Ministerstwo Cyfryzacji

Projekt Rekomendacji Ministra Cyfryzacji dotyczących warunków technicznych i organizacyjnych powierzenia danych administracji publicznej do przetwarzania w publicznej chmurze obliczeniowej

Projekt 2018.07.09

Spis treści

1. Zakres stosowania rekomendacji

1. Rekomendacje powinny być stosowane podczas formułowania warunków zamówienia zawierających lub dopuszczających wykorzystanie przetwarzania danych w chmurze obliczeniowej poza zasobami technicznymi administracji publicznej.
2. Rekomendacje powinny być stosowane podczas formułowania klauzul w umowach zawieranych z Dostawcą usług dotyczących przetwarzania w chmurze obliczeniowej.
3. Rekomendacje określają minimalny zakres obowiązków i koniecznych dostosowań organizacyjnych po stronie Zamawiającego w przypadku korzystania z usług świadczonych w chmurze obliczeniowej.
4. W każdym z przypadków wymagane będzie po stronie Zamawiającego zastosowanie dodatkowych, adekwatnych do danej sytuacji, środków i mechanizmów wynikających z przeprowadzonej analizy ryzyka.

2. Definicje

1. Publiczna chmura obliczeniowa – usługa zapewnienia przetwarzania danych, w ramach której:
    a. przetwarzanie opiera się na zasobach technicznych, nie będących własnością Zamawiającego i pozostających poza kontrolą organów administracji publicznej, z wyjątkiem mechanizmów kontroli zawartych w umowie świadczenia usług;
    b. Dostawca jest technicznie, prawnie i organizacyjnie przygotowany do świadczenia usług dla więcej niż jednego odbiorcy, w tym podmiotów nie będących jednostkami administracji publicznej;
    c. świadczenie usług opiera się na ustandaryzowanym katalogu skalowalnych usług infrastrukturalnych, platformowych lub oprogramowania, oferowanych zarówno podmiotom publicznym jak i komercyjnym, a także osobom fizycznym;
    d. usługi udostępniane są zdalnie przez sieć Internet, bez technicznych ograniczeń terytorialnych po stronie Zamawiającego i użytkownika;

e. płatność za usługę realizowana jest w modelu subskrypcyjnym, a opłata zależy od rzeczywistego wykorzystania, które może być zmienne;

f. zarządzanie zasobami fizycznymi leży całkowicie po stronie Dostawcy i jest oparte o koncepcję skalowalnych pul zasobów współdzielonych bez odwołań kontraktowych do fizycznych egzemplarzy urządzeń, ich konfiguracji, modeli ani typów sprzętu.

2. Dostawca – podmiot będący usługodawcą usług publicznej chmury obliczeniowej, odpowiedzialny za zapewnienie parametrów funkcjonalnych i technicznych, w tym poufności, integralności i dostępności oferowanego rozwiązania chmurowego.
3. Zamawiający – jednostka administracji publicznej.
4. Modele świadczenia usług w chmurze:
   a. IaaS (*Infrastrukture as a Service*) – usługi o charakterze infrastrukturalnym, np. hosting serwerów, macierzy, sieci;
   b. SaaS (*Software as a Service*) – usługi oprogramowania, np. chmurowe systemy CRM, systemy do zarządzania projektami, portale zarządzania dokumentami;
   c. PaaS (*Platform as a Service*) – usługi o charakterze platformowym, np. usługi baz danych i serwerów aplikacyjnych.

