

Opis Przedmiotu Zamówienia

Przedmiotem Zamówienia jest wsparcie w zakresie uzyskania zgodności z wymaganiami zawartymi w „Komunikacie Urzędu Komisji Nadzoru Finansowego dotyczącym przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej” z dnia 23 stycznia 2020 roku, zwanym dalej „Komunikatem UKNF”, przy wdrożeniu usług obejmujących swoim zakresem:

1. Wysyłanie i podpisywanie dokumentów elektronicznie – usługa realizowana przez firmę Digital Gateways w oparciu o infrastrukturę chmury publicznej Microsoft Azure;
2. Zdalną weryfikację tożsamości – usługa realizowana przez firmę Digital Gateways w oparciu o infrastrukturę chmury publicznej Microsoft Azure;
3. Dostęp do informacji o rachunku, Account Information Service (PSD2) – usługa realizowana przez firmę Kontomatik w oparciu o infrastrukturę chmury GCP.

Doradztwo obejmuje w szczególności:

- 1) Analizę wewnętrznych regulacji Banku i zaproponowanie treści zmian tych regulacji lub wytworzenie nowych regulacji dopełniających obecnie istniejące regulacje i z nimi zgodnych, dostosowujących działalność Banku do procesów niezbędnych dla zgodności Banku z wymogami Komunikatu KNF,
- 2) Wytworzenie dokumentacji notyfikującej usługę chmurową w UKNF,
- 3) Wsparcie Banku w zakresie identyfikacji zagrożeń (lub uznaniu braku ich występowania) zgodnie z Komunikatem UKNF,
- 4) Ocenę ryzyka zidentyfikowanych zagrożeń (wpływ ryzyka na Bank i prawdopodobieństwo wystąpienia),
- 5) Wsparcie Banku w zakresie przygotowania planu zarządzania zidentyfikowanym ryzykiem i opisu mitygantów dla zidentyfikowanych ryzyk,
- 6) Weryfikację zgodności dokumentacji potwierdzającą spełnienie minimalnych wymagań przez dokumentację kontraktową posiadaną przez wybranego przez Bank dostawcę danej usługi (wykaz wymagań wraz ze wskazaniem sposobu spełnienia),
- 7) Wsparcie Banku w przygotowaniu dokumentacji potwierdzającej spełnienie minimalnych wymagań przez dostawcę w zakresie faktycznego sposobu świadczenia usługi (certyfikaty, deklaracje zgodności etc.),
- 8) Wsparcie Banku w przygotowaniu dokumentacji potwierdzającej spełnienie minimalnych wymagań przez Bank (plan ciągłości działania, przetwarzania informacji w chmurze obliczeniowej oraz zakończenia przetwarzania informacji).

I. Zagadnienia będące przedmiotem doradztwa prawnego:

1. doradztwo prawne w kwestiach dotyczących zgodności z Komunikatem UKNF, w tym w procesie przygotowania i złożenia informacji podmiotu nadzorowanego w sprawie przetwarzania informacji w chmurze obliczeniowej do UKNF;
2. bieżące doradztwo prawne, w tym w szczególności:
 - 1) w zakresie notyfikacji informacji nadzorczej do UKNF;
 - 2) oceny, w zakresie prawnym, dokumentów przekazywanych do UKNF w ramach projektu oraz dokumentów przygotowywanych w związku z zawiadomieniem KNF o zamiarze przetwarzania informacji w chmurze obliczeniowej;
4. wsparcie w zakresie zarządzania projektem od strony prawnej, w szczególności:
 - 1) zidentyfikowanie istotnych obszarów prawnych dla celów notyfikacji, zgodnie z Komunikatem UKNF oraz wskazanie sposobu ich zagospodarowania;
 - 2) doradztwo właściwym jednostkom Banku, w zakresie prawnym, przy przygotowaniu odpowiedniej dokumentacji.

II. Zagadnienia będące przedmiotem wsparcia przy tworzeniu dokumentacji:

1. W ramach wsparcia zostanie zapewniony udział przedstawicieli Wykonawcy w przygotowaniu dokumentacji wymaganej od podmiotu nadzorowanego, spełniającej wymagania Komunikatu UKNF. Dokumentacja to procedury, procesy i analizy, jakie Bank powinien przeprowadzić i udokumentować pod kątem przygotowania Banku do działania w sferze usług chmurowych w odniesieniu do poszczególnych zapisów wybranych regulacji. Zagadnienia będące przedmiotem wsparcia, to w szczególności:
 - 1) proces klasyfikacji informacji i aspekty przetwarzania informacji;
 - 2) opis ryzyk i ich skutków oraz mitygantów w procesie analizy ryzyka;
 - 3) ocena architektury rozwiązań dostawców;
 - 4) propozycja planów wycofania się z usługi;
 - 5) udokumentowanie wymagań w zakresie norm i standardów dla dostawcy usługi;
 - 6) scenariusze testowe usługi i ich przetestowanie;
 - 7) role pracowników i współpracowników (matryca RACI);
 - 8) plan przetwarzania informacji;
 - 9) pozostałe procedury lub/i procesy.

2. Pełna przewidywana zawartość repozytorium dokumentacji powstałej w ramach realizacji Przedmiotu Zamówienia:
 - 1) DOKUMENTACJA PROJEKTOWA
 - a. Architektura rozwiązania – dokument będzie dostarczony przez dostawców usług.
 - b. Plan wyjścia z usług chmury obliczeniowej.
 - c. Plan ciągłości działania.
 - d. Plan monitorowania bezpieczeństwa usług chmury obliczeniowej.
 - e. Plan monitorowania parametrów jakościowych funkcjonowania usług chmury obliczeniowej.
 - f. Plan przeprowadzenia testów usług chmury obliczeniowej.
 - 2) ORGANIZACJA PRACY I KOMPETENCJE
 - a. Zestawienie ról i podział odpowiedzialności osób uczestniczących we wdrożeniu i utrzymaniu usług chmury obliczeniowej.
 - b. Rejestr kompetencji personelu zaangażowanego w zarządzanie usługami chmurowymi.
 - c. Struktura organizacyjna w zakresie cyberbezpieczeństwa.
 - 3) DOKUMENTY FORMALNE
 - a. Umowa Outsourcingowa.
 - b. Kwalifikacja stosowania modelu referencyjnego UKNF.
 - c. Plan przetwarzania informacji w chmurze obliczeniowej.
 - d. Udokumentowanie istnienia Repozytorium Dokumentacji.
 - e. Zawiadomienie UKNF o przetwarzaniu informacji w chmurze obliczeniowej.
 - 4) KLASYFIKACJA INFORMACJI
 - a. Procedura przeprowadzania klasyfikacji i oceny informacji dla projektów wykorzystujących chmurę publiczną.
 - b. Procedura ponownej klasyfikacji i oceny informacji dla projektów wykorzystujących chmurę publiczną.
 - c. Wynik klasyfikacji oraz oceny informacji.
 - 5) SZACOWANIE RYZYKA
 - a. Procedura szacowania ryzyka dla projektów wykorzystujących chmurę publiczną na bazie istniejącej w Banku metodyki szacowania ryzyka.
 - b. Wyniki szacowania ryzyka.
 - c. Wniosek na Zarząd zatwierdzający wyniki szacowania ryzyka.

- 6) OCENA SPEŁNIENIA WYMOGÓW KOMUNIKATU UKNF
 - a. Ocena spełnienia wymagań Komunikatu UKNF względem umowy z dostawcą chmury obliczeniowej.
 - b. Ocena spełnienia wymagań normatywnych Komunikatu UKNF względem dostawcy chmury obliczeniowej.
 - c. Ocena spełnienia wymagań Komunikatu względem lokalizacji centrum przetwarzania danych dostawcy usług chmury obliczeniowej.
 - d. Ocena spełnienia wymagań Komunikatu w zakresie ochrony informacji przez dostawcę usług chmury obliczeniowej.
 - e. Ocena spełnienia wymagań Komunikatu UKNF względem szyfrowania informacji przetwarzanych w chmurze obliczeniowej.
 - f. Ocena spełnienia wymagań Komunikatu UKNF względem zarządzania ryzykiem.

- 7) POZOSTAŁE ZASADY, PROCEDURY I WYTYCZNE
 - a. Zasady zarządzania dostępem do usług chmury obliczeniowej dla dostawców zewnętrznych.
 - b. Zasady zarządzania kluczami szyfrującymi.
 - c. Zasady stosowanych zabezpieczeń technologicznych i rozwiązań organizacyjnych.
 - d. Zasady zarządzania ciągłością działania.
 - e. Zasady zgodności z prawem licencyjnym oraz regulacyjnym.
 - f. Zasady przeglądu i weryfikacji zarządczej systemu bezpieczeństwa związanego z użytkowaniem usług chmury obliczeniowej.