04.

3.6. W związku ze szczególnym znaczeniem outsourcingu usług chmury obliczeniowej, UNKF opublikował komunikat z 23 października 2017 r. dotyczący „korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej".

3.7. EBA w Wytycznych z 25 lutego 2019 r. w sprawie outsourcingu uregulowała swoje oczekiwania w tym obszarze, uwzględniając w nich również zagadnienie outsourcingu chmury obliczeniowej.

3.8. UKNF przyjął Wytyczne EBA jako obowiązujące w polskim sektorze bankowym, z pewnymi wyłączeniami. UKNF w pkt. 47 Stanowiska ws. Wytycznych EBA zaznaczył bowiem, że w odniesieniu do części poświęconej outsourcingowi w chmurze obliczeniowej stosowane będzie podejście krajowe.

3.9. W konsekwencji, 23 stycznia 2020 r. opublikowano aktualny Komunikat Chmurowy, który zastąpił komunikat z października 2017 r. W odpowiedzi na wątpliwości wynikające z Komunikatu Chmurowego, UNKF na swojej stronie internetowej publikuje również pytania i odpowiedzi (Q&A) zawierające wskazówki interpretacyjne dla postanowień Komunikatu oraz jego doprecyzowania.

3.10. Biorąc pod uwagę zasadę legalizmu, cel istnienia przepisów outsourcingowych, rozwój technologii informatycznych oraz chronologię publikowanych aktów nadzorczych, w naszej ocenie nie ulega wątpliwości, że podstawą dla stosowania wymogów Komunikatu Chmurowego wobec podmiotów nadzorowanych (w tym banków), powinno być wykorzystanie chmury obliczeniowej w sposób nadający temu korzystaniu charakter outsourcingu chmury obliczeniowej. Innymi słowy, dla stosowania wymogów outsourcingu, korzystanie z chmury przez Bank bezpośrednio lub poprzez Partnera powinno mieć charakter właśnie powierzenia (bądź podpowierzenia) wykonywania tych czynności, tj. wykonywania ich na polecenie i na korzyść Banku, a nie samodzielnie na własne potrzeby Partnera. Cecha ta znajduje odzwierciedlenie zarówno w rozumieniu outsourcingu przedstawianym przez organy nadzoru (np. w definicji „outsourcingu" zawartej w Wytycznych EBA, definicji „outsourcingu chmury obliczeniowej" zawartej w Komunikacie Chmurowym[4]), jak i w art. 6a. Prawa bankowego. Dodatkowo we wskazanych definicjach z Wytycznych EBA oraz Komunikatu Chmurowego pojawia się inna istotna cecha outsourcingu, tj. polecenie wykonywania „typowych" czynności – wedle kryterium, czy powierzona czynność byłaby realizowana samodzielnie, gdyby usługa chmury obliczeniowej była niedostępna.

Outsourcing jako podstawa do stosowania Komunikatu Chmurowego

3.11. Zgodnie z przytoczoną wyżej matrycą stosowania Komunikatu Chmurowego oba przypadki zastosowania w niej opisane, w naszej ocenie, odnoszą się do sytuacji, gdy zachodzi outsourcing chmury obliczeniowej (jak wskazuje nagłówek w tabeli tejże matrycy). Podmioty nadzorowane, w tym banki, mają więc obowiązek stosować Komunikat w dwóch przypadkach:

a) w sytuacji gdy w chmurze obliczeniowej są przetwarzane informacje prawnie chronione (dla banków w szczególności te objęte tajemnicą bankową) i odbywa się to w ramach outsourcingu chmury obliczeniowej innego niż szczególny; lub

4 „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.

b) w sytuacji gdy chmura obliczeniowa jest wykorzystywana w modelu outsourcingu chmury obliczeniowej o cechach outsourcingu szczególnego. W tej sytuacji przesłanka przetwarzania informacji prawnie chronionych w chmurze jest wtórna, gdyż sam szczególny wpływ outsourcingu na działalność nadzorowaną Banku jest podstawą do stosowania Komunikatu Chmurowego.

3.12. Należy więc zwrócić uwagę, że punktem wyjścia dla określenia, czy występuje obowiązek stosowania Komunikatu Chmurowego jest za każdym razem stwierdzenie, że dochodzi do outsourcingu chmury obliczeniowej. Musi zatem istnieć związek pomiędzy usługą chmury obliczeniowej a poleceniem wykonywania tej usługi (powierzeniem) na rzecz i w imieniu Banku (czy też trafniej: „na polecenie i na korzyść Banku").

3.13. Powyższe rozumienie można również odnaleźć w pkt. II.1. Komunikatu Chmurowego, zgodnie z którym „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". Ponadto, zgodnie z pkt. II.3 Komunikatu Chmurowego "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".

3.14. W pkt. VI. 2.7. Komunikatu Chmurowego UKNF wskazuje również, że Bank powinien uwzględnić w szacowaniu ryzyka: „stanowisko w sprawie usług (dostawców usług chmury obliczeniowej), które są wykorzystywane do świadczenia własnych usług przez bezpośrednich dostawców podmiotów nadzorowanych, zgodnie z którym:

a) podmiot nadzorowany powinien upewnić się, w jakim zakresie świadczona przez bezpośredniego dostawcę usługa wykorzystuje usługi chmury obliczeniowej, a w szczególności czy dochodzi do przetwarzania informacji prawnie chronionej w usłudze chmury obliczeniowej;

b) zależnie od faktycznego wykorzystania usług chmury obliczeniowej oraz zakresu przetwarzanych informacji podmiot nadzorowany powinien zapewnić, że przetwarzanie informacji jest realizowane z uwzględnieniem postanowień niniejszego komunikatu".

3.15. Należy zauważyć, że w cytowanym wyżej pkt. VI.2.7. b UKNF odnosi się do okoliczności „faktycznego wykorzystania". Biorąc pod uwagę domniemany cel Komunikatu Chmurowego, za bezpośredniego dostawcę (VI.2.7 Komunikatu) należy rozumieć dostawcę IT/dostawcę SaaS, a nie przedsiębiorcę (Partnera), który akcesoryjnie/pomocniczo korzysta ze standardowych rozwiązań chmurowych takich jak poczta/edytor tekstu/kalendarza spotkań. Zbieżne z tym podejściem wydaje się również wskazanie w cytowanych wyżej Q&A autonomiczności wykorzystania chmury jako okoliczności istotnej dla oceny obowiązku notyfikacji korzystania z chmury obliczeniowej (a jak można z tego wywnioskować – również samego obowiązku stosowania Komunikatu Chmurowego).

3.16. W dalszej części Opinii zagadnienie autonomiczności jest szerzej poruszone. Z powyższego wynika natomiast, że celem Komunikatu Chmurowego jest w szczególności za-

prezentowanie rozumienia przez UKNF przepisów Prawa bankowego w zakresie outsourcingu, co koresponduje mocno ze stwierdzeniem, że to właśnie zakwalifikowanie danej współpracy jako mającej charakter outsourcingu chmury obliczeniowej jest podstawą do stosowania wymogów Komunikatu Chmurowego.

Outsourcing chmury obliczeniowej a outsourcing regulowany i tajemnica bankowa

3.17. Jak wskazano powyżej, obowiązek stosowania Komunikatu Chmurowego powinien mieć swoje zaczepienie w relacji outsourcingu (lub odpowiednio podoutsourcingu) chmury obliczeniowej, która dla pewnych kategorii podmiotów nadzorowanych może łączyć się z obowiązkiem spełnienia ustawowych warunków outsourcingu regulowanego. Będzie tak w szczególności w sytuacji, gdy outsourcing chmury obliczeniowej będzie się kwalifikował jako outsourcing regulowany. Na tym tle pojawia się zagadnienie, czy podmiot nadzorowany, który nie podlega bezpośrednio regulacjom outsourcingu, powinien być zobowiązany do samodzielnego stosowania Komunikatu. Pytanie to wynika z faktu, że „podmioty nadzorowane" objęte Komunikatem Chmurowym to bardzo szerokie pojęcie, obejmujące również takie podmioty jak np. spółki publiczne, tj. notowane na rynku regulowanym, które same z siebie nie są regulowane w zakresie outsourcingu. Należy więc zbadać, w jakich sytuacjach stosowanie Komunikatu Chmurowego w oderwaniu od przepisów outsourcingowych jest zasadne z perspektywy nadzoru nad rynkiem finansowym. Szczegółowe omówienie tego aspektu na przykładzie pośredników kredytu hipotecznego i spółek publicznych znajduje się w pkt. 3.58 Opinii, natomiast na tym etapie warto je zasygnalizować, gdyż dobrze obrazuje ono rozbieżność wymogów Komunikatu Chmurowego względem outsourcingu regulowanego oraz przepisów o tajemnicy bankowej.

3.18. W kontekście przedmiotu Opinii i analizowanego zagadnienia wykorzystania chmury obliczeniowej przez Partnera jedno z podstawowych pytań dotyczy tego, w jakich okolicznościach korzystanie z chmury przez Partnera może być traktowane jako podoutsourcing regulowany na gruncie prawa bankowego, a w jakich będzie to stanowić podstawę do stosowania Komunikatu Chmurowego. Zakwalifikowanie wykorzystania jako ewentualny outsourcing lub podoutsourcing regulowany „uruchomi" dodatkowo zagadnienia związane z podoutsourcingiem łańcuchowym. Powyższa problematyka wiąże się ściśle z regulacjami dostępu do tajemnicy bankowej, których kształt jest najpoważniejszym argumentem dla przyjęcia dominującej obecnie koncepcji zakazu podoutsourcingu łańcuchowego. Wydaje się natomiast, że jednym ze źródeł problemów interpretacyjnych co do stosowania Komunikatu jest rozszerzenie kwestii dostępu do danych objętych tajemnicą na aspekt przetwarzania informacji prawnie chronionych, a jednoczesne powiązanie tego z kwalifikacją outsourcingu.

