**PRZETWARZANIE INFORMACJI W CHMURZE OBLICZENIOWEJ ZGODNIE**

**Z KOMUNIKATEM UKNF Z 23 STYCZNIA 2020**

**– ZAŁOŻENIA METODYKI**

1. ZAŁOŻENIA OGÓLNE I ORGANZIACYJNE
   1. Metodyka ma zastosowanie w każdym wypadku, gdy informacje Zakładu Ubezpieczeń przetwarzane są, w jakimkolwiek zakresie, przy użyciu publicznej lub hybrydowej Chmury obliczeniowej bezpośrednio lub za pośrednictwem Dostawcy (podwykonawcy), niebędącym Dostawcą usługi chmury obliczeniowej, jednak korzystającego z Usług chmury obliczeniowej innego podmiotu.
   2. W przypadku gdy Dostawca usługi chmury obliczeniowej, korzysta z usług innego Dostawcy chmury obliczeniowej, proces należy realizować przy uwzględnieniu obu Usług chmurowych.
   3. Przypisanie ról i odpowiedzialności w procesie należy do Zakładu Ubezpieczeń. Należy zapewnić co najmniej:
      1. udział właściciela merytorycznego procesu co najmniej w zakresie zgromadzenia wymaganych informacji o procesie;
      2. udział przedstawicieli jednostek odpowiedzialnych za bezpieczeństwo, co najmniej w charakterze doradczym (opiniodawczym) na etapie szacowania ryzyka;
      3. udział przedstawicieli IT, co najmniej w charakterze doradczym (opiniodawczym) na etapie szacowania ryzyka technicznego (technologicznego);
      4. udział inspektora ochrony danych lub innej osoby wyznaczonej do nadzoru nad obszarem ochrony danych osobowych, co najmniej w charakterze doradczym (opiniodawczym) na etapie klasyfikacji informacji i szacowania ryzyka w zakresie zgodności z prawem ochrony danych osobowych.
   4. Należy zapewnić, by decyzja o postępowaniu z ryzykiem była podejmowana przez najwyższe kierownictwo Zakładu Ubezpieczeń lub osoby przez nie upoważnione.
   5. Należy zapewnić, by w każdym wypadku Zarząd Zakładu Ubezpieczeń posiadał wiedzę o rozpoczęciu korzystania z Usług chmury obliczeniowej.
   6. Wszystkie czynności w ramach realizacji metodyki powinny być dokumentowane w postaci pisemnej lub elektronicznej, w sposób zapewniający identyfikację osoby dokonującej czynności oraz integralność sporządzonej informacji
2. INWENTARYZACJA (OPIS PROCESU)
   1. Należy sporządzić opis planowanego procesu, w ramach którego wykorzystywana ma być Chmura obliczeniowa, określając możliwie precyzyjnie – co najmniej:
      1. przebieg poszczególnych etapów procesu biznesowego, w ramach którego zakłada się korzystanie z Chmury obliczeniowej, w tym określenie, możliwie szczegółowo i precyzyjnie, rodzaju przetwarzanych informacji i ich kategorii;
      2. skalę zakładanego przetwarzania, co najmniej przez wskazanie, czy skala jest mała, średnia czy duża, oraz wskazując przyjęte w tym zakresie kryteria;
      3. zakładaną architekturę rozwiązania, lub co najmniej wskazanie usług, z których Zakład Ubezpieczeń zamierza korzystać oraz zakładanej konfiguracji – o ile te informacje są dostępne.
3. KLASYFIKACJA INFORMACJI
   1. Celem klasyfikacji informacji jest zapewnienie, że informacje uzyskują ochronę na odpowiednim poziomie, z perspektywy związanych z nimi wymogami prawnymi oraz ich wagi.
   2. W praktyce klasyfikacje odnoszą się najczęściej do kryteriów: poufności, integralności i dostępności (zasad dostępu do informacji) z perspektywy skutków finansowych i regulacyjnych dla organizacji. Dobrą praktyką jest określenie ponadto ramowych minimalnych warunków zabezpieczeń obowiązujących w odniesieniu do poszczególnych klas informacji. (Przykład: Załącznik nr 1, Tabela nr 2)
   3. Zakład Ubezpieczeń powinien posiadać wdrożoną i stosowaną klasyfikację informacji, w oparciu o przyjęte przez siebie kryteria. Klasyfikacja może opierać się na kryterium określonym przez Zakład Ubezpieczeń, pod warunkiem że odzwierciedlać będzie ona co najmniej podział na informacje prawnie chronione w rozumieniu Komunikatu oraz pozostałe informacje.
   4. Niniejsza metodyka opiera się na następującej klasyfikacji:
      1. **Klasa A – informacje publiczne**
      2. **Klasa B – informacje wewnętrzne**
      3. **Klasa C – informacje ważne**
      4. **Klasa D – informacje szczególnie chronione**
      5. **Klasa E – informacje krytyczne**
   5. Zinwentaryzowane zgodnie z pkt 2 informacje należy przypisać do klas, przed przystąpieniem do procesu oceny informacji.
4. OCENA INFORMACJI

Cel: ustalenie czy w konkretnym analizowanym przypadku dopuszczalne jest korzystanie przez ZAKŁAD UBEZPIECZEŃ z chmury obliczeniowej

* 1. Ocena dokonywana jest w sposób usystematyzowany, w odniesieniu do konkretnej Usługi chmurowej i konkretnego procesu, podlegającego migracji do chmury.
  2. Ocena powinna obejmować – co najmniej:
     1. analizę występowania ograniczeń regulacyjnych mogących uniemożliwiać lub ograniczać korzystanie z Chmury obliczeniowej (np. ograniczenia terytorialne);
     2. analizę występowania ograniczeń kontraktowych, mogących uniemożliwiać lub ograniczać korzystanie z Chmury obliczeniowej (np. z uwagi na ograniczenia terytorialne, ograniczenia w zakresie korzystania z podwykonawców, itd.);
     3. analizę występowania ograniczeń wewnątrzorganizacyjnych (np. wewnętrzne procedury ograniczające możliwości korzystania z Chmury obliczeniowej dla określonych rodzajów informacji);
     4. ocenę występowania ewentualnych innych okoliczności prawnych lub biznesowych właściwych dla analizowanego przypadku i udokumentowania takich okoliczności
     5. określenie charakteru analizowanej informacji jako objętej lub nieobjętej tajemnicą (status informacji chronionej w rozumieniu Komunikatu)
     6. abstrakcyjną (tj. nieodnoszącą się do konkretnego zagrożenia) ocenę wpływu na bezpieczeństwo informacji w oparciu o przyjęte przez Zakład Ubezpieczeń kryteria; jako minimum ocena powinna odnosić się do skutków potencjalnego zagrożenia dla:
* reputacji,
* finansów,
* ciągłości działania Zakładu Ubezpieczeń oraz
* uprawnienia do prowadzenia działalności regulowanej przez Zakład Ubezpieczeń;
  + 1. stwierdzenie, w oparciu o dokonaną ocenę, czy proces obejmuje Outsourcing szczególny w rozumieniu Komunikatu;
    2. oszacowanie wartości informacji; dokonując oceny należy wziąć pod uwagę co najmniej następujące czynniki:
       - potencjalne kary finansowe związane z takim naruszeniem;
       - koszty związane z identyfikacją i usuwaniem naruszenia
       - koszty i utracone przychody (utrata klientów, utrata informacji o środkach materialnych i niematerialnych itp.)
       - koszty reputacyjne oraz wydatki poniesione na obszar public relations
    3. **rozstrzygnięcie o dopuszczalności (lub niedopuszczalności) korzystania z Chmury obliczeniowej oraz ewentualnie warunków takiego korzystania.**
  1. Klasyfikacja i ocena informacji powinna odbywać się cyklicznie, nie rzadziej niż raz na rok oraz za każdym razem:
     1. dla każdej planowanej do wykorzystania lub wykorzystywanej Usługi chmury obliczeniowej;
     2. dla każdego nowego rodzaju informacji który Zakład Ubezpieczeń zamierza przetwarzać w procesie;
     3. po wystąpieniu następujących zdarzeń: zmiana prawa, regulacji, regulaminów lub postanowień umów, które to zmiany mogą wpływać na zgodność postępowania podmiotu nadzorowanego w kontekście przetwarzania informacji w Chmurze obliczeniowej;
     4. zwiększenia lub zmniejszania skali przetwarzania informacji w procesie;
     5. w przypadku istotnego zwiększenia się wartości przetwarzanych informacji.

1. SZACOWANIE RYZYKA

Cel: identyfikacja ryzyk i zarządzenie nimi

* 1. Zakres szacowania ryzyka (poziom szczegółowości analizy) powinien być określony zgodnie z zasadą proporcjonalności. W każdym jednak wypadku należy uwzględnić kroki opisane w niniejszym rozdziale.
  2. Szacowanie ryzyka wymaga identyfikacji zagrożeń związanych z Chmurą obliczeniową, w szczególności zagrożeń wynikających z okoliczności wskazanych w rozdziale VI Komunikatu. Zagrożenia standardowo dotyczą w szczególności następujących obszarów ryzyka:
     1. lokalizacje przetwarzania (rozproszenie geograficzne);
     2. korzystanie z Usług chmury obliczeniowej w sposób inny niż zamierzony;
     3. dostęp do informacji chronionej;
     4. kontrola nad danymi (własność danych);
     5. podatności interfejsów, błędy konfiguracji;
     6. zakres szyfrowania;
     7. kompetencje techniczne;
     8. vendor lock-in;
     9. poddanie umowy prawu obcemu lub obcej jurysdykcji;
     10. ograniczona kontrola nad przebiegiem współpracy z Dostawcą;
     11. adhezyjność warunków umowy z Dostawcą.
  3. Identyfikując zagrożenie należy wskazać jego źródło (np. postanowienia umowy, dokumentacja bezpieczeństwa, dostępna publicznie informacja o stwierdzonych podatnościach usługi).
  4. Określone okoliczności mogą być źródłem zagrożenia z perspektywy prawnej, organizacyjnej lub technicznej lub każdej z nich równocześnie, co należy uwzględnić identyfikując i analizując zagrożenie.
  5. Każde zagrożenie powinno zostać ocenione pod kątem wpływu jego wystąpienia na aspekty wskazane w pkt 4.2.6. z uwzględnieniem przyjętych na jego podstawie kryteriów.
  6. Każde zagrożenie powinno zostać ocenione pod kątem poziomu prawdopodobieństwa jego wystąpienia. Oceniając poziom prawdopodobieństwa, Zakład Ubezpieczeń powinien wziąć pod uwagę co najmniej wiedzę historyczną nt. wystąpienia podobnych zagrożeń, dostępną ekspercką wiedzę w tym zakresie, oraz ustaloną zgodnie z pkt 4.2.8 wartość informacji,
  7. Poziomowi wpływu oraz poziomowi prawdopodobieństwa przypisuje się wartość liczbową, w celu ustalenia poziomu ryzyka początkowego, uzyskiwanego jako iloczyn tych dwóch wartości.
  8. Zakład Ubezpieczeń może zidentyfikować interakcje między zagrożeniami (ich wzajemne wzmocnienia) lub przypisać określonym obszarom dodatkową wagę (z uwagi na szczególne okoliczności dotyczące Zakładu Ubezpieczeń). W takim wypadku poziom ryzyka początkowego podlega odpowiedniemu podwyższeniu.
  9. Dla każdego ryzyka na poziomie innym niż niski, określa się środki zaradcze w postaci planu postępowania z ryzykiem, a następnie – poziom ryzyka szczątkowego. Dla każdego ryzyka szczątkowego określa się plan postępowania z ryzykiem (unikanie, redukcja, przenoszenie, akceptacja).
  10. Każde ryzyko powinno być monitorowane, a wyniki monitorowania – raportowane zgodnie z zasadami przyjętymi przez Zakład Ubezpieczeń.
  11. W celu zarządzania ryzykiem, określa się plan postępowania z ryzykiem, przypisując do poszczególnych ryzyk osoby odpowiedzialne za stosowanie środków zaradczych.
  12. Wyniki szacowania ryzyka powinny być przeglądane regularnie, nie rzadziej niż raz do roku, oraz w każdym przypadku zajścia istotnych okoliczności mogących wpływać na poziom ryzyka.

1. ZGROMADZENIE DOKUMENTACJI I WERYFIKACJA ZGODNOŚCI

CEL: zagregowanie wszystkich wymogów, rozliczalność procesu

* 1. W celu zapewnienia dostępności dokumentacji na wypadek kontroli organu nadzoru należy zgromadzić:
     1. dokumentację, wymaganą Komunikatem lub przepisami prawa tj. np. plan przetwarzania informacji w chmurze, plan ciągłości działania, exit plan itp.; oraz
     2. wypełniony szablon szacowania ryzyka wraz z dokumentacją stanowiącą podstawę szacowania ryzyka (np. umowa z Dostawcą, zamówione opinie prawne, wewnętrzna dokumentacja potwierdzająca posiadane kompetencje techniczne, dokumentacja środków bezpieczeństwa itd.).
  2. W zależności od potrzeb, należy zweryfikować kompletność procesu w oparciu o checklistę wymogów określonych w Komunikacie oraz przepisach sektorowych.

1. DECYZJA O ROZPOCZĘCIU KORZYSTANIA Z USŁUGI CHMURY OBLICZENIOWEJ
   1. Decyzję powinno podjąć najwyższe kierownictwo Zakładu Ubezpieczeń lub osoba przez nie upoważniona.
2. INFORMOWANIE UKNF O KORZYSTANIU Z USŁUGI CHMURY OBLICZENIOWEJ