KNF | KOMISJA NADZORU FINANSOWEGO

23 października 2017 r.

Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej

Wstęp

W związku z dużym postępem technologicznym i coraz powszechniejszym dostępem do usług przetwarzania danych w chmurze obliczeniowej[1] oraz zgłaszanymi potrzebami ze strony podmiotów nadzorowanych w tym zakresie, Urząd Komisji Nadzoru Finansowego (dalej: UKNF) identyfikuje konieczność przedstawienia stanowiska nadzoru w odniesieniu do specyfiki korzystania przez podmioty nadzorowane z przedmiotowych usług. Stanowisko poniższe dotyczy publicznego i współdzielonego modelu przetwarzania danych zawierających informacje prawnie chronione w chmurze obliczeniowej, jak również elementów chmury hybrydowej o takim charakterze. UKNF stoi na stanowisku, że usługa przetwarzania danych w chmurze obliczeniowej (dalej: Usługa) ma charakter – powierzenia wykonywania czynności – i tym samym podlega właściwym dla danego sektora usług finansowych przepisom prawa w tym zakresie. Przedstawione poniżej stanowisko stanowi uszczegółowienie wybranych dobrych praktyk i zaleceń zawartych w Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (dalej: Rekomendacja D), Rekomendacji D-SKOK dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska w spółdzielczych kasach oszczędnościowo-kredytowych oraz Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji, powszechnych towarzystwach emerytalnych, towarzystwach funduszy inwestycyjnych, podmiotach infrastruktury rynku kapitałowego, firmach inwestycyjnych w zakresie outsourcingu, w odniesieniu do specyfiki usług przetwarzania danych w chmurze obliczeniowej.

Realizacja czynności w ramach umów outsourcingu, powinna być zgodna z wymogami określonymi w przepisach prawa oraz innych regulacjach zewnętrznych obowiązujących w poszczególnych sektorach rynku finansowego.

W związku z ochroną tajemnic oraz informacji prawnie chronionych, podmioty nadzorowane powinny, w szczególności, uwzględnić okoliczność w jakim państwie usługodawca posiada siedzibę oraz w jakich państwach będzie on faktyczne wykonywał powierzone czynności, w kontekście systemu prawnego, który w tych państwach obowiązuje. Ochrona tajemnic oraz informacji, która w Polsce zagwarantowana jest również przez prawo karne, może doznawać

[1] Model świadczenia usług zapewniający niezależny od lokalizacji, dogodny dostęp sieciowy „na żądanie" do współdzielonej puli konfigurowalnych zasobów obliczeniowych (np. serwerów, pamięci masowych, aplikacji lub usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale dostawcy usług (na podstawie NIST Special Publication 800-145 „The NIST Definition of Cloud Computing", National Institute of Standards and Technology).

uszczerbku wówczas, gdy system prawny w państwie wykonywania czynności przez usługodawcę nie przewiduje podobnej ochrony, tj. takiej, w której naruszenie odpowiednich tajemnic jest penalizowane.

I. Identyfikacja potrzeb biznesowych, podstawa do podjęcia decyzji, planowanie

Nadzór oczekuje, że podmiot nadzorowany już w fazie planowania wykorzystania Usługi przeprowadzi prace umożliwiające osiągnięcie zgodności z obowiązującymi przepisami prawa i regulacjami zewnętrznymi. Od chwili rozpoczęcia korzystania z Usługi odpowiedzialność za zgodność jej funkcjonowania leży po stronie podmiotu nadzorowanego, dlatego przed podjęciem decyzji podmiot nadzorowany powinien zidentyfikować i określić w jaki sposób może spełnić obowiązujące wymagania prawne i nadzorcze. Podmiot nadzorowany powinien zaplanować przeprowadzanie systematycznej identyfikacji, monitorowania oraz raportowania w ramach systemu informacji zarządczej zgodności świadczonej przez dostawcę Usługi z wymaganiami dotyczącymi obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego wynikającymi z obowiązujących przepisów prawa, regulacji zewnętrznych i wewnętrznych, zawartych umów i przyjętych w podmiocie nadzorowanym standardów.
W fazie planowania wdrożenia Usługi i przygotowania do podjęcia decyzji podmiot nadzorowany powinien uwzględniać poniższe kwestie:

I.1

W ramach analizy kosztów i korzyści związanych z korzystaniem z Usługi należy przeprowadzić analizę SWOT tego rozwiązania, uwzględniając między innymi:

a) analizy innych (nie wykorzystujących technologii chmurowych) rozwiązań, które mogą być stosowane w planowanej lub bieżącej działalności biznesowej,
b) możliwość upadłości dostawcy lub jego nagłego wycofania się ze świadczenia Usługi,
c) koszty i granice możliwych do podjęcia działań w wypadku nagłego wycofania się dostawcy ze świadczenia Usługi lub ewentualnej rezygnacji podmiotu nadzorowanego z Usługi, w kontekście:

    - zwrotu danych i przejęcia przetwarzania powierzonych danych przez podmiot nadzorowany lub przekazania Usługi innemu dostawcy,
    - pozyskanej od dostawcy wiedzy o wadach i zaletach oraz ograniczeniach implementacyjnych i funkcjonalnych danej Usługi, w tym o ograniczeniach technologicznych i innych mających wpływ na możliwość migracji Usługi do innego dostawcy lub na możliwość kontynuowania powierzonych czynności samodzielnie,

d) wymagania z zakresu bezpieczeństwa i ochrony danych w odniesieniu do każdego poziomu bezpieczeństwa danych występującego w aktualnej klasyfikacji wykorzystywanej informacji, a także oszacowanej możliwości zmian tej klasyfikacji w przyszłości, mając na uwadze ograniczoną zdolność podmiotu nadzorowanego do wprowadzania nowych mechanizmów kontrolnych do Usługi,
e) model funkcjonowania wsparcia Usługi.

I.2

W ramach przygotowania do wdrożenia podmiot nadzorowany powinien w szczególności:

a) dysponować dokładną wiedzą odnośnie możliwości konfiguracji planowanej Usługi,
b) określić wymagania wynikające z obowiązujących przepisów prawa, regulacji zewnętrznych i wewnętrznych, zawartych umów i przyjętych w podmiocie nadzorowanym standardów, wymagania biznesowe, funkcjonalne i techniczne oraz warunki zapewnienia zgodności z tymi wymaganiami, w szczególności:
   - przeprowadzić inwentaryzację i klasyfikację informacji, które planuje się powierzyć dostawcy Usługi,
   - określić wymagania w zakresie bezpieczeństwa i ochrony danych w odniesieniu do każdego poziomu bezpieczeństwa występującego w klasyfikacji, zgodnie z obowiązującymi regulacjami (przepisami prawa, regulacjami zewnętrznymi, regulacjami wewnętrznymi).

Tryb prowadzenia prac w celu wdrożenia Usługi powinien zapewniać rozliczalność podejmowanych działań w kontekście ról, uprawnień, odpowiedzialności, harmonogramu, budżetu i jakości tych działań. Powinien on określać również zasady zarządzania ryzykiem, zmianą oraz wyznaczać warunki brzegowe zaniechania realizacji wdrożenia Usługi. Powinny zostać określone punkty i metody pomiaru efektywności działań właściwe dla każdego kontekstu ich prowadzenia.

II. Zarządzanie ryzykiem Usługi

Przed wdrożeniem Usługi podmiot nadzorowany powinien przeprowadzić kompleksowe oszacowanie ryzyka (identyfikacja, analiza, ocena) oraz przygotować plan postępowania z ryzykiem (w ujęciu norm ISO/IEC 27005:2011 i PN-ISO/IEC 27005:2011), uwzględniający wszystkie fazy życia Usługi, relację podmiotu nadzorowanego z dostawcą oraz wpływ włączenia Usługi do aktualnego systemu zarządzania bezpieczeństwem informacji (funkcjonującego w oparciu o dobre praktyki opisane w normach ISO/IEC 27001, PN-ISO/IEC 27001:2014-12 (certyfikacja nie jest wymagana), dalej: SZBI), uwzględniając w tym procesie m.in. specyficzne dla przetwarzania danych w chmurze obliczeniowej ryzyka, występujące zarówno po stronie dostawcy Usługi, jak i podmiotu nadzorowanego, wynikające, w szczególności, z następujących czynników:

a) rozproszenia geograficznego przetwarzanych lub przechowywanych danych w kontekście zapewnienia zgodności świadczonej Usługi z przepisami prawa obowiązującymi w Polsce, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi w podmiocie nadzorowanym standardami,
b) trybu i zakresu dostępu pracowników i podwykonawców dostawcy Usługi oraz potencjalnie stron trzecich do powierzonych danych, wynikającego zarówno z regulacji wewnętrznych dostawcy i podwykonawców, jak również przepisów prawa i regulacji zewnętrznych ich obowiązujących,
c) ograniczonego wpływu podmiotu nadzorowanego na kształt oraz zakres nowych funkcjonalności Usługi,
d) ograniczonej możliwości sprawowania kontroli nad działalnością dostawcy w zakresie świadczonej przez niego Usługi, polegającej na bezpośredniej weryfikacji

stosowanych przez dostawcę mechanizmów kontrolnych, w tym w zakresie środków ochrony i kontroli dostępu do pomieszczeń dostawcy, w których odbywa się świadczenie Usługi,

e) słabości mechanizmów izolacji zasobów wykorzystywanych do przetwarzania lub przechowywania danych przez dostawcę, jak również podatności interfejsów zarządzających Usługą udostępnianych jego klientom,
f) kształtu procesu usuwania powierzonych danych oraz braku bezpośredniej kontroli nad jego przebiegiem,
g) możliwości jednostronnego kształtowania i zmiany ceny oraz innych warunków świadczenia Usługi przez dostawcę w powiązaniu z długością okresu wypowiedzenia umowy,
h) pogorszenia jakości świadczenia Usługi w trybach lub zakresach nieuwzględnianych w SLA,
i) dostępu użytkowników do Usługi z sieci wewnętrznej podmiotu nadzorowanego i spoza tej sieci,
j) specyfiki mechanizmów zapewniających integrację Usługi z systemami podmiotu nadzorowanego – w tym z uwzględnieniem wszystkich dostępnych modeli uwierzytelniania do zasobów chmurowych oferowanych w ramach Usługi przez dostawcę,
k) korzystania z Usługi przy użyciu urządzeń mobilnych.

II.1

Podmiot nadzorowany powinien zarządzać ryzykami prowadzącymi do braku zgodności z przepisami prawa, regulacjami zewnętrznymi i wewnętrznymi oraz przyjętymi przez podmiot nadzorowany standardami poprzez stosowanie odpowiednich mechanizmów kontrolnych - takie ryzyka nie mogą być akceptowane ani transferowane.

II.2

Oszacowane poziomy ryzyka Usługi (przed i po zastosowaniu dodatkowych mechanizmów kontrolnych) powinny być przedmiotem porównania z właściwymi poziomami ryzyka rozwiązań teleinformatycznych niewykorzystujących tego rodzaju technologii. Wynik tego porównania powinien być uwzględniany jako istotna przesłanka przesądzająca o odstąpieniu od wdrożenia lub zaprzestaniu korzystania z Usługi.

Proces zarządzania ryzykiem Usługi powinien mieć charakter ciągły, działania monitorujące powinny skutecznie wskazywać moment koniecznego przeglądu ryzyka Usługi, w szczególności w przypadku zidentyfikowania nowego ryzyka oraz w przypadku istotnych zmian w trybie lub zakresie wykorzystania Usługi lub relacjach z dostawcą. Niezależnie od wyników monitorowania, przegląd ryzyka Usługi powinien być prowadzony regularnie (minimum raz w roku).

Podmiot nadzorowany powinien posiadać aktualną wiedzę o SZBI dostawcy i jego podwykonawców - w tym, w szczególności, zapewnić sobie wgląd w aktualną, regularną ocenę właściwych SZBI przez niezależnych ekspertów, wewnętrzne kontrole i audyt dostawcy i podwykonawców Usługi – jest to warunkiem efektywnego prowadzenia procesu zarządzania ryzykiem Usługi.

II.3

Podmiot nadzorowany powinien posiadać dokumenty potwierdzające poziom spełnienia wymagań dotyczących skuteczności mechanizmów kontrolnych po stronie dostawcy Usługi i jego podwykonawców, mitygujących ryzyka związane ze świadczoną Usługą, w tym:

a) wykaz obowiązków dostawcy wynikający z zapisów umowy, deklarację profesjonalnych kompetencji i/lub zabezpieczenie należytego wykonania umowy,
b) posiadane przez dostawcę certyfikaty zgodności z odpowiednimi międzynarodowymi normami i standardami np. ISO 27001, ISO 27017, ISO 27018, ISAE 3000, ISAE 3400, ISAE 3402, SSAE 16,
c) raporty z audytów dostawcy przeprowadzonych przez firmy trzecie na zlecenie dostawcy lub podmiotu nadzorowanego,
d) wyniki dotychczas przeprowadzonych wewnętrznych audytów dostawcy w zakresie Usługi,
e) plany działania dostawcy zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową, rozwiązania w zakresie Disaster Recovery, metody zapewnienia wysokiej dostępności Usługi, procedury wykonywania, przechowywania i archiwizacji kopii zapasowych,
f) ocena zapewnienia przez dostawcę odpowiedniej ochrony wykorzystywanych centrów danych, urządzeń komputerowych i telekomunikacyjnych,
g) ocena (w formie opinii prawnej), kiedy i pod jakimi warunkami, dostawca jest zobowiązany przekazać odpowiednie dane organom państw lub stronom trzecim (w oparciu o regulacje obowiązujące w kraju dostawcy) i jakie powiadomienie podejmuje się dostarczyć podmiotowi nadzorowanemu, w celu spełnienia zobowiązania, w szczególności w sytuacji kiedy dostawca, który pomimo deklaracji przetwarzania danych na terenie UE, będzie zobowiązany w określonych okolicznościach do przekazywania danych poza granice UE, z uwagi na prawo lokalne dla głównej siedziby dostawcy tudzież wykonywania przez niego działalności.

II.4

Podmiot nadzorowany powinien uwzględnić ryzyka związane z powierzeniem przez dostawcę Usługi wykonywania określonych czynności w zakresie Usługi jego podwykonawcom, w funkcjonującym w podmiocie nadzorowanym systemie zarządzania ryzykiem.

W przypadku uznania ryzyka za zbyt wysokie podmiot nadzorowany nie powinien akceptować wykorzystywania w ramach Usługi określonego podwykonawcy czy innych stron trzecich.

II.5

Podmiot nadzorowany powinien oszacować i zarządzać ryzykiem zakończenia współpracy z dostawcą w zakresie Usługi, w szczególności mając na uwadze możliwość nieoczekiwanego i nieplanowanego wycofania się dostawcy ze współpracy, np. w wyniku likwidacji firmy dostawcy lub zaprzestania przez niego świadczenia Usługi lub w wyniku decyzji podmiotu nadzorowanego. Podmiot nadzorowany powinien posiadać strategię dotyczącą zakończenia korzystania z Usługi i plan działań minimalizujących takie ryzyko.

Strategia zakończenia współpracy powinna uwzględniać m.in. następujące kwestie:

a) warunki umowy z dostawcą powinny umożliwiać podmiotowi nadzorowanemu bezpieczne zakończenie korzystania z Usługi, w tym zwrot danych w odpowiednim formacie, zakresie i trybie,
b) określenie działań dotyczących migracji danych, łącznie z harmonogramem, specyfikacją wymagań IT i bezpieczeństwa oraz potrzebnych narzędzi.

III. Wymagania dotyczące umowy z dostawcą

Umowa podmiotu nadzorowanego z dostawcą Usługi powinna zapewniać możliwość sprawowania kontroli nad działaniami dostawcy w zakresie wykorzystywanej Usługi, w szczególności powinna zawierać zapisy określające:

a) zakresy odpowiedzialności stron umowy,
b) zakres informacji i dokumentacji przekazywanych przez dostawcę w związku ze świadczeniem Usługi,
c) zapewnienie, że świadczenie Usługi odbywać się będzie zgodnie z wymaganiami obowiązujących przepisów prawa, regulacji zewnętrznych i wewnętrznych oraz przyjętych przez podmiot nadzorowany standardów,
d) możliwość modyfikacji warunków świadczenia Usługi, mechanizmy umożliwiające dokonywanie zmiany w zakresie oraz obszarach wykonywania umowy, rozszerzenia jej zakresu, dodawania nowych funkcjonalności,
e) warunki rozwiązania umowy,
f) okres wypowiedzenia umowy i procedury bezpiecznego zakończenia współpracy, w tym zwrotu oraz usunięcia danych,
g) prawo do przeprowadzenia audytu lub certyfikacji przez podmiot nadzorowany i upoważnione przez niego firmy trzecie, łącznie z prawem do przeprowadzenia inspekcji na miejscu w lokalizacjach przechowywania i przetwarzania danych,
h) możliwość wykonywania obowiązków kontrolnych przez organ nadzorczy,
i) gwarancje, rękojmie i kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej i procedur postępowania w takich sytuacjach,
j) zgodne z przepisami prawa określenie zakresu odpowiedzialności za szkody wyrządzone klientom,
k) uwzględnienie zasad licencjonowania i prawa do własności intelektualnej,
l) wskazanie języka, formy, warunków i przedmiotu Usługi oraz wsparcia Usługi,
m) zasady i tryb obsługi zgłoszeń dotyczących problemów w zakresie świadczonej Usługi,
n) obowiązek zapewnienia odpowiedniego poziomu bezpieczeństwa i ochrony powierzonych danych, określenia lokalizacji centrów, w których dane będą przechowywane i przetwarzane, ze szczególnym uwzględnieniem obsługi danych przez podwykonawców,
o) parametry jakości (w trybie SLA) Usługi oraz parametry ciągłości działania Usługi (RTO[2] i RPO[3]),
p) zasady wymiany i ochrony informacji, w tym warunki nadawania pracownikom podmiotów zewnętrznych praw dostępu do informacji,

[2] RTO (ang. Recovery Time Objective) – czas, w jakim należy przywrócić usługę po wystąpieniu awarii
[3] RPO (ang. Recovery Point Objective) – akceptowalny poziom utraty danych wyrażony w jednostkach czasu

q) wymagania dotyczące ochrony i bezpieczeństwa informacji, w tym dodatkowe warunki udzielania dostępu do informacji o wysokim stopniu poufności,
r) zapewnienie, że zadania, zakresy odpowiedzialności i rozliczalność działań wszystkich podwykonawców, agentów, pośredników i osób, które mają dostęp do danych i są zaangażowane w ich obsługę lub przetwarzanie, są transparentne i mogą być jasno identyfikowane przez podmiot nadzorowany na każdym kroku,
s) zasady w zakresie podoutsourcingu,
t) lista podwykonawców z lokalizacjami, kwalifikacja i zakres czynności świadczonych przez podwykonawców,
u) specyfikacja wymagań odnośnie procesów IT dostawcy, łącznie z zarządzaniem bezpieczeństwem, utrzymaniem i eksploatacją, rozwojem, jak również wymagania bezpieczeństwa w obszarze zarządzania zasobami ludzkimi,
v) procedury zarządzania incydentami i współpracy w tym zakresie, obejmujące zarówno pracowników podmiotu nadzorowanego, jak i dostawców Usługi oraz – w przypadku istotnego narażenia na skutki danego incydentu – również innych stron trzecich (klientów, kontrahentów itp.), zapewniające odpowiednio szybkie powiadamianie zainteresowanych stron i podejmowanie działań, adekwatnie do poziomu istotności incydentu;
w) realizację wsparcia Usługi przez dostawcę - podmiot nadzorowany powinien wziąć pod uwagę, że - ze względu na często globalny charakter usług świadczonych przez dostawcę - umowy mogą nie uwzględniać stref czasowych lub uwzględniać je w sposób niekorzystny dla podmiotu nadzorowanego i w związku z tym powinien zapewnić, by czas rozwiązywania problemów w ramach realizacji wsparcia był objęty gwarantowanym poziomem świadczenia Usługi.
x) jurysdykcję sądu oraz prawo właściwe dla umowy umożliwiające skuteczne dochodzenie roszczeń na gruncie umowy przez podmiot nadzorowany.

Podmiot nadzorowany powinien korzystać, jeżeli to możliwe, z oferowanych przez dostawcę rozszerzonych programów zapewnienia zgodności i bezpieczeństwa, umożliwiających w szczególności: bezpośredni kontakt i komunikację z oficerami bezpieczeństwa i pracownikami komórek ds. zgodności (compliance) po stronie dostawcy, korzystanie z rozszerzonego zakresu informacji o incydentach, dotyczących również infrastruktury dostawcy lub innych klientów dostawcy, które mogą mieć wpływ na bezpieczeństwo danych podmiotu nadzorowanego,

IV. Funkcjonowanie Usługi

IV.1
Podmiot nadzorowany, w celu skutecznego wypełnienia zobowiązań wynikających z odpowiedzialności za jakość i bezpieczeństwo usług świadczonych na rzecz klientów i kontrahentów oraz bezpieczeństwo ich danych, powinien, w szczególności, zapewnić sobie właściwy poziom eksperckiej wiedzy i umiejętności w celu przygotowania, wdrożenia, zarządzania, w tym kontrolowania wszystkich aspektów korzystania z Usługi.
Podmiot nadzorowany powinien zapewnić sobie, stały i bez istotnych ograniczeń wpływających na efektywność działania SZBI, kontakt z wyznaczonymi i odpowiednio

upoważnionymi przez dostawcę Usługi pracownikami, którzy są w pełni kompetentni do przekazywania wyjaśnień i informacji dotyczących działań dostawcy, jego procesów i procedur dotyczących zleconej Usługi przetwarzania danych oraz jej bezpieczeństwa.
Zasady współpracy pomiędzy podmiotem nadzorowanym a dostawcą Usługi powinny uwzględniać między innymi reguły w zakresie komunikacji i koordynacji wykonywanych przez dostawcę czynności (np. w zakresie przeprowadzania migracji danych, czynności konserwacyjnych, skanowania infrastruktury teleinformatycznej itp.), minimalizujące ich negatywny wpływ na jakość i bezpieczeństwo usług świadczonych przez podmiot nadzorowany.
Podmiot nadzorowany powinien w należyty sposób uwzględnić specyfikę Usługi w prowadzonych działaniach monitorujących, kontrolnych i audytowych w ramach SZBI.

IV.2

Podmiot nadzorowany powinien wdrożyć mechanizmy bezpieczeństwa i ochrony informacji w zakresie Usługi, jak również mechanizmy ochrony swoich zasobów i infrastruktury IT związanych z korzystaniem z Usługi – w postaci działań włączonych w sformalizowany system zarządzania środowiskiem teleinformatycznym podmiotu nadzorowanego.
Podmiot nadzorowany powinien regularnie uzyskiwać od dostawcy potwierdzenie świadczenia Usługi zgodnie z wymaganiami bezpieczeństwa i ochrony danych – minimum raz w roku lub po każdej istotnej zmianie w powiązanych procesach biznesowych, usługach, konfiguracji lub otoczeniu prawnym.

IV.3

W celu spełnienia wymagań dotyczących bezpieczeństwa informacji podczas transmisji należy zapewnić, że transmisje danych pomiędzy podmiotem nadzorowanym a infrastrukturą dostawcy, pomiędzy zasobami w infrastrukturze dostawcy i pomiędzy infrastrukturą dostawcy a innymi zewnętrznymi dostawcami usług są chronione przed nieautoryzowanym dostępem i modyfikacją oraz że zapewniona jest dostępność i oczekiwana przepustowość ruchu sieciowego.
W celu spełnienia określonych wyżej wymagań podmiot nadzorowany i dostawca w ramach swoich zakresów kompetencji zapewniają m.in.:

a) szyfrowanie i ochronę integralności transmitowanych i przechowywanych danych za pomocą nieskompromitowanych metod,
b) silne uwierzytelnienie użytkowników uprzywilejowanych oraz uwierzytelnienie urządzeń w celu transmisji danych,
c) wysoką dostępność połączeń sieciowych i odpowiednią, wymaganą przepustowość.

IV.4

Podmiot nadzorowany i dostawca Usługi powinni zapewnić w szczególności następujące elementy systemu zarządzania bezpieczeństwem przetwarzanych informacji:

a) spójne wprowadzanie wymagań dotyczących bezpieczeństwa danych w zakresie posiadanych kompetencji, dla przykładu poprzez ustanowienie adekwatnego poziomu kontroli dostępu,
b) zdefiniowanie parametrów dostępności danych zgodnych z parametrami RTO i RPO procesów biznesowych korzystających z Usługi,
c) uzgodnienie sposobów bezpiecznego usuwania przetwarzanych danych (łącznie z kopiami zapasowymi i danymi zgromadzonymi w archiwach, kopiach i snapshotach

maszyn wirtualnych, itp.) i zobowiązanie dostawcy do przeprowadzenia i udokumentowania, na wniosek podmiotu nadzorowanego, powyższych czynności,

d) zapewnienie zgodności Usługi, w zakresie kompetencji dostawcy, z wymaganiami podmiotu nadzorowanego dotyczącymi bezpieczeństwa powinno uwzględniać aspekty poufności, integralności i dostępności informacji oraz rozliczalności działań użytkowników,
e) podmiot nadzorowany powinien zapewnić niezależną od oferowanej w ramach Usługi lokalizację składowania kopii zapasowych danych uznanych za krytyczne na podstawie właściwej klasyfikacji informacji w podmiocie nadzorowanym oraz powinien określić tryb i zakres przekazywania kopii oraz format przechowywanych danych.

IV.5

Podmiot nadzorowany powinien zapewnić sobie niezbędną wiedzę o procesie zarządzania incydentami dostawcy Usługi oraz jego podwykonawców w celu wykorzystania jej w procesie zarządzania ryzykiem Usługi, w szczególności do analizy ryzyka oraz przygotowania planu postępowania z ryzykiem.

Wszelkie zmiany zachodzące w procesach zarządzania incydentami dostawcy Usługi oraz jego podwykonawców powinny być bezzwłocznie notyfikowane podmiotowi nadzorowanemu, w trybie i zakresie umożliwiającym efektywne działanie SZBI podmiotu nadzorowanego.

Tryb i zakres procesów zarządzania incydentami dostawcy Usługi i jego podwykonawców oraz zasady współpracy w przypadku wystąpienia incydentu powinny zapewnić podmiotowi nadzorowanemu, że świadczenie Usługi przez dostawcę odbywać się będzie zgodnie z wymaganiami obowiązujących przepisów prawa, regulacji zewnętrznych i wewnętrznych oraz przyjętych przez podmiot nadzorowany standardów.

W szczególności, podmiot nadzorowany powinien uzyskać zapewnienie, że dostawca Usługi i jego podwykonawcy:

a) rejestrują oraz przechowują informacje o zdarzeniach wpływających negatywnie na zachowanie atrybutów bezpieczeństwa informacji (poufności, integralności, dostępności) oraz że dostęp do tej informacji jest odpowiednio zarządzany i monitorowany,
b) posiadają odpowiednie procedury reakcji na te zdarzenia, w tym analizy scenariuszy istotnych zagrożeń,
c) stosują format danych oraz mechanizm przekazywania informacji dot. incydentu spełniający określane przez podmiot nadzorowany wymagania,
d) posiadają zasady obejmujące potencjalną integrację z systemami wsparcia zarządzaniem zdarzeniami i incydentami podmiotu nadzorowanego w trybie i zakresie wynikającym z właściwych planów postępowania z ryzykiem podmiotu nadzorowanego w kontekście efektywnego funkcjonowania wskazanych tam mechanizmów kontrolnych,
e) będą niezwłocznie przekazywać podmiotowi nadzorowanemu informacje o wszelkich incydentach mogących bezpośrednio lub pośrednio zagrozić bezpieczeństwu powierzonych im danych, w trybie i zakresie umożliwiającym efektywne działanie SZBI podmiotu nadzorowanego,

f) na każde żądanie podmiotu nadzorowanego będą niezwłocznie przekazywać wszelkie informacje o aktualnie prowadzonych i projektowanych działaniach w związku z postępowaniem z incydentem,
g) zapewnią przekazanie raportu z incydentu, zgodnego z wymaganiami SZBI podmiotu nadzorowanego, zawierającego m.in. opis podejmowanych działań naprawczych oraz zapobiegawczych,
h) zapewnią, że każde zdarzenie dostępu pracownika dostawcy Usługi lub jego podwykonawcy, niezwiązane ze zleconymi w ramach umowy Usługi czynnościami, będzie niezwłocznie traktowane i raportowane podmiotowi nadzorowanemu jako incydent,
i) posiadają efektywny proces i zasady gromadzenia i zabezpieczania dowodów związanych z incydentami, które będą mogły zostać wykorzystane w ewentualnych postępowaniach sądowych oraz dostarczą je w miarę możliwości na żądanie podmiotu nadzorowanego między innymi w postaci śladów audytowych czynności związanych z powierzonymi danymi w postaci np. odpowiednio posegregowanych zapisów w logach, kopiach obrazów lub stanów maszyn wirtualnych.

V. Zakończenie współpracy z dostawcą Usługi

Podmiot nadzorowany powinien posiadać odpowiedni plan działania na wypadek wystąpienia błędów lub niewłaściwego funkcjonowania Usługi, jak również posiadać oraz testować w ramach procesu zarządzania ciągłością działania, rozwiązania zapewniające ciągłość działania procesów realizowanych przez Usługę.
Istotnym aspektem zarządzania ryzykiem zakończenia współpracy z dostawcą Usługi jest również posiadanie efektywnego planu działania, uwzględniającego między innymi:

a) warunki umowy z dostawcą, które powinny umożliwiać podmiotowi nadzorowanemu bezpieczne zakończenie świadczenia Usługi, w tym zwrot danych w odpowiednim formacie, trybie i czasie,
b) oszacowany wpływ zakończenia współpracy z dostawcą Usługi na funkcjonowanie procesów biznesowych wykorzystujących Usługę na wypadek przerwania jej świadczenia przez dostawcę lub podmiot nadzorowany,
c) sposób migracji danych, łącznie z harmonogramem, specyfikacją wymagań środowiska teleinformatycznego i bezpieczeństwa oraz potrzebnych narzędzi, wpływ na strukturę organizacyjną, procesy zarządzania środowiskiem teleinformatycznym i jego bezpieczeństwem.

V.1
W celu ograniczenia ryzyka związanego z zakończeniem współpracy z dostawcą w zakresie Usługi podmiot nadzorowany powinien zapewnić potrzebny personel, środki techniczne i technologie, w szczególności:

a) infrastrukturę wymaganą do efektywnego przetwarzania zwróconych danych w taki sposób, by procesy wykorzystujące Usługę mogły funkcjonować bez przestojów, a ewentualne przerwanie ciągłości ich działania nie naruszałoby właściwych dla nich parametrów ciągłości działania,

b) zespół projektowy niezbędny do przeprowadzenia wdrożenia i kontynowania powierzonych wcześniej czynności samodzielnie lub powierzenia ich innemu dostawcy,
c) szczegółowy plan wdrożenia działań związanych z zaprzestaniem korzystania z Usługi, uwzględniający najbardziej niekorzystne scenariusze zdarzeń, harmonogram czynności z określonymi zasobami, kamieniami milowymi oraz podziałem odpowiedzialności, wymagane narzędzia, konieczne scenariusze testowe oraz kryteria akceptacji testów czynności przetwarzania danych przejętych z powrotem przez podmiot nadzorowany lub przekazanych innemu dostawcy.