3.19. Należy więc wyraźnie zaznaczyć, że z perspektywy prawnej ochrona tajemnicy bankowej oraz katalog okoliczności zezwalających na jej ujawnienie jest zupełnie odrębnym zagadnieniem od tego, czy współpraca Banku z Partnerem ma charakter outsourcingu regulowanego lub outsourcingu chmury obliczeniowej. „Przetwarzanie" informacji prawnie chronionych nie jest pojęciem tożsamym z „ujawnieniem" informacji prawnie chronionych w postaci tajemnicy bankowej, która to sytuacja jest zasadniczo regulowana przepisami Prawa bankowego. Przepisy o tajemnicy bankowej nie regulują zagadnienia przetwarzania informacji nią objętych w takim duchu, w jakim robi to RODO

w odniesieniu do danych osobowych, tj. w rozumieniu „przetwarzania" jako dowolnych operacji na danych, nie tylko operacji ujawnienia. Przepisy dotyczące tajemnicy bankowej mają za zasadnicze zadanie zapewnić poufność informacji objętych tajemnicą (z wszelkimi wyjątkami od tej zasady), a przy tym narzucają pewne ograniczenia co do zakresu możliwego przetwarzania[5]. W tym drugim przypadku czynią to jednakże wybiórczo, a nie w sposób generalny odnoszący się do „przetwarzania".

3.20. Istnieją zatem wątpliwości, czy oczekiwanie UKNF co do stosowania Komunikatu Chmurowego w oparciu o okoliczność przetwarzania informacji prawnie chronionych w chmurze nie narzuca podmiotom nadzorowanym wymogów wykraczających poza zakres nadzoru przewidziany w bezwzględnie obowiązujących przepisach prawa. Przepisy prawa bankowego nigdzie nie przewidują bowiem, aby przetwarzanie tajemnicy bankowej było równoznaczne ze współpracą o charakterze outsourcingu. O ile z perspektywy organu nadzoru można wskazać pewne racje przemawiające za takim podejściem (chęć ochrony danych objętych tajemnicą w obliczu wykładniczo rosnącego wolumenu i sposobów przetwarzania danych), tak dla praktyki bankowej oraz porządku prawnego takie podejście wprowadza wiele niepewności.

3.21. Prawo bankowe reguluje zagadnienie tajemnicy bankowej, której zakres przedmiotowy określony jest w art. 104 ust. 1 Prawa bankowego. Obejmuje ona wszystkie informacje dotyczące czynności bankowej uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której Bank tę czynność wykonuje. Ten sam przepis określa zakres podmiotowy tajemnicy. Obowiązek zachowania tajemnicy bankowej dotyczy: (i) Banku, (ii) osób w nim zatrudnionych oraz (iii) osób, za których pośrednictwem Bank wykonuje czynności bankowe. Z perspektywy analizowanych zagadnień kluczowa jest ta ostatnia kategoria osób. Budzi ona wątpliwości interpretacyjne w związku z dodanym później wyjątkiem od obowiązku zachowania tajemnicy, opisanym w art. 104 ust. 2 pkt. 2 lit. a–b Prawa bankowego. Zgodnie z tym ostatnim przepisem obowiązek zachowania tajemnicy bankowej nie dotyczy określonych przepisami sytuacji, takich jak ujawnienie informacji objętych tajemnicą bankową przedsiębiorcom lub przedsiębiorcom zagranicznym, którym, zgodnie z art. 6a ust. 1 i art. 6b–6d Prawa bankowego, Bank powierzył wykonywanie, stale lub okresowo, czynności związanych z działalnością bankową lub którym powierzono wykonywanie czynności zgodnie z art. 6a ust. 7. Prawa bankowego, w zakresie niezbędnym do należytego wykonywania tych czynności.

3.22. Poprzez cytowany wyżej art. 104 ust. 2 pkt 2) lit. a-b Prawa bankowego przejawia się związek pomiędzy regulacjami dotyczącymi outsourcingu i przepisami o tajemnicy bankowej.

3.23. W praktyce bankowej, w ślad za przywołanym wyżej stanowiskiem GINB z 2004 r., można spotkać się z założeniem, że dostęp do tajemnicy bankowej jest zasadniczą przesłanką dla zaistnienia outsourcingu bankowego. Warto jednakże zwrócić uwagę na poniższy fragment tegoż stanowiska:

> „Do kategorii czynności faktycznych związanych z działalnością bankową należy, w opinii GINB, zaliczyć przede wszystkim wykonywanie na zlecenie Banku czynności, z którymi wiąże się dostęp wykonawcy do informacji „wrażliwych" z punktu widze-

5 Por. zagadnienia związane z przetwarzaniem tajemnicy na potrzeby zautomatyzowanego podejmowania decyzji biznesowych przez bank – art. 105a Prawa bankowego.

nia prowadzonej działalności bankowej, w szczególności do wiadomości na temat klientów banków, w tym objętych tajemnicą bankową. Kryterium ujawniania przedsiębiorcy lub przedsiębiorcy zagranicznemu tego rodzaju informacji nie powinno być jednak w omawianym przypadku traktowane jako jedyne podczas rozstrzygania, czy powierzenie przez Bank określonych czynności jest przedmiotem regulacji art. 6a–6d Prawa bankowego".

3.24. GINB wskazuje, że dostęp do tajemnicy jest kryterium kwalifikacji współpracy jako outsourcingu regulowanego, jednakże należy to odnosić do wykonywania na zlecenie Banku czynności, z którymi wiąże się dostęp wykonawcy do takich informacji[6]. Nie należy z tego wywodzić, że jakikolwiek dostęp podmiotu zewnętrznego (Partnera) do danych objętych tajemnicą, będzie automatycznie kwalifikował daną relację jako outsourcing regulowany. Również w literaturze prawniczej słusznie podnosi się, że kryterium dostępu do tajemnicy bankowej nie jest bezwzględnie przesądzające o kwalifikacji outsourcingu regulowanego z art. 6a. Prawa bankowego[7]. Należy zatem zaznaczyć tę odrębność w kontekście podejścia do regulacji korzystania z chmury obliczeniowej. Skoro dostęp do danych objętych tajemnicą bankową nie stanowi bezwzględnej przesłanki o uznaniu danej współpracy za outsourcing regulowany, tym bardziej nie powinno jej stanowić „przetwarzanie" takich informacji, które z definicji jest pojęciem szerszym.

3.25. Bezsporne jest, że dostęp do informacji objętych tajemnicą bankową dla podmiotu zewnętrznego może występować też na innej podstawie prawnej, niż outsourcing regulowany. Przykładem może być chociażby współpraca Banku z biegłym rewidentem, który ma prawo żądać dostępu do danych objętych tajemnicą zgodnie z art. 105 ust.1 pkt 2) lit. i) Prawa bankowego. Jako „Partner" działa na zlecenie Banku, natomiast nie jest to współpraca w charakterze outsourcingu, pomimo że występuje dostęp do danych objętych tajemnicą bankową. Biegły rewident zobowiązany jest przy tym do zachowania tajemnicy zawodowej na podstawie odrębnych przepisów o tajemnicy biegłego rewidenta[8].

3.26. Tajemnica bankowa może być ponadto ujawniona podmiotom trzecim na podstawie zgody beneficjenta tajemnicy. Art. 104 ust. 3 Prawa bankowego przewiduje bowiem możliwość ujawnienia informacji podmiotom trzecim, z zastrzeżeniem art. 105, art. 106a i art. 106b Prawa bankowego, wyłącznie gdy osoba, której informacje te dotyczą, na piśmie upoważni Bank do przekazania określonych informacji wskazanej przez siebie osobie lub jednostce organizacyjnej. Upoważnienie może być także wyrażone w postaci elektronicznej.

3.27. Kwalifikacja współpracy jako outsourcingu regulowanego jest zatem zasadniczo niezależna od obowiązku stosowania Komunikatu Chmurowego i od podstawy prawnej ujawnienia tajemnicy bankowej.

3.28. Wobec powyższego zagadnienia w dalszej części Opinii dokonano próby systemowego przedstawienia zagadnień outsourcingu chmury obliczeniowej, outsourcingu regu-

6 W kontekście oceny, czy występują czynności faktyczne opisane art. 6a ust. 1 pkt 2 Prawa bankowego rozważenia wymaga również istotność poszczególnych danych w kontekście uznania ich za tajemnicę bankową oraz szerszy kontekst, a mianowicie: w jakim procesie i jakim celu są one wykorzystywane.

7 Zob. T. Czech, *Ujawnienie tajemnicy prawnie chronionej jako przesłanka outsourcingu bankowego*, M.Pr.Bank. 2012, nr 10, s. 80-89.

8 Art. 78. ustawy z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (Dz. U. z 2020 r. poz. 1415 z późn. zm.).

lowanego oraz dostępu podmiotów trzecich do danych objętych tajemnicą. W Opinii przedstawiona jest również możliwa, w ocenie autora, interpretacja przepisów prawa oraz zasad stosowania określonych w Komunikacie Chmurowym, na podstawie której przedstawiono rekomendacje dalszych działań możliwych do podjęcia przez ZBP, jako reprezentanta interesów sektora bankowego. Banki mogą samodzielnie wykorzystać przedstawione argumenty jako kierunkowe podejście, natomiast Opinia nie stanowi wiążącej porady prawnej. Z oczywistych względów, porada tego rodzaju wymagałaby analizy konkretnego stanu faktycznego.

Kiedy stosować Komunikat Chmurowy?

3.29. Biorąc pod uwagę powyższe wnioski, a w szczególności rozróżnienie między przepisami dotyczącymi outsourcingu a przepisami w zakresie ochrony tajemnicy bankowej, należy stwierdzić, że samo przetwarzanie informacji prawnie chronionych w chmurze obliczeniowej nie jest przesłanką do zaistnienia outsourcingu, lecz tylko takie, które odbywa się w ramach relacji o charakterze outsourcingu chmury obliczeniowej.

3.30. Jak zatem odróżnić przetwarzanie danych w chmurze obliczeniowej o charakterze outsourcingu chmury obliczeniowej od przetwarzania pozbawionego takiego charakteru? W tym celu pomocny może być tzw. test autonomiczności, polegający na weryfikacji szeregu kryteriów opisanych poniżej[9]. Przeprowadzenie testu jest punktem wyjścia dla rozważań o konieczności stosowania Komunikatu Chmurowego w razie wykorzystania chmury obliczeniowej przez Partnera. Test jest elementem szerszej logiki prawnej, jaką przedstawiamy w Schemacie, ilustrującym zagadnienie stosowania Komunikatu, outsourcingu regulowanego oraz kwestii tajemnicy bankowej.

Test autonomiczności

3.31. Test autonomiczności korzystania z chmury obliczeniowej przez Partnera pozwala zweryfikować, czy korzystanie tworzy relację outsourcingu (lub odpowiednio podoutsourcingu) chmury obliczeniowej wobec Banku. Pozwala też wyeliminować błąd uproszczonego myślenia, polegający na założeniu, że gdy współpraca z Partnerem ma charakter outsourcingu regulowanego, to przy wykorzystaniu chmury obliczeniowej zawsze występuje outsourcing.

3.32. Wykorzystanie chmury obliczeniowej przez Partnera nie będzie się wiązało z zaistnieniem outsourcingu chmury obliczeniowej w relacji do Banku w sytuacji, gdy spełnione są łącznie następujące warunki:

a) usługa chmury obliczeniowej nie jest niezbędna dla realizacji przedmiotu usługi świadczonej przez Partnera;

b) wykorzystanie usługi chmury obliczeniowej przez Partnera ma charakter autonomiczny (tj. usługa chmurowa nie jest elementem charakterystycznym, cechą funkcjonalną, bezpośrednim, cząstkowym elementem usługi Partnera, nie stanowi istoty zleconej czynności, a jej realizacja nie ma charakteru podpowierzenia wykonywania czynności przez Bank, np. nie jest infrastrukturą chmurową dla dostarczanej aplikacji, która by wpływała na uznanie, że Partner świadczy usługę, w ramach której dochodzi do outsourcingu usługi chmury obliczeniowej dla Banku);

9 Nazwa „test autonomiczności" jest nazwą własną autora. Przywołane kryteria były konsultowane z ekspertami w zakresie prawa, ryzyka i bezpieczeństwa, biorącymi udział w ramach prac Grupy Roboczej ZBP opracowującej standard PolishCloud 2.0.

c) usługa chmury obliczeniowej nie jest udostępniana do bezpośredniego wykorzystania przez Bank ani nie jest dostępna na jego żądanie (np. Bank nie korzysta z licencji na usługę chmurową, nie loguje się do konta pozwalającego na dostęp do tej usługi[10]. Dla przykładu, rozmowa on-line odbywa się „na zaproszenie" Partnera za pomocą jego usługi chmury obliczeniowej, a bank korzysta z zaproszenia jako „gość" – nie wchodzi tym sposobem w zakres wykorzystywanych licencji Partnera).

3.33. Jeżeli powyższe warunki są spełnione, usługa chmury obliczeniowej nie będzie wobec banku stanowiła outsourcingu chmury obliczeniowej w rozumieniu Komunikatu Chmurowego, ani też podoutsourcingu chmury obliczeniowej. Bank nie będzie miał obowiązku stosować postanowień Komunikatu Chmurowego wobec takiego wykorzystania chmury obliczeniowej. Jak bowiem wykazano powyżej, Komunikat Chmurowy w swej istocie powinien być interpretowany w zgodzie z celem przepisów outsourcingu regulowanego.

3.34. Kryteria testu autonomiczności nawiązują również do przytaczanego wyżej w opinii pkt. VI.2.7.b Komunikatu Chmurowego, w którym UKNF wskazuje, że stosowanie Komunikatu Chmurowego zależy od faktycznego wykorzystania usług chmurowych do świadczenia usługi dla Banku, przy czym wymaga zaznaczenia, że wyraźnie jest tam wskazana koniunkcja dla przesłanek zakresu czynności i przetwarzania informacji prawnie chronionych („oraz"). Uzasadnia to zatem stwierdzenie, że:

a) test autonomiczności można traktować jako narzędzie do oceny „zakresu" czynności decydującego o outsourcingu chmury obliczeniowej;

b) samo przetwarzanie informacji prawnie chronionych w chmurze nie jest wystarczającą przesłanką dla zaistnienia outsourcingu chmury obliczeniowej i w konsekwencji obowiązku stosowania Komunikatu, musi ono być połączone co najmniej z outsourcingiem chmury obliczeniowej innym niż szczególny (zob. pkt 3.19 Opinii).

3.35. Podsumowując, jak dodatkowo zobrazowano w Schemacie, w wyniku testu autonomiczności:

a) Bank stosuje Komunikat Chmurowy we współpracy z Partnerami, gdy:

i) Wykorzystanie chmury przez Partnera nosi znamiona outsourcingu (tj. nie jest autonomiczne – negatywny wynik testu autonomiczności) oraz ma cechy outsourcingu szczególnego opisane w Komunikacie Chmurowym.[11]

ii) Wykorzystanie chmury przez Partnera nosi znamiona outsourcingu innego niż szczególny (tj. nie jest autonomiczne – negatywny wynik testu autonomiczności) oraz wiąże się z przetwarzaniem informacji prawnie chronionych.

b) Bank nie stosuje Komunikatu Chmurowego we współpracy z Partnerami, gdy:

10 W Q&A pojawił się przykład usługi chmurowej do przechowywania dokumentów.

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) wpływałaby 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.

i) Wykorzystanie chmury przez Partnera ma charakter autonomiczny (pozytywny wynik testu autonomiczności).

ii) Wykorzystanie chmury nosi znamiona outsourcingu innego niż szczególny (nie jest autonomiczne – negatywny wynik testu autonomiczności), ale nie wiąże się z przetwarzaniem informacji prawnie chronionych.

3.36. Test autonomiczności daje wynik bezwzględny, co oznacza, że tylko w razie jego pozytywnego wyniku będzie zachodziło autonomiczne wykorzystanie chmury obliczeniowej. W każdym innym przypadku wykorzystania chmury obliczeniowej przez Partnera będzie zachodził podoutsourcing chmury obliczeniowej – szczególny lub inny niż szczególny.

3.37. Test autonomiczności jest tożsamy dla Partnerów w ramach outsourcingu regulowanego, jak i Partnerów poza outsourcingiem regulowanym. Bank może wykorzystywać test autonomiczności w szczególności w sytuacji, kiedy poweźmie informacje o wykorzystaniu chmury obliczeniowej przez Partnera, mającym znamiona outsourcingu chmury obliczeniowej.

Stosowanie Komunikatu a tajemnica bankowa i outsourcing regulowany

3.38. Wymaga wyraźnego zastrzeżenia, że o ile Bank w określonych wyżej sytuacjach nie ma obowiązku stosowania Komunikatu Chmurowego, to nie wyłącza to obowiązków zarówno Banku, jak i Partnera, w zakresie ochrony informacji prawnie chronionych, w szczególności tych wynikających z przepisów Prawa bankowego w odniesieniu do tajemnicy bankowej.

3.39. Przetwarzanie informacji objętych tajemnicą bankową w usługach chmury obliczeniowej wymaga jej odpowiedniego zabezpieczenia w celu ograniczenia kręgu podmiotów posiadających dostęp do tych informacji do podmiotów, które są upoważnione ustawowo do wglądu w te informacje. Pytaniem otwartym pozostaje, po czyjej stronie leży ten obowiązek – czy zawsze po stronie Banku, czy też po stronie Partnera.

3.40. Nie ulega wątpliwości, że Bank odpowiada wobec swoich klientów za naruszenia tajemnicy spowodowane działaniami lub zaniechaniami podmiotów, którym powierza wykonywanie czynności w ramach outsourcingu regulowanego, w tym outsourcingu chmury obliczeniowej, o ile do takiego dochodzi.

3.41. Partner natomiast zasadniczo odpowiada również indywidualnie za zabezpieczenie danych objętych tajemnicą i w razie naruszenia obowiązku zachowania tajemnicy w poufności może odpowiadać prawnie w następujący sposób:

a) wobec Banku, na podstawie odpowiedzialności odszkodowawczej za niewykonanie lub nienależyte wykonanie umowy – o ile udostępnienie informacji objętych tajemnicą naruszy postanowienia umowy zawartej przez Partnera z Bankiem;

b) wobec Banku na podstawie odpowiedzialności odszkodowawczej na zasadzie winy (art. 415 Kodeksu cywilnego) – w szczególności jeżeli wymiana informacji objętych tajemnicą odbywa się na innej podstawie prawnej, bez zobowiązań umownych. W takiej sytuacji, zawinione przez Partnera nienależyte zabezpieczenie informacji przetwarzanych w chmurze, pozwalające na dostęp do nich nieuprawnionych podmiotów, jeśli wyrządzi Bankowi szkodę, będzie podstawą do ewentualnej odpowiedzialności odszkodowawczej;

c) indywidualnie w ramach odpowiedzialności karnej – zgodnie z art. 171 ust. 5 Prawa bankowego kto, będąc obowiązany do zachowania tajemnicy bankowej, ujawnia lub wykorzystuje informacje stanowiące tajemnicę bankową, niezgodnie z upoważnieniem określonym w ustawie, podlega grzywnie do 1 000 000 złotych i karze pozbawienia wolności do lat 3. W takiej sytuacji, odpowiedzialność Partnera zależy m.in. od tego, czy ustawa nakłada na niego obowiązek zachowania informacji objętych tajemnicą w poufności. Wbrew pozorom, zagadnienie to nie jest oczywiste, zostanie ono omówione bliżej w dalszej części Opinii.

3.42. Wobec powyższego, w naszej ocenie, w zakresie odpowiedzialności Banku leży przede wszystkim zwrócenie uwagi na postanowienia umów łączących bank z Partnerem w zakresie zobowiązania do zapewnienia poufności danych przez Partnera, w szczególności danych objętych tajemnicą bankową. W przypadku Partnerów działających w ramach outsourcingu regulowanego bank ma przy tym obowiązek weryfikować łańcuch powierzenia zleconych czynności do ewentualnych dalszych partnerów.

3.43. W celu zidentyfikowania wykorzystania chmury wymagającego dalszej analizy (tj. w ramach outsourcingu chmury obliczeniowej) Bank może posłużyć się testem autonomiczności. Analiza podstaw prawnych udostępnienia informacji objętych tajemnicą bankową przez Partnera do Dostawcy chmury może zostać podjęta przez Bank w szczególności w sytuacji, w której Bank poweźmie informacje, że taki dostęp występuje.

Zidentyfikowanie dostępu Dostawcy chmury do informacji objętych tajemnicą – możliwe działania

3.44. W przypadku negatywnego wyniku testu autonomiczności, a jednocześnie powzięcia przez Bank informacji o możliwym dostępie podmiotów nieuprawnionych do informacji objętych tajemnicą i przetwarzanych w chmurze obliczeniowej przez Partnera w ramach outsourcingu regulowanego, rekomendowane jest zweryfikowanie zakresu takiego dostępu. W szczególności obejmuje to zweryfikowanie, czy Partner korzysta z chmury we własnej działalności w sposób, w który rzeczywiście wiąże się on z przetwarzaniem informacji objętych tajemnicą w chmurze obliczeniowej, w taki sposób, że Dostawca usługi chmury ma do nich dostęp, np. czy prowadzi równolegle innego rodzaju działalność, a czynności związane z dostępem do tajemnicy wykonuje wyłącznie w oparciu o infrastrukturę techniczną udostępnioną przez Bank lub zewnętrznego dostawcy działającego na zlecenie Banku.

3.45. Jeśli taki dostęp występuje, to możliwe dalsze działania obejmują w szczególności usankcjonowanie tej sytuacji poprzez zastosowanie odpowiedniej podstawy prawnej takiego dostępu.

3.46. Zgodnie ze Schematem dla Partnerów w ramach outsourcingu regulowanego rozwiązaniem może być przekwalifikowanie korzystania z chmury na podoutsourcing regulowany – wtedy podstawą dostępu będzie art. 104 ust. 2 pkt 2 b Prawa bankowego. Wymaga to zmiany faktycznego sposobu współpracy na taki, który pozwoli przyjąć, że zachodzi outsourcing chmury obliczeniowej (test autonomiczności da wynik negatywny) przy jednoczesnej kwalifikacji jako podoutsourcing regulowany.

3.47. Alternatywną podstawę prawną może stanowić pozyskanie zgody beneficjentów tajemnicy na udostępnienie tajemnicy takim podmiotom trzecim (art. 104 ust. 3 Prawa bankowego). Scenariusz ten może być trudny do zrealizowania w praktyce.

3.48. **Wykładnia rozszerzająca art. 104 ust. 1 Prawa bankowego.** Pewnym rozwiązaniem w zakresie podstawy prawnej udostępnienia tajemnicy może być również oparcie się o pierwotne regulacje tajemnicy bankowej zawarte w art. 104 ust. 1 Prawa bankowego. Regulacja ta pochodzi jeszcze z brzmienia Prawa bankowego sprzed wprowadzenia przepisów dot. outsourcingu regulowanego. Zgodnie z ww. przepisem obowiązek zachowania tajemnicy bankowej dotyczy (i) Banku, (ii) osób w nim zatrudnionych oraz (iii) osób, za których pośrednictwem Bank wykonuje czynności bankowe. Kluczowym elementem tego rozwiązania jest dotychczasowa interpretacja trzeciej z wymienionych kategorii podmiotów zobowiązanych do zachowania tajemnicy bankowej i dalsza jej ewolucja, uwzględniająca upływ czasu oraz zmieniające się warunki rynkowe, w szczególności wydłużające się łańcuchy dostaw nowych technologii. Dostęp do nowych technologii jest niezbędny do działalności banków oraz utrzymania ich konkurencyjności wobec tzw. *challenger banków*, budowanych w oparciu o najnowsze rozwiązania informatyczne. Skala przetwarzania danych w gospodarce, w tym także w sektorze bankowym, rośnie wykładniczo. Nie omija to przetwarzania danych objętych tajemnicą bankową, co niesie zupełnie nowe wyzwania i możliwości niż jeszcze dekadę temu. W tym kontekście warto zaznaczyć, że w doktrynie prawniczej[12] silną reprezentację posiada tzw. otwarta (rozszerzająca) wykładnia pojęcia „osób, za których pośrednictwem Bank wykonuje czynności bankowe" („**osoby pośredniczące**" lub „**podmioty wspomagające**"). W ramach tej wykładni przyjmuje się, że obowiązek tajemnicy bankowej obejmuje nie tylko pracowników Banku, lecz także osoby współpracujące z Bankiem na podstawie umowy zlecenia, w ramach jednoosobowej działalności gospodarczej, dostawców w ramach outsourcingu regulowanego, ich personel[13], a także osoby mające w praktyce dostęp do informacji objętych tajemnicą – „osoby, których działanie umożliwia funkcjonowanie Banku"[14]. Stanowisko takie uzasadnia się w szczególności tym, że „z punktu widzenia ochrony interesu beneficjenta tajemnicy bankowej nie jest istotne, czy Bank wiąże z tymi osobami stosunek pracy, czy inny stosunek umowny, ponieważ celem wprowadzenia ochrony informacji objętych tajemnicą bankową jest to, by został zapewniony wysoki standard ochrony danych konfidencjonalnych"[15]. W doktrynie podnosi się również, że obowiązek zachowania tajemnicy bankowej dotyczy, wbrew literalnemu brzmieniu art. 104 ust. 1. Prawa bankowego, wszystkich podmiotów, które uzyskały dostęp do chronionych informacji w związku ze swoim udziałem w wykonywaniu przez Bank czynności bankowych. Intencją ustawodawcy, jak również funkcją instytucji tajemnicy bankowej jest to, aby każdy podmiot, który uzyska dostęp do informacji chronionych, był zobowiązany do zachowania ich w tajemnicy.[16] Dotyczy to również usług w zakresie zarządzania systemem informatycznym, które nie stanowią pośredniczenia w wykonywaniu czynności bankowych, a wykonujący je podmiot nie jest pracownikiem banku. Mimo to uznano, że do określenia obowiązków usługodawcy znajduje zastosowanie przepis art. 104 ust. 1 Prawa bankowego[17].

12 por. K. Królikowska, Komentarz do art. 104 Prawa bankowego [w:] B. Bajor i in., *Prawo bankowe. Komentarz do przepisów cywilnoprawnych*, WKP 2020,

13 Ibidem.

14 Ibidem, podobnie R. Sikorski, Komentarz do art. 104 Prawa bankowego [w:] R. Sikorski (red.), Prawo Bankowe. Komentarz, wyd. 1, Warszawa 2015, Legalis; por. J. Byrski w: Tajemnica prawnie chroniona [...] który postuluje *de lege ferenda* aby wymienić w art. 104 ust. 1 wprost przedsiębiorców wykonujących „czynności faktyczne związane z działalnością bankową", czyli dostawców outsourcingu regulowanego.

15 K. Królikowska, ibidem.

16 Por. Z. Ofiarski Komentarz do art. 104 Prawa bankowego, Prawo bankowe. Komentarz, LEX 2013.

17 Ibidem.

Słusznie więc w literaturze odchodzi się od wąskiej interpretacji pojęcia „osób pośredniczących", zakładającej, że są to tylko osoby fizyczne pełniące rolę pośredników lub – jeszcze dalej – mające pełnomocnictwo do działania w imieniu banku. Wąska interpretacja jako swój fundament przyjmuje wykładnię językową art. 104 ust. 1. Prawa bankowego, uwzględniającą przede wszystkim dosłowne brzmienie przepisu, a nie jego cel i funkcję.

3.49. Biorąc pod uwagę opisane wyżej zmiany w sferze faktycznej, która regulowana jest normami Prawa bankowego, a także wskazywany wyżej cel regulacji, wydaje się, że wykładnia rozszerzająca, będąca podstawą dla jej ewolucji zaproponowanej poniżej, powinna być przeważająca do czasu ewentualnej nowelizacji przepisów. Należy się zgodzić z przytoczonym powyżej poglądem, że celem regulacji art. 104 ust. 1 Prawa bankowego jest bowiem zasadniczo objęcie obowiązkiem zachowania tajemnicy bankowej w poufności każdego podmiotu, który, działając w ramach szeroko rozumianego polecenia banku, wchodzi w posiadanie takich informacji.[18] Idąc z duchem czasu, w ocenie autora należy obecnie mówić o „podmiotach wspomagających", a nie „osobach wspomagających", wskazując na różnorodność tych podmiotów (nie tylko osoby fizyczne, ale i osoby prawne). Elementem ewolucji wykładni rozszerzającej jest przyjęcie, że w sytuacji gdy Partner współpracuje z Bankiem, wchodząc w posiadanie tajemnicy bankowej na podstawie rozszerzonej wykładni art. 104 ust. 1 Prawa bankowego, może ją udostępnić dalej podmiotom, które z nim współpracują na analogicznych zasadach, jak personel Partnera – tj. pod warunkiem zobowiązania ich do zachowania w poufności informacji objętych tajemnicą oraz poinformowania o odpowiedzialności prawnej związanej z dostępem do tej informacji. Przyjmując taką wykładnię, Dostawca chmury obliczeniowej współpracujący z Partnerem w modelu autonomicznym (pozytywny wynik testu autonomiczności), co do którego stosuje się art. 104 ust. 1 Prawa bankowego, mógłby otrzymać dostęp do informacji objętych tajemnicą na tej samej podstawie prawnej, tj. art. 104 ust. 1 Prawa bankowego. Zasadniczo więc traktowany byłby analogicznie jak członek personelu Partnera, który otrzymuje dostęp do informacji w celu realizacji świadczeń Partnera na rzecz banku. W konsekwencji tego podejścia Dostawca chmury byłby objęty obowiązkiem dotrzymania tajemnicy bankowej w sposób pierwotny[19]. Przyjęciu tej koncepcji nie szkodzi przy tym istnienie przepisu art. 104 ust. 2 pkt. 2 lit. a–b Prawa bankowego, przewidującego możliwość ujawnienia dostawcy i poddostawcy outsourcingu regulowanego informacji objętych tajemnicą. Przepis ten nie jest sprzeczny z art. 104 ust. 1 Prawo bankowego, w szczególności nie zawiera sformułowań, które wskazywałby, że jest on jedyną podstawą prawną dla udostępnienia informacji objętych tajemnicą w ramach współpracy w outsourcingu regulowanym. W kontekście analizowanego zagadnienia kluczowe jest określenie, czy przy udostępnieniu informacji objętych tajemnicą jednocześnie dochodzi do outsourcingu chmury obliczeniowej (test autonomiczności), co kwalifikowałoby taką sytuację jako podoutsourcing regulowany. W przypadku, gdy wykorzystanie chmury realizuje przesłanki outsourcingu (podoutsourcingu) regulowanego (tj. negatywny test autonomiczności oraz dostęp Dostawcy chmury do danych objętych tajemnicą), konieczne jest zastosowanie właściwej podstawy prawnej udostępnienia danych, tj. art. 104 ust. 2 pkt. 2 lit. a–b Prawa bankowego.

18 Ibidem, por. także M. Kłaczyński, *Tajemnica bankowa w outsourcingu*, TPP 2002, nr 3, s. 11.

19 Podział na podmioty „pierwotnie" oraz „w ramach wtórnego obiegu informacji" objęte obowiązkiem zachowania tajemnicy zaproponował J. Byrski w: *Tajemnica prawnie chroniona w działalności bankowej* 2010, wyd. 1 (Rozdz. III., §1 pkt. I.).

3.50. Istotnym elementem relacji przepisów art. 104 ust. 1 oraz art. 104 ust. 2 pkt 2 Prawa bankowego jest także kwestia odpowiedzialności karnej. W literaturze[20] przyjmuje się, że przepisy art. 104 ust. 5 oraz art. 104 ust. 6 Prawa bankowego określające m.in. zasady wykorzystania informacji objętych tajemnicą przez dostawców w ramach outsourcingu regulowanego nie nakładają wprost obowiązku zachowania tajemnicy bankowej na te podmioty oraz osoby w nich zatrudnione. W konsekwencji nie jest możliwe zastosowanie sankcji karnych przewidzianych w art. 171 ust. 5 Prawa bankowego wobec tych podmiotów w razie zakwalifikowania danej relacji jako outsourcing (podoutsourcing) regulowany. Co do powyższego podejścia można mieć pewne wątpliwości ze względu na cel regulacji przepisów o tajemnicy przytaczany powyżej, natomiast z uwagi na charakter odpowiedzialności karnej, wymagającej jasnej podstawy prawnej (obowiązek zachowania tajemnicy musi wprost wynikać z ustawy) wypada się zgodzić z przywołanym wyżej stanowiskiem. W konsekwencji podmiot objęty pierwotnym obowiązkiem zachowania tajemnicy na gruncie art. 104 ust. 1 Prawa bankowego (w tym w ramach zaproponowanej ewolucji wykładni rozszerzającej) byłby odpowiedzialny karnie za poufność tajemnicy bankowej, natomiast odpowiedzialność karna podmiotu otrzymującego informacje na postawie art. 104 ust. 2 pkt. 2 lit. a–b za ich poufności jest co najmniej wątpliwa.

3.51. Podsumowując, zaproponowana wyżej ewolucja rozszerzającej wykładni art. 104 ust. 1 Prawa bankowego znajduje swoje prawne uzasadnienie i może zostać zastosowana w przypadku autonomicznego wykorzystania chmury przez Partnera poprzez uznanie Dostawcy chmury obliczeniowej i jego personelu oraz poddostawców za tzw. podmioty wspomagające, pierwotnie objęte obowiązkiem zachowania poufności tajemnicy bankowej na gruncie art. 104 ust. 1 Prawa bankowego. Warunkiem jej zastosowania jest możliwość zakwalifikowania samego Partnera jako podmiotu, który jest objęty art. 104 ust. 1 Prawa bankowego. W ślad za doktryną takim podmiotem może być Partner współpracujący z Bankiem w ramach outsourcingu regulowanego.

3.52. W kwestii praktycznego zastosowania wyżej zaproponowanej wykładni rozszerzającej należy uwzględnić również oczekiwania organu nadzoru i ewentualne skutki dla całego sektora bankowego, gdyż powszechne jej wykorzystanie stanowiłoby prawne usankcjonowanie dostępu do informacji objętych tajemnicą dla kategorii podmiotów obejmującej m.in. dostawców usług chmury obliczeniowej.

3.53. Podejściem łączącym zapotrzebowanie sektora bankowego na prawo odpowiadające praktyce rynkowej z ochroną stabilności sektora bankowego oraz prywatności danych klientów może być zastosowanie rozszerzonej wykładni art. 104 ust. 1 Prawa bankowego w ograniczonym zakresie Partnerów, w oparciu o szacowanie ryzyka współpracy z danym Partnerem oraz ryzyko operacyjne wynikające z udostępnienia informacji objętych tajemnicą podmiotom współpracującym z Partnerem, jak np. dostawcy określonych usług chmury obliczeniowej w modelu autonomicznym. Jeżeli usługa realizowana przez Partnera zaklasyfikowana byłaby przez Bank jako krytyczna[21], a ryzyko dla Banku związane z dostępem Dostawcy chmury do informacji przetwarzanych przez Partnera w ramach tejże usługi byłoby nieakceptowalne, Bank mógłby wybrać scenariusz alternatywny, tj. innej podstawy prawnej lub uniemożliwienia dostępu do informacji

20 ibidem.

21 Na przykład biorący udział w procesach kluczowych lub krytycznych Banku, zgodnie z Rekomendacją M, lub też wedle kryteriów analogicznych do kryteriów outsourcingu szczególnego chmury obliczeniowej, opisanych w Komunikacie Chmurowym.

takiemu Dostawcy chmury obliczeniowej. Przykładowo: jako proces krytyczny można zakwalifikować sprzedaż kredytów. W ramach tego procesu ocena ryzyka kredytowego powinna być kwalifikowana jako krytyczna, podczas gdy współpraca z poszczególnym pośrednikami kredytowymi już niekoniecznie. Sam proces sprzedaży może być procesem krytycznym, ale konkretne czynności Partnera nie muszą być krytyczne – klient może skorzystać z innego Partnera, żeby zrealizować ten sam proces.

3.54. Wobec nowo zawieranych umów dodatkowym środkiem ochronnym przy zastosowaniu rozszerzonej wykładni art. 104 ust. 1 Prawa bankowego mogłoby być również przyjęcie przez Bank obowiązku udokumentowania zakresu wykorzystania chmury przez Partnera w outsourcingu regulowanym. Mógłby on by być realizowany np. poprzez załącznik do umowy z Partnerem obejmujący informacje objęte obowiązkiem notyfikacyjnym z Komunikatu Chmurowego. Załącznik taki mógłby stanowić podstawę do ewentualnej weryfikacji przez organ nadzoru zasadności przyjętego przez Bank podejścia, pozwalając tym samym mitygować ewentualne obawy organu nadzoru w zakresie zbyt szerokiego przyjęcia tego podejścia w skali sektorowej.

3.55. Dopełniając powyższe rozważania, jak przedstawiono w Schemacie, przy przyjęciu wykładni rozszerzającej art. 104 ust. 1 Prawa bankowego nie byłoby potrzeby stosowania Komunikatu Chmurowego z uwagi na autonomiczność wykorzystania i brak znamion outsourcingu chmury obliczeniowej. Konieczne natomiast byłoby:

a) nałożenie przez Partnera obowiązku zachowania informacji objętych tajemnicą bankową na Dostawcę chmury obliczeniowej oraz jego personel i poddostawców;

b) dla nowych umów – udokumentowanie wykorzystania chmury obliczeniowej przez Partnera zgodnie z pkt. 3.54 Opinii.

3.56. **Zablokowanie dostępu**. Scenariusz uniemożliwienia dostępu do informacji objętych tajemnicą bankową może być zastosowany w braku ustalenia odpowiedniej podstawy prawnej dla dostępu do tajemnicy przez Dostawcę usługi chmurowej oraz w przypadku odrzucenia przez Bank możliwości zastosowania rozszerzonej wykładni art. 104 ust. 1. Prawa bankowego omawianej powyżej. W takiej sytuacji, gdy mamy do czynienia z autonomicznym wykorzystaniem chmury obliczeniowej przez Partnera, odpowiedzialnością Banku jest zobowiązanie Partnera do zabezpieczenia danych przed dostępem Dostawcy usługi chmury obliczeniowej (np. poprzez odpowiednie szyfrowanie informacji objętych tajemnicą, zaprzestanie wykorzystywania chmury obliczeniowej w zakresie współpracy z Bankiem, wykorzystanie dodatkowych zabezpieczeń oferowanych przez Dostawcę chmury obliczeniowej, udostępnienie przez Bank odpowiednika usługi chmury obliczeniowej). Warto zwrócić uwagę, że zgodnie z Komunikatem Chmurowym przez ujawnienie przetwarzanych informacji rozumie się: „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”.

3.57. **Partnerzy poza outsourcingiem regulowanym.** W stosunku do Partnerów współpracujących z Bankiem poza outsourcingiem bankowym najczęściej istnieje „dedykowana" podstawa prawna do uzyskania informacji objętej tajemnicą przez Partnera (np. przez biegłego rewidenta na podstawie art. 105 ust. 3 Prawa bankowego). Biegły rewident ma obowiązek zachowania tajemnicy na bazie odrębnych przepisów. O ile więc wykorzystanie chmury jest autonomiczne, odpowiedzialność za ochronę informacji w niej przetwarzanych spoczywa zasadniczo na Partnerze. Bank może oczywiście podjąć dalszą analizę takiej sytuacji, w szczególności gdy poweźmie odpowiednie informacje o wykorzystaniu chmury obliczeniowej i oceni, że taka sytuacja rodzi dla Banku nieakceptowalne ryzyka (np. w związku z niedostatecznymi zobowiązaniami w zakresie poufności). W takiej sytuacji możliwe do podjęcia działania obejmują i) pozyskanie zgody beneficjentów tajemnicy, ii) zobowiązanie Partnera do zablokowania dostępu do danych lub iii) przekwalifikowanie wykorzystania chmury na podoutsourcing regulowany. Ten ostatni środek będzie również skutkował zmianą charakteru współpracy z samym Partnerem na outsourcing regulowany.

Pośrednicy jako podmioty nadzorowane zobowiązane do stosowania Komunikatu Chmurowego

3.58. Na wstępie należy zaznaczyć, że o ile pośrednicy kredytów hipotecznych oraz ich agenci są podmiotami nadzorowanymi *sensu largo*, tj. są wymienieni w art. 1 ust. 2 pkt. 8 Ustawy o nadzorze[22], to nadzór ten odbywa się zgodnie z przepisami Ustawy o kredycie hipotecznym. Ustawa ta nie reguluje zagadnienia outsourcingu, przewidując wyłącznie określone wymogi dla personelu pośrednika lub agenta. Ustawa o kredycie hipotecznym nie zawiera odpowiedników art. 6a–6d Prawa bankowego, które nakładałyby na podmioty w niej uregulowane szczególne warunki w zakresie powierzania wykonywania czynności związanych z działalnością pośrednika lub agenta. Ustawa ta również nie przewiduje odrębnych przepisów w zakresie tajemnicy. Nadzór UKNF nad pośrednikami i ich agentami w zakresie outsourcingu odbywa się w sposób pośredni, poprzez nałożenie wymogów outsourcingowych na banki współpracujące z pośrednikami i agentami. Warto zauważyć, że dość podobne zagadnienie powstaje przy nadzorze nad spółkami publicznymi (spółki notowane na rynkach regulowanych), które również są podmiotami nadzorowanymi w myśl Ustawy o nadzorze. W tym przypadku również nadzór nad spółkami publicznymi nie obejmuje zagadnienia outsourcingu. Co do zasady więc spółki publiczne nie mają obowiązku samodzielnego stosowania Komunikatu Chmurowego (chyba że jednocześnie prowadzą działalność regulowaną w zakresie outsourcingu – np. banki notowane na giełdzie). W tym kontekście sytuacja pośredników kredytu hipotecznego i agentów jest zbliżona do sytuacji spółki publicznej świadczącej dla Banku usługi w ramach outsourcingu regulowanego (np. dostawca usług IT) lub też relacji zakład ubezpieczeń – agent ubezpieczeniowy. Spółka publiczna realizująca usługi w outsourcingu regulowanym na rzecz Banku nie jest zobowiązana do samodzielnego stosowania Komunikatu przez sam fakt, że przetwarza takie dane w chmurze i jest podmiotem nadzorowanym *sensu largo*. W praktyce może być zobowiązana do realizacji wymogów Komunikatu Chmurowego, lecz będzie to wynikało z wymogów współpracy

22 *8) nadzór nad pośrednikami kredytu hipotecznego oraz ich agentami, sprawowany zgodnie z przepisami ustawy z dnia 23 marca 2017 r. o kredycie hipotecznym oraz o nadzorze nad pośrednikami kredytu hipotecznego i agentami (Dz. U. z 2020 r. poz. 1027).*

narzuconych przez Bank, a nie z postanowień Komunikatu Chmurowego. Podobnie jest z pośrednikami kredytu hipotecznego, gdyż w obu przypadkach określony bezpośrednio przepisami prawa nadzór nad tymi podmiotami nie obejmuje kwestii outsourcingu. Wobec powyższego pozostaje otwarte pytanie, jaka jest podstawa prawna obowiązku stosowania Komunikatu Chmurowego przez agentów ubezpieczeniowych[23] (i wydawałoby się analogicznie – pośredników kredytu hipotecznego i ich agentów) oraz inne podmioty nadzorowane *sensu largo*. Dlaczego dla pewnych podmiotów (*vide* spółki publiczne) przewiduje się wyjątki, a dla innych (agenci ubezpieczeniowi) takich wyjątków się nie przewiduje? Wydaje się, że konieczność stosowania Komunikatu powinna mieć swoje zaczepienie w relacji outsourcingu chmury obliczeniowej, która dla pewnych kategorii podmiotów nadzorowanych łączy się z obowiązkiem spełnienia warunków outsourcingu regulowanego. Podstawy prawnej do stosowania Komunikatu Chmurowego wobec takich pośredników i agentów należy ewentualnie poszukiwać w ogólnych normach kompetencyjnych KNF jako organu nadzoru nad rynkiem finansowym, zadając sobie jednocześnie pytanie, czy są one wystarczające do tak daleko idącego uregulowania działalności gospodarczej w drodze aktu *soft law*. Wydaje się, że uzasadnienie podejścia organu nadzoru jest spowodowane troską o ochronę danych objętych tajemnicą w obliczu rosnącego wolumenu i ilości sposobów przetwarzania danych. Należałoby podjąć dialog z organem nadzoru, aby określić, czy w każdym przypadku takie podejście jest rzeczywiście zgodne z zasadą proporcjonalności regulacji.

4. ANALIZA PRZYPADKÓW

Przykład 1 – Partner w ramach outsourcingu regulowanego (pośrednik)

4.1. *Umowa z Partnerem, który jest pośrednikiem kredytu hipotecznego na pośrednictwo kredytowe, w reżimie outsourcingu regulowanego. Partner korzysta na własne potrzeby z pakietu biurowego w formule chmury obliczeniowej, w modelu SaaS. Poczta oraz przechowywanie dokumentów funkcjonuje w oparciu o serwery i oprogramowanie Dostawcy usługi chmury obliczeniowej, a w ramach tych rozwiązań mogą być przetwarzane dane objęte tajemnicą bankową. Partner nie udostępnia tych rozwiązań na rzecz Banku.*

4.2. Bank nie ma w takiej sytuacji obowiązku stosowania Komunikatu, gdyż:

a) usługa chmurowa nie jest w tym przypadku niezbędna dla realizacji przedmiotu usługi Partnera (czynności pośrednictwa mogą się odbywać różnymi kanałami komunikacji z klientem);

b) usługa chmurowa jest wykorzystywana autonomicznie przez Partnera i nie jest elementem charakterystycznym, cechą funkcjonalną, cząstkowym elementem usługi, np. nie jest infrastrukturą chmurową dla usługi końcowej – usługa poczty lub oprogramowania biurowego jest pomocnicza dla całości działalności Partnera;

c) usługa chmurowa nie jest udostępniana do bezpośredniego wykorzystania przez Bank (Bank nie korzysta z licencji na rozwiązania chmurowe, nie loguje się do konta Partnera, nie korzysta z jego wirtualnej przestrzeni dyskowej);

23 Ten przykład i uzasadnienie podawane jest w Q&A.

d) samo przetwarzanie informacji prawnie chronionych w chmurze nie jest wystarczającą przesłanką do stosowania Komunikatu Chmurowego, jeśli nie łączy się z outsourcingiem.

4.3. Bank ma natomiast obowiązek zabezpieczyć w umowie z Partnerem zasady poufności informacji prawnie chronionych, zaś Partner – zabezpieczyć dane przed dostępem podmiotów trzecich. Jeżeli taki dostęp zostałby zidentyfikowany przez Bank, należy ocenić ryzyko z tym związane oraz zastosować jeden z możliwych scenariuszy:

a) przeprowadzenie analizy ryzyka, uwzględnienie rozszerzonej wykładni art. 104 ust. 1 Prawa bankowego (zob. 3.48. Opinii) i ewentualne udokumentowanie wykorzystania chmury (dla nowych umów);

b) pozyskanie zgody beneficjenta tajemnicy na udostępnienie (zob. pkt 3.47 Opinii);

c) uniemożliwienie dostępu do danych (zob. pkt 3.56 Opinii);

d) przekwalifikowanie korzystania na podoutsourcing regulowany (zob. pkt 3.46 Opinii).

4.4. W tym konkretnym przypadku dyskusyjne jest natomiast, czy pośrednik jako podmiot nadzorowany *sensu largo* miałby obowiązek samodzielnego stosowania Komunikatu Chmurowego – zob. pkt. 3.58 Opinii.

Przykład 2 – Usługa mailingu

4.5. *Umowa z dostawcą usługi kampanii marketingowych dedykowanych określonym klientom (tzw. targetowane kampanie). Usługa jest oparta o zewnętrzną pocztę chmurową (np. w formule SaaS), dane objęte tajemnicą są przetwarzane w chmurze obliczeniowej.*

4.6. Bank ma w takiej sytuacji obowiązek zweryfikować zgodność z Komunikatem Chmurowym, gdyż charakter usługi chmury obliczeniowej będzie przesądzał o tym, że zachodzi relacja outsourcingu chmury obliczeniowej, a zarazem są w chmurze przetwarzane informacje prawnie chronione (tajemnica bankowa). Komunikat zatem się stosuje, nawet, jeśli jest to outsourcing inny niż szczególny. W tym przypadku usługa chmurowa jest jednak niezbędna dla realizacji usługi Partnera – usługa polega bowiem na wysyłaniu w imieniu Banku treści handlowych, co oznacza, że istotą powierzenia jest usprawnienie procesu wysyłki poczty poprzez wykorzystanie narzędzi informatycznych, którymi nie dysponuje Bank. Wysyłka poczty przy wykorzystaniu chmury obliczeniowej jest więc elementem składowym tej usługi, jej cechą funkcjonalną.

Przykład 3 – Usługa tłumaczenia

4.7. *Umowa z Partnerem – biurem tłumacza przysięgłego – na tłumaczenia dokumentów (umów z klientami Banku), realizowana w modelu outsourcingu regulowanego[24]. Biuro tłumaczeń korzysta na własne potrzeby z pakietu biurowego w formule chmury obliczeniowej, w modelu SaaS. Poczta oraz przechowywanie dokumentów funkcjonuje w oparciu o serwery i oprogramowanie Dostawcy usługi chmury obliczeniowej, a w ramach tych rozwiązań mogą być przetwarzane dane objęte tajemnicą bankową. Partner nie udostępnia tych rozwiązań na rzecz Banku.*

24 Kwalifikacja w tym przypadku jako outsourcing regulowany jest dyskusyjna. Tłumacze przysięgli są zobowiązani do zachowania tajemnicy zawodowej odrębnymi przepisami ustawy z dnia 25 listopada 2004 r. o zawodzie tłumacza przysięgłego (Dz. U. z 2019 r. poz. 1326; z późn. zm.), więc można rozważać inną podstawą prawną udostępnienia tajemnicy bankowej – art. 104 ust. 1 Prawa bankowego.

4.8. Bank nie ma w takiej sytuacji obowiązku stosowania Komunikatu, z tych samych względów jak w Przykładzie 1 (zob. pkt 4.2-4.3 Opinii).

Przykład 4 – Partner poza outsourcingiem regulowanym

4.9. *Współpraca z zewnętrznym audytorem (biegły rewident), który korzysta z przechowywania dokumentów w oparciu o serwery i oprogramowanie Dostawcy usługi chmury obliczeniowej, a w ramach tych rozwiązań mogą być przetwarzane dane objęte tajemnicą bankową.*

4.10. W takiej sytuacji nie zachodzi ani outsourcing regulowany wobec biegłego rewidenta, ani też outsourcing chmury obliczeniowej (negatywny wynik testu autonomiczności). Dostęp do tajemnicy przez biegłego rewidenta odbywa się na dedykowanej podstawie prawnej (art. 105 ust. 1. Prawa bankowego), a biegły rewident jest ustawowo zobowiązany do zachowania jej w poufności na podstawie odrębnych przepisów. Bank nie ma obowiązku weryfikacji okoliczności ani sposobu korzystania z chmury obliczeniowej przez biegłego rewidenta, ale może dodatkowo podjąć dalsze działania w takiej sytuacji, w szczególności gdy poweźmie odpowiednie informacje o wykorzystaniu chmury obliczeniowej w sposób nieautonomiczny i oceni, że narusza to umowę lub taka sytuacja rodzi dla Banku nieakceptowalne ryzyka (np. w związku z niedostatecznymi zobowiązaniami w zakresie poufności). W takiej sytuacji możliwe do podjęcia działania obejmują i) pozyskanie zgody beneficjentów tajemnicy, ii) zobowiązanie Partnera do zablokowania dostępu Dostawcy chmury do danych lub iii) przekwalifikowanie wykorzystania chmury na podoutsourcing regulowany. Ten ostatni środek będzie również skutkował zmianą charakteru współpracy z samym Partnerem na outsourcing regulowany.

Przykład 5 – Partner poza outsourcingiem regulowanym

4.11. *Współpraca z zewnętrznym audytorem (biegły rewident), który dostarcza Bankowi oprogramowanie do analizy umów kredytowych w formule SaaS, korzystając z zewnętrznego hostingu chmury obliczeniowej. Rozwiązanie przetwarza dane objęte tajemnicą bankową.*

4.12. Pomimo że współpraca z biegłym rewidentem nie musi stanowić outsourcingu i występuje odrębna podstawa prawna do udostępnienia danych objętych tajemnicą bankową, Bank będzie miał w takiej sytuacji obowiązek zweryfikować zgodność z Komunikatem Chmurowym. Charakter doradztwa będzie polegał głównie na udostępnieniu usługi informatycznej wykorzystującej funkcjonalnie chmurę obliczeniową, co przesądzi o tym, że zachodzi relacja outsourcingu chmury obliczeniowej. W konsekwencji, z uwagi na przetwarzanie (nawet przy braku dostępu) informacji prawnie chronionych (tajemnica bankowa), Komunikat będzie się stosował – nawet jeśli jest to outsourcing inny niż szczególny. W tym przypadku chmura obliczeniowa jest elementem funkcjonalnym usługi biegłego rewidenta, przy czym bez znaczenia jest ewentualna okoliczność, że największa wartość biznesowa tej usługi tkwi w wiedzy eksperckiej biegłego rewidenta, jaka kryje się za oprogramowaniem (np. w jego algorytmach).

Odpowiedzi na pytania

4.13. **Pytanie 1.** *Czy Bank ma obowiązek weryfikować spełnienie wymogów Komunikatu Chmurowego w sytuacji, gdy współpracuje z Partnerem w ramach outsourcingu regulowanego, który korzysta z usługi chmury obliczeniowej?*

4.14. **Odpowiedź:**

4.15. Bank stosuje Komunikat Chmurowy we współpracy z Partnerami, gdy:

a) wykorzystanie chmury przez Partnera nosi znamiona outsourcingu (tj. nie jest autonomiczne – negatywny wynik testu autonomiczności) oraz ma cechy outsourcingu szczególnego opisane w Komunikacie Chmurowym;

b) wykorzystanie chmury przez Partnera nosi znamiona outsourcingu innego niż szczególny (tj. nie jest autonomiczne – negatywny wynik testu autonomiczności) oraz wiąże się z przetwarzaniem informacji prawnie chronionych[25].

4.16. Należy wtedy zweryfikować wszystkie wymogi Komunikatu Chmurowego oraz notyfikować UKNF.

4.17. Bank nie stosuje Komunikatu Chmurowego we współpracy z Partnerami, gdy:

a) wykorzystanie chmury przez Partnera ma charakter autonomiczny (pozytywny wynik testu autonomiczności);

b) wykorzystanie chmury nosi znamiona outsourcingu innego niż szczególny (nie jest autonomiczne – negatywny wynik testu autonomiczności), ale nie wiąże się z przetwarzaniem informacji prawnie chronionych.

4.18. **Pytanie 2.** *Czy Bank ma obowiązek weryfikować spełnienie wymogów Komunikatu Chmurowego w sytuacji, gdy współpracuje z Partnerem poza outsourcingiem regulowanym, który korzysta z usługi chmury obliczeniowej (np. biegłym rewidentem)?*

4.19. **Odpowiedź:** Analogicznie jak w odpowiedzi na Pytanie 1, z zastrzeżeniem, że jeśli korzystanie z chmury obliczeniowej w sposób nieautonomiczny (negatywny wynik testu autonomiczności) będzie się wiązało z dostępem Dostawcy chmury obliczeniowej do danych objętych tajemnicą bankową, wykorzystanie chmury obliczeniowej przez Partnera będzie również stanowiło podoutsourcing regulowany. W konsekwencji współpraca z Partnerem również zmieni swoją kwalifikację, ponieważ funkcjonalne wykorzystanie chmury obliczeniowej nada współpracy z Partnerem cechę outsourcingu usługi chmury obliczeniowej.

4.20. **Pytanie 3.** *Czy kwestia dostępu do danych objętych tajemnicą bankową przez Dostawcę usługi chmury obliczeniowej ma wpływ na obowiązek stosowania Komunikatu Chmurowego w określonych wyżej sytuacjach?*

4.21. **Odpowiedź:** Kwestia dostępu do danych w kontekście obowiązku stosowania Komunikatu Chmurowego jest kwestią wtórną. Istotny jest już sam fakt przetwarzania danych prawnie chronionych (w tym tajemnicy), gdzie „przetwarzanie" jest pojęciem szerszym od „dostępu". Kwestia dostępu jest natomiast istotna z perspektywy oceny, czy zachodzi wyłącznie outsourcing chmury obliczeniowej, czy ewentualnie równocześnie outsourcing

25 Gdy przetwarzanie będzie się wiązało z dostępem Dostawcy chmury do danych objętych tajemnicą bankową, wykorzystanie chmury obliczeniowej będzie jednocześnie stanowiło podoutsourcing regulowany.

regulowany. Punktem wyjścia dla stosowania Komunikatu jest zaistnienie współpracy o charakterze outsourcingu chmury obliczeniowej. W sytuacji braku takiej współpracy (pozytywny test autonomiczności) i zidentyfikowania dostępu Dostawcy chmury do informacji objętych tajemnicą konieczne jest zastosowanie odpowiedniej podstawy prawnej lub wyeliminowanie dostępu Dostawcy chmury do danych objętych tajemnicą.

4.22. **Pytanie 4.** *Jaka jest podstawa prawna obowiązku samodzielnego stosowania Komunikatu Chmurowego w przypadku pośredników kredytu hipotecznego, jako podmiotów nadzorowanych w rozumieniu Ustawy o nadzorze?*

4.23. **Odpowiedź:** Konieczność stosowania Komunikatu powinna mieć swoją podstawę w relacji outsourcingu chmury obliczeniowej, która dla pewnych kategorii podmiotów nadzorowanych łączy się z obowiązkiem spełnienia warunków outsourcingu regulowanego. W przypadku, gdy dany podmiot (np. pośrednik kredytu hipotecznego lub spółka publiczna) jest podmiotem nadzorowanym sensu largo (wymieniony w Ustawie o nadzorze), natomiast nie jest regulowany w zakresie outsourcingu, nie ma bezpośredniej i wyraźnej podstawy prawnej do narzucania tym podmiotom regulacji w zakresie outsourcingu. Podstawy prawnej do stosowania Komunikatu Chmurowego wobec takich pośredników i agentów należy ewentualnie poszukiwać w ogólnych normach kompetencyjnych KNF jako organu nadzoru nad rynkiem finansowym.

5. WNIOSKI I REKOMENDOWANE DZIAŁANIA

5.1. Podsumowując ustalenia zawarte w analizie, po pierwsze należy odróżnić kwestie przesłanek stosowania Komunikatu Chmurowego od kwestii dostępu do tajemnicy bankowej oraz kwalifikacji współpracy jako outsourcingu regulowanego.

5.2. W celu określenia obowiązku stosowania Komunikatu Chmurowego, Bank powinien uwzględnić przede wszystkim, czy współpraca z Partnerem odbywa się w modelu outsourcingu regulowanego (art. 6a Prawa bankowego), czy też poza reżimem outsourcingu regulowanego.

5.3. W pierwszym przypadku obowiązki Banku zależą głównie od tego, czy wykorzystanie chmury przez Partnera odbywa się w sposób autonomiczny. Aby to określić, proponujemy przeprowadzenie szeregu czynności, z których pierwszą jest przeprowadzenie tzw. testu autonomiczności. Kolejne czynności zależą od wyniku tego testu oraz zaistnienia określonych przesłanek. Ich sekwencja oraz zależności opisane są w Schemacie stanowiącym Załącznik nr 1 do Opinii. W zakresie dostępu do tajemnicy przez Dostawcę chmury obliczeniowej w modelu autonomicznym, jeśli takowy zostanie zidentyfikowany przez Bank, możliwe jest podjęcie kilku scenariuszy działania: i) pozyskanie zgody beneficjentów tajemnicy, ii) zobowiązanie Partnera do zablokowania dostępu do danych, iii) przekwalifikowanie wykorzystania chmury na podoutsourcing regulowany, iv) ocena ryzyka i przyjęcie rozszerzonej wykładni art. 104 ust.1 Prawa bankowego oraz ewentualne udokumentowanie wykorzystania chmury przez Partnera. Szczegółowe przesłanki i kolejność czynności opisane są w Schemacie stanowiącym Załącznik nr 1 oraz w tekście Opinii.

5.4. W przypadku Partnerów poza ramami outsourcingu regulowanego, odpowiedzialność za zachowanie poufności spoczywa zasadniczo indywidualnie na Partnerze. Bank

nie ma obowiązku badać w takiej sytuacji okoliczności wykorzystania przez Partnera chmury obliczeniowej, jednakże jeśli Bank w zidentyfikuje wykorzystanie usług chmurowych przez Partnera:

a) w przypadku powzięcia wątpliwości na temat charakteru tego wykorzystania – może wykonać test autonomiczności w celu dokonania oceny, czy zachodzi outsourcing chmury obliczeniowej – szczegółowe przesłanki i kolejność dalszych czynności opisane są w Schemacie.

b) w przypadku gdy oceni, że taka sytuacja rodzi dla Banku nieakceptowalne ryzyka (np. w związku z niedostatecznymi zobowiązaniami w zakresie poufności), może podjąć działania obejmujące i) pozyskanie zgody beneficjentów tajemnicy, ii) zobowiązanie Partnera do zablokowania dostępu do danych lub iii) przekwalifikowanie wykorzystania chmury na podoutsourcing regulowany. Ten ostatni środek będzie również skutkował zmianą charakteru współpracy z samym Partnerem na outsourcing regulowany.

5.5. W odniesieniu do samodzielnego obowiązku stosowania Komunikatu Chmurowego przez pośredników kredytu hipotecznego i ich agentów należy zauważyć, że rozszerzenie obowiązków w zakresie outsourcingu poprzez objęcie ww. podmiotów Komunikatem Chmurowym nie znajduje swego bezpośredniego oparcia w przepisach prawa dotyczących outsourcingu. Wymagania oparte na ogólnych kompetencjach nadzoru powinny brać pod uwagę przede wszystkim zasadę proporcjonalności stosowania regulacji.

5.6. W ujęciu sektorowym rekomendujemy ZBP podjęcie dialogu z organem nadzoru w celu wypracowania odpowiednich rozwiązań, pozwalających pogodzić perspektywę nadzoru i ryzyka w skali sektora finansowego z realiami rynku usług IT oraz kosztami realizacji wymogów regulacyjnych.

6. ZASTRZEŻENIA

6.1. Opinia została sporządzona w oparciu o stan prawny istniejący w dacie jej sporządzenia, a Kancelaria nie ponosi odpowiedzialności w przypadku późniejszych zmian w przepisach prawa, które mają wpływ na treść Opinii, jej cel lub zakres.

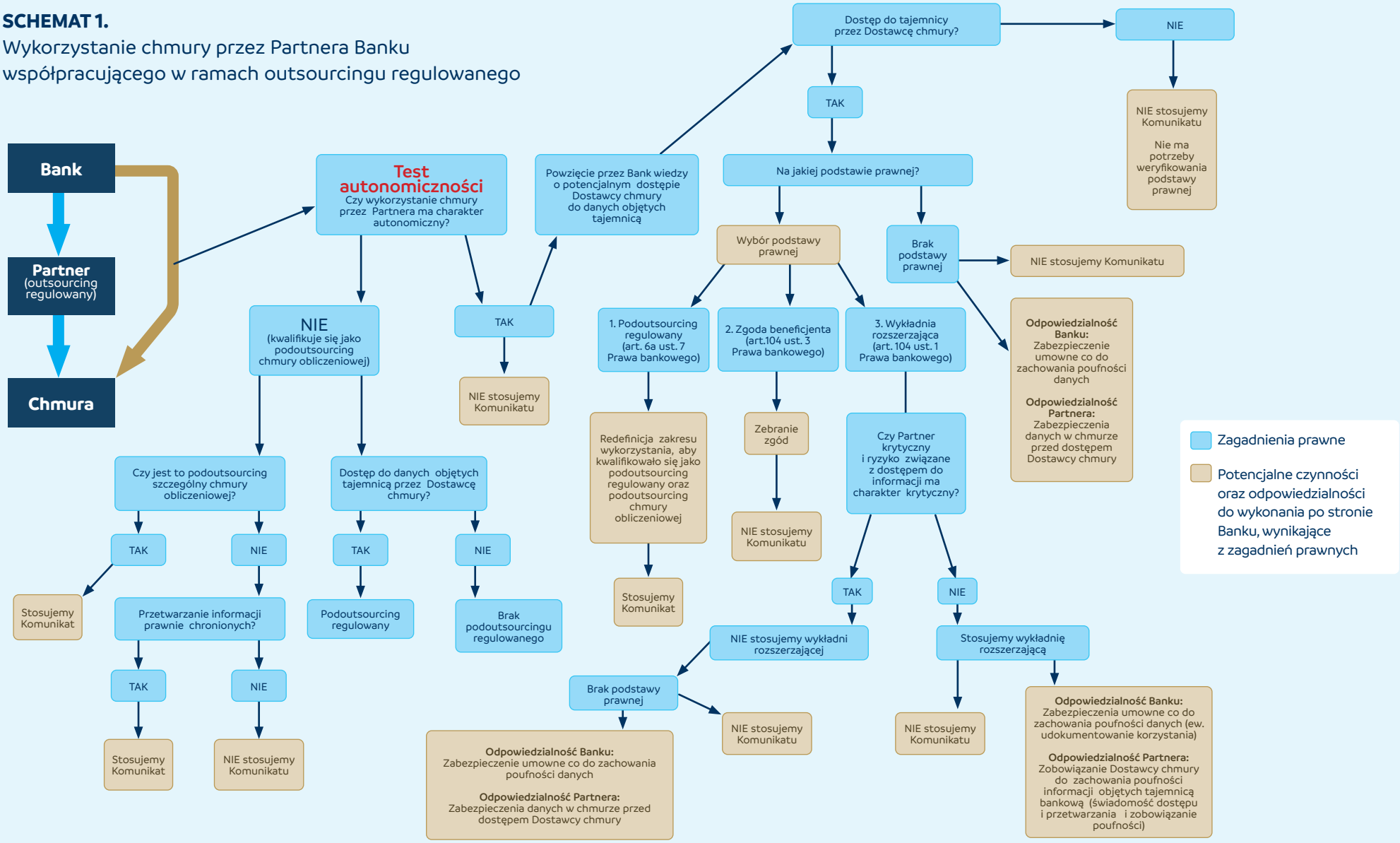
6.2. Opinia ogranicza się ściśle do spraw w niej poruszonych i nie należy dokonywać jej rozszerzenia na jakiekolwiek inne zagadnienia.

6.3. Proponowane rozwiązania mają charakter modelowy i pomocniczy – możliwość ich zastosowania w danym przypadku powinna zostać poprzedzona analizą okoliczności faktycznych i prawnych konkretnego przypadku. W związku tym opinia nie stanowi wiążącej porady prawnej dla któregokolwiek z jej odbiorców, a Kancelaria nie ponosi odpowiedzialności za działania podjęte w oparciu o jej treść.

r.pr. Szymon Ciach
Senior Associate
Kochański & Partners sp.k.

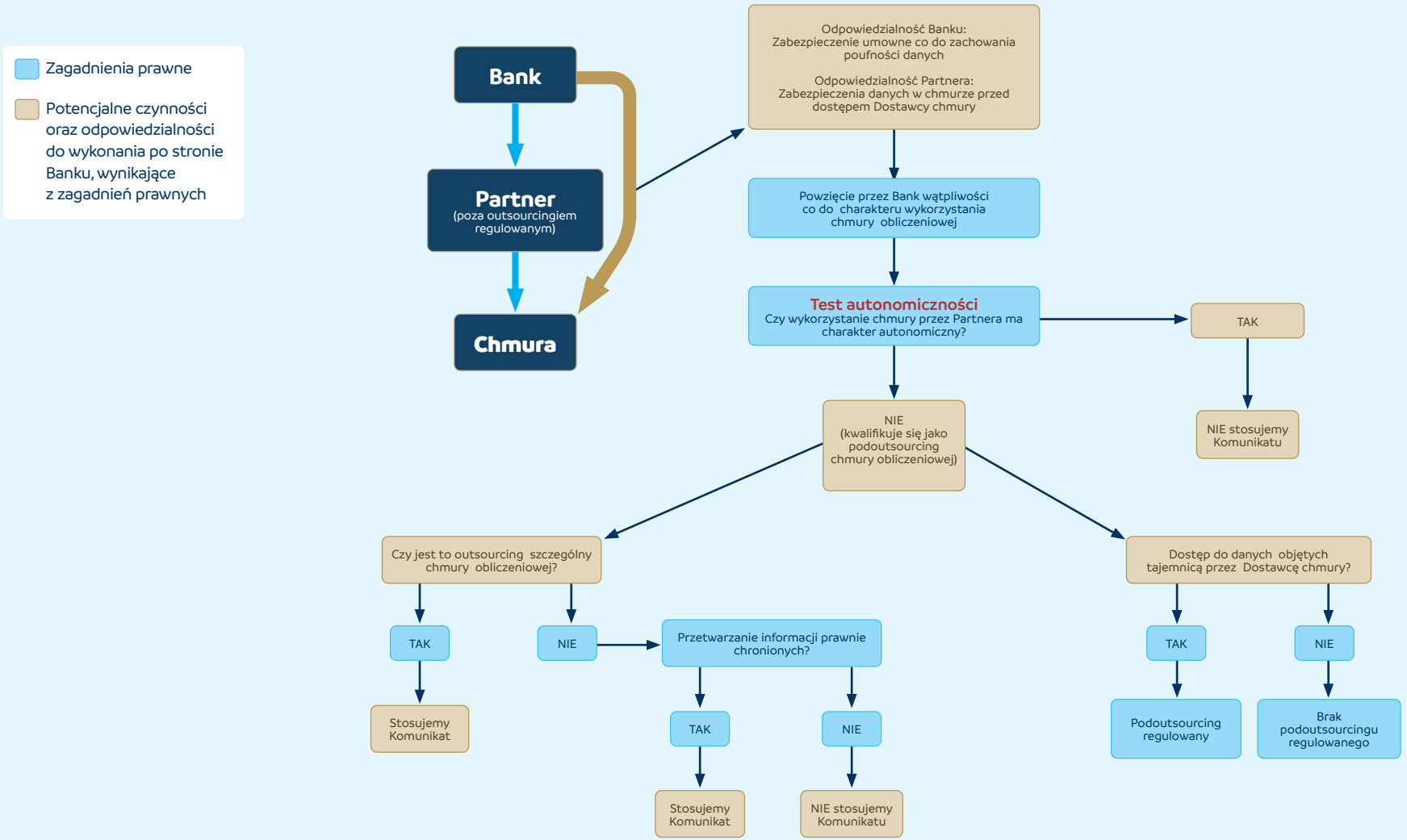
SCHEMAT 1.

Wykorzystanie chmury przez Partnera Banku współpracującego w ramach outsourcingu regulowanego



SCHEMAT 2.

Wykorzystanie chmury przez Partnera Banku współpracującego poza ramami outsourcingu regulowanego



Związek Banków Polskich