3. Kryteria równoważności przetwarzania w chmurze

1. Przetwarzanie danych w chmurze publicznej może zostać uznane za równoważne do przetwarzania w zasobach technicznych jednostki administracji publicznej po kontraktowym zagwarantowaniu i spełnieniu następujących warunków:
   a. zawarciu z Dostawcą, w części dotyczącej przetwarzania danych w chmurze obliczeniowej, umowy o świadczenie usług – wymaganej ze względu na fakt, że usługi przetwarzania danych w chmurze obliczeniowej mają charakter powierzenia wykonywania poszczególnych czynności (tym samym podlegają one właściwym przepisom prawa w zakresie powierzenia realizacji tych czynności);
   b. spełnieniu przez Dostawcę oraz przez jego rozwiązania techniczne i organizacyjne, wymagań przewidzianych dla systemu zarządzania bezpieczeństwem informacji zawartych w aktualnych normach PN ISO/IEC 27001 oraz PN ISO/IEC 27002 wraz z dodatkowymi zabezpieczeniami przewidzianymi przez aktualne normy PN ISO/IEC 27017 i PN ISO/IEC 27018 (spełnienie wymagań jest potwierdzone raportami z regularnych audytów zewnętrznych bądź odpowiednimi certyfikatami wydanymi przez akredytowane organizacje).
2. <u>Niedopuszczalne jest:</u>
   a. <u>korzystanie z usług w publicznej chmurze obliczeniowej na podstawie nieuregulowanych kontraktowo opcji umów licencyjnych;</u>
   b. przetwarzanie w publicznej chmurze obliczeniowej informacji objętych ustawą o ochronie informacji niejawnych;

c. przetwarzanie w publicznej chmurze obliczeniowej rejestrów publicznych powołanych na mocy ustawy oraz zbiorów danych administracji, których zawartość i publikacja wywołuje bezpośrednio skutki prawne.

3. Niniejsze Rekomendacje nie wyłączają stosowania przepisów regulujących dopuszczalność przetwarzania w chmurze szczególnych kategorii danych, w tym danych medycznych i innych danych wrażliwych.

4. Planowanie przetwarzania w chmurze obliczeniowej

1. Przed rozpoczęciem przetwarzania danych w publicznej chmurze obliczeniowej, w ramach procesu planowania należy co najmniej:
   a. określić wymagania biznesowe, funkcjonalne i techniczne wynikające z obowiązujących przepisów prawa, regulacji zewnętrznych oraz regulacji wewnętrznych Zamawiającego, zawartych umów i standardów przyjętych u Zamawiającego;
   b. przeprowadzić analizę kosztów i korzyści związanych z korzystaniem z usług publicznej chmury obliczeniowej;
   c. przeprowadzić analizę mającą na celu porównanie pełnych kosztów rozwiązań chmurowych oraz pełnych kosztów uruchomienia rozwiązania we własnych zasobach Zamawiającego;
   d. uzyskać potwierdzenie braku możliwości realizacji czynności (które mają być przedmiotem przekazania do rozwiązań chmurowych) przez inną jednostkę administracji publicznej świadczącą usługi o charakterze usług chmurowych lub uzyskać potwierdzenie, że usługa taka nie jest i nie będzie świadczona przez inne jednostki administracji publicznej w planowanym okresie realizacji przedsięwzięcia (projektu) Zamawiającego;
   e. przeprowadzić szacowanie ryzyka oraz zapewnić w szczególności, że analiza ryzyka bierze pod uwagę aspekty odpowiedzialności Dostawcy w zależności od wybranego wariantu usług chmurowych – Infrastruktury (IaaS), Platformy (PaaS) lub Oprogramowania (SaaS);
   f. ocenić przygotowanie Zamawiającego do wypełnienia ról przewidzianych dla Zamawiającego w ramach realizacji współpracy z Dostawcą usług chmurowych – w szczególności ocenić możliwości zapewnienia odpowiednio wykwalifikowanego personelu w celu kontroli adekwatności realizacji zleconych usług, nadzoru nad realizacją zleconych usług, nadzoru nad zapewnieniem bezpieczeństwa przekazanych danych, analizy dzienników zdarzeń i innych informacji, których przekazania Zamawiający wymaga od Dostawcy;
   g. dokonać analizy skutków oraz analizy kosztów i możliwości podjęcia działań w sytuacji potencjalnej upadłości Dostawcy, nagłego wycofania się Dostawcy ze świadczenia usług publicznej chmury obliczeniowej lub ewentualnej rezygnacji Zamawiającego z korzystania z tych usług, w szczególności mając na uwadze:
      i. możliwości zwrotu powierzonych danych;
      ii. możliwości przekazania świadczenia usług innemu Dostawcy;

iii. możliwości pozyskania od Dostawcy wiedzy o stosowanym rozwiązaniu (w tym ograniczeniach implementacyjnych, funkcjonalnych, technologicznych), która może być istotna w sytuacji migracji usług do innego Dostawcy lub w przypadku realizowania czynności samodzielnie przez Zamawiającego;

h. przeprowadzić inwentaryzację i klasyfikację informacji, które planuje się powierzyć Dostawcy;

i. określić wymagania w zakresie bezpieczeństwa i ochrony danych w odniesieniu do każdego poziomu bezpieczeństwa występującego w klasyfikacji;

j. dokonać analizy wymagań z zakresu bezpieczeństwa i ochrony powierzanych danych, mając na uwadze ograniczone możliwości Zamawiającego do wprowadzania nowych mechanizmów kontrolnych do usług świadczonych przez Dostawcę;

k. przeprowadzić analizę wpływu na ochronę danych osobowych (ocena skutków na ochronę danych), w której należy uwzględnić wszystkie zagrożenia i podatności mające wpływ na bezpieczeństwo przetwarzanych danych osobowych oraz zgodność z wymogami prawnymi związanymi z ochroną danych osobowych;

l. dokonać oceny możliwości i potencjału Dostawcy pod kątem możliwości realizacji powierzanych czynności (przykładowo, kompetencje Dostawcy można oceniać na podstawie dotychczas zrealizowanych przez Dostawcę podobnych usług, uzyskanych przez Dostawcę niezależnych certyfikacji, w szczególności w zakresie bezpieczeństwa informacji i ochrony danych osobowych);

m. dokonać analizy zasad funkcjonowania wsparcia technicznego ze strony Dostawcy dla świadczonych usług publicznej chmury obliczeniowej.

2. Potwierdzenie przeprowadzenia weryfikacji powyższych punktów powinno zostać udokumentowane.

3. Przed rozpoczęciem przetwarzania danych w publicznej chmurze obliczeniowej planowane rozwiązanie wykorzystujące chmury obliczeniowe powinno zostać zweryfikowane i zaakceptowane przez osoby, świadczące pracę lub usługi na rzecz Zamawiającego, odpowiedzialne za bezpieczeństwo informacji oraz ochronę danych osobowych (Inspektora Ochrony Danych Osobowych).

5. Zarządzanie ryzykiem

1. Przed rozpoczęciem korzystania z usług chmurowych Zamawiający powinien przeprowadzić kompleksowe oszacowanie ryzyka (identyfikacja, analiza, ocena) oraz przygotować plan postępowania z ryzykiem, uwzględniający w szczególności wszystkie fazy realizacji planowanego przedsięwzięcia (projektu), relację Zamawiającego z Dostawcą oraz wpływ włączenia planowanego przedsięwzięcia (projektu) do aktualnie posiadanego systemu zarządzania bezpieczeństwem informacji.

2. W szczególności należy uwzględnić ryzyka specyficzne dla przetwarzania danych w chmurze obliczeniowej, występujące zarówno po stronie Zamawiającego, jak również po stronie Dostawcy, związane z:

a. zakresem oraz ilością i kategoriami przetwarzanych danych osobowych (w szczególności przetwarzanie dużych ilości danych pociąga za sobą wyższe poziomy ryzyka);

b. rozproszeniem geograficznym przetwarzanych danych w kontekście zapewnienia zgodności z przepisami prawa obowiązującymi w Polsce, regulacjami zewnętrznymi oraz regulacjami wewnętrznymi Zamawiającego;

c. bezpieczeństwem danych osobowych, w tym ryzyka mające wpływ na prawa i wolności osób, których te dane dotyczą (ocena skutków na ochronę danych[1]);

d. poszczególnymi czynnościami przetwarzania danych osobowych (w szczególności czynności związane z „profilowaniem" danych osobowych pociągają za sobą wyższe poziomy ryzyka);

e. bezpieczeństwem danych przesyłanych przez sieć internet (ryzyka związane z możliwością nieautoryzowanego dostępu lub modyfikacji przesyłanych danych) – możliwe mechanizmy bezpieczeństwa to na przykład wykorzystywanie dedykowanych połączeń, sieci VPN (Virtual Private Network), szyfrowanie połączeń (np. HTTPS z implementacjami TLS);

f. brakiem lub ograniczeniem łączności poprzez sieć internet (ryzyka związane z ograniczeniem komunikacji, np. wskutek błędnego zaplanowania wymaganej przepustowości, przeciążenia lub awarii po stronie operatora telekomunikacyjnego, ataków typu DDoS) – możliwe mechanizmy bezpieczeństwa to na przykład wykorzystywanie redundantnych łączy od różnych operatorów telekomunikacyjnych;

g. słabością kontroli dostępu i zarządzania uprawnieniami użytkowników, w tym związane z zakresem dostępu pracowników i podwykonawców Dostawcy oraz potencjalnie stron trzecich do powierzonych danych, wynikającego zarówno z regulacji wewnętrznych Dostawcy, jak również z przepisów prawa i regulacji zewnętrznych obowiązujących w kraju, w którym Dostawca przetwarza dane (ryzyka związane z możliwością dostępu do danych przez organy państwowe kraju, w którym Dostawca przetwarza dane);

h. specyfiką mechanizmów zapewniających integrację planowanego przedsięwzięcia (projektu) z systemami Zamawiającego – w tym z uwzględnieniem dostępnych modeli uwierzytelniania do zasobów chmurowych oferowanych w ramach świadczonych usług przez Dostawcę;

i. fizyczną lokalizacją centrów przetwarzania danych (ryzyka związane z umiejscowieniem fizycznych centrów przetwarzania danych w wielu krajach bądź w krajach uniemożliwiających Zamawiającemu weryfikację bezpieczeństwa przetwarzanych danych, ryzyka związane z systemami prawnymi obowiązującymi w krajach, w których przetwarzane są dane Zamawiającego, np. określającymi inne zasady ochrony danych niż obowiązujące w Polsce) – możliwe mechanizmy bezpieczeństwa to na przykład ograniczenie przetwarzania danych wyłącznie do terytorium Unii Europejskiej (w tym również przez podwykonawców Dostawcy), zakaz ujawniania danych organom państw, w których przetwarzane są dane Zamawiającego, o ile nie wynika to wprost z przepisów obowiązującego prawa lub z umowy zawartej pomiędzy Zamawiającym i Dostawcą;

[1] Urząd Ochrony Danych Osobowych udostępnił wytyczne dotyczące oceny skutków dla ochrony danych – https://uodo.gov.pl/pl/10/9.

j. vendor lockingiem (uzależnieniem od konkretnego dostawcy usług bądź od konkretnego producenta sprzętu lub oprogramowania) – możliwe mechanizmy bezpieczeństwa to w szczególności opracowanie i regularne testowanie planów migracji przetwarzania danych do środowiska innego Dostawcy lub Zamawiającego;

k. ograniczoną możliwością sprawowania kontroli nad działalnością Dostawcy w zakresie świadczonych przez niego usług;

l. brakiem lub słabościami odizolowania środowiska przetwarzania danych Zamawiającego od środowisk innych Klientów Dostawcy (ryzyka związane z wykorzystywaniem przez Dostawcę jednego środowiska teleinformatycznego do świadczenia usług dla wielu Klientów, co może skutkować ujawnieniem danych jednego Klienta innemu Klientowi) – możliwe mechanizmy bezpieczeństwa to w szczególności fizyczne odseparowanie środowisk;

m. podatnościami po stronie oprogramowania użytkownika – możliwe mechanizmy bezpieczeństwa to w szczególności wykorzystywanie szyfrowania komunikacji (np. HTTPS, SFTP), wykorzystywanie zdalnego pulpitu do połączeń z dedykowanymi serwerami;

n. procesem usuwania powierzonych danych oraz brakiem bezpośredniej kontroli nad jego przebiegiem;

o. możliwością jednostronnego kształtowania i zmiany warunków świadczenia usługi przez Dostawcę w powiązaniu z długością okresu wypowiedzenia umowy;

p. pogorszeniem jakości świadczenia usług w trybach lub zakresach nieuwzględnianych w parametrach SLA[2];

q. dostępem z urządzeń mobilnych do systemów przetwarzających dane Zamawiającego;

r. zakończeniem współpracy z Dostawcą, 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 usług dotyczących publicznej chmury obliczeniowej lub w wyniku decyzji Zamawiającego.

3. Po przeprowadzonej ocenie ryzyka powinna zostać opracowana lista mechanizmów niezbędnych do wdrożenia w celu zminimalizowania poziomu zidentyfikowanych ryzyk.

4. Proces zarządzania ryzykiem powinien mieć charakter ciągły. Przegląd ryzyk należy przeprowadzać w szczególności w przypadku zidentyfikowania nowego istotnego ryzyka oraz w przypadku istotnych zmian w trybie lub zakresie wykorzystywania publicznej chmury obliczeniowej. Przegląd ryzyk powinien być prowadzony regularnie, nie rzadziej jednak niż raz w roku.

5. Proces szacowania ryzyka powinien być dokumentowany – w szczególności dokumentowane powinny być zidentyfikowane ryzyka, ich ocena oraz plan minimalizacji zidentyfikowanych ryzyk.

6. Oszacowane poziomy ryzyka powinny być przedmiotem porównania z właściwymi poziomami ryzyka rozwiązań niewykorzystujących przetwarzania w publicznej chmurze obliczeniowej. Wynik tego porównania powinien być uwzględniany jako istotna przesłanka

[2] SLA – ang. Service Level Agreement.

potencjalnie mogąca przesądzać o wdrożeniu lub odstąpieniu od wdrożenia bądź o zaprzestaniu korzystania z publicznej chmury obliczeniowej.

6. Wymagania dotyczące umowy z Dostawcą

Umowa z Dostawcą powinna zapewniać możliwość sprawowania kontroli nad działaniami Dostawcy w zakresie świadczonych przez niego usług, w szczególności powinna zawierać zapisy określające:

1. zakresy praw, obowiązków i odpowiedzialności obu stron umowy, w tym podział ról pomiędzy osobami / rolami po stronie Zamawiającego i Dostawcy;
2. zapewnienie, że świadczenie usług przez Dostawcę odbywać się będzie zgodnie z wymaganiami obowiązujących przepisów prawa, regulacji zewnętrznych oraz regulacji wewnętrznych Zamawiającego;
3. zasady opracowania i wdrożenia stosownych polityk i procedur zapewniających prawidłową realizację zleconych czynności oraz bezpieczeństwo danych przekazanych przez Zamawiającego;
4. postanowienia / klauzule o powierzeniu przetwarzania przez Dostawcę danych osobowych zgodnie z przepisami o ochronie danych osobowych);
5. wymóg powołania przez Dostawcę, zgodnie z przepisami o ochronie danych osobowych, inspektora ochrony danych bądź zapewnienie korzystania z usług osoby zewnętrznej pełniącej taką funkcję;
6. uzgodnienia w zakresie wskazania państw, w jakich Dostawca posiada siedzibę oraz państw, w których faktycznie będą wykonywane powierzone czynności, z uwzględnieniem kontekstu systemu prawnego, który w tych państwach obowiązuje (ochrona tajemnic oraz informacji, która w Polsce zagwarantowana jest przez prawo, może doznawać uszczerbku wówczas, gdy system prawny w państwie wykonywania czynności przez Dostawcę nie przewiduje podobnej ochrony, tj. takiej, w której naruszenie odpowiednich tajemnic jest penalizowane) – zalecane jest określenie, że fizyczne lokalizacje centrów przetwarzania, którymi Dostawca posłuży się do realizacji umowy, znajdują się na terytorium państw Unii Europejskiej (zarówno Dostawca, jak również jego podwykonawcy nie będą przetwarzać danych poza terytorium Unii Europejskiej);
7. zasady realizacji żądań osób fizycznych oraz sposób współpracy w przypadku wniosków osób fizycznych o realizację praw określonych w przepisach o ochronie danych osobowych;
8. sposób komunikacji pomiędzy Zamawiającym i Dostawcą w sprawach dotyczących bezpieczeństwa informacji, w tym zachowania poufności i ochrony danych osobowych;
9. zakaz ujawniania przez Dostawcę jakichkolwiek informacji Zamawiającego, w szczególności z zakresu przetwarzanych danych, ich zawartości, przyrostu, przesyłania, i innych działań Zamawiającego, w szczególności zakaz ujawniania bądź przekazania przez Dostawcę powierzonych danych osobowych jakimkolwiek organom publicznym i osobom trzecim, o ile obowiązek ujawnienia bądź przekazania nie wynika wprost z przepisów prawa Unii Europejskiej bądź z przepisów prawa poszczególnych państw członkowskich;

10. zobowiązanie Dostawcy do zapewnienia poufności, integralności i dostępności informacji i danych Zamawiającego (w tym obowiązek zapewnienia należytego zabezpieczenia danych), w okresie obowiązywania umowy, a także do zachowania poufności w stosownym okresie po jej wygaśnięciu lub rozwiązaniu;
11. zobowiązanie Dostawcy do poinformowania i wyegzekwowania obowiązku zachowania poufności informacji i danych przekazanych przez Zamawiającego, zgodnie z warunkami zawartej umowy, od osób mających w imieniu i na rzecz Dostawcy dostęp do informacji i danych Zamawiającego;
12. zasady przekazywania, na żądanie Zamawiającego, listy upoważnionych osób mających dostęp do środowiska przetwarzania wraz z pełnioną przez nie funkcją w organizacji Dostawcy;
13. procedury zarządzania dostępem w sposób wykluczający uzyskanie dostępu przez osoby nieuprawnione;
14. kary umowne z tytułu naruszenia zasad bezpieczeństwa oraz ochrony informacji i danych przekazanych przez Zamawiającego, w tym danych osobowych;
15. obowiązek Dostawcy zapewnienia skutecznego niszczenia danych z uszkodzonych komponentów infrastruktury w przypadku ich wymiany;
16. warunki rozwiązania umowy;
17. w przypadku umów zawartych na okres dłuższy niż rok, możliwość bezkosztowego rozwiązania relacji kontraktowej z Dostawcą, z wyprzedzeniem nie dłuższym niż roczne;
18. okres wypowiedzenia umowy i procedury bezpiecznego zakończenia współpracy, w tym zwrotu bądź usunięcia danych (wedle wyboru Zamawiającego) oraz procedury przeniesienia danych do innego Dostawcy lub do systemów teleinformatycznych Zamawiającego;
19. opracowanie i regularne testowanie planu odstąpienia od umowy z Dostawcą (exit-plan);
20. prawo do przeprowadzania audytu lub kontroli przez Zamawiającego i upoważnione przez niego podmioty i osoby trzecie, w tym prawo dostępu do obszaru przetwarzania danych i nośników, na których znajdują się przetwarzane dane;
21. możliwość wykonywania obowiązków kontrolnych przez organ nadzorczy;
22. zgodne z przepisami prawa zakres odpowiedzialności Dostawcy za szkody wyrządzone osobom trzecim;
23. przeniesienie na Zamawiającego prawa do własności intelektualnej;
24. zasady i tryb obsługi zgłoszeń dotyczących incydentów i problemów w zakresie usług świadczonych przez Dostawcę, w tym obowiązek niezwłocznego zgłaszania zidentyfikowanych incydentów związanych z bezpieczeństwem informacji i danych osobowych powierzonych przez Zamawiającego (w szczególności zgodnie z wymaganiami przepisów o ochronie danych osobowych);
25. okresowe i incydentalne raportowanie z zakresu zagrożeń i zdarzeń bezpieczeństwa w środowisku teleinformatycznym Dostawcy;
26. 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 Dostawcy;

27. parametry jakości (SLA) usług świadczonych przez Dostawcę, w tym:
    a. szczegółowy opis usług świadczonych przez Dostawcę;
    b. godziny świadczenia usługi;
    c. oczekiwane wartości oraz mierniki w zakresie wydajności i dostępności usług świadczonych przez Dostawcę;
    d. mierniki w zakresie bezpieczeństwa IT;
    e. sposób komunikacji;
    f. zasady raportowania przez Dostawcę parametrów w zakresie wydajności i jakości świadczonych usług;
    g. zasady sankcjonowania przez Zamawiającego przekroczenia przez Dostawcę parametrów SLA;
    h. zasady przeglądów i aktualizacji parametrów SLA;
28. obowiązek Dostawcy do informowania z odpowiednim wyprzedzeniem / we właściwym czasie Zamawiającego, co najmniej o:
    a. planowanych zmianach (w tym dodatkowych funkcjonalnościach) w świadczonych usługach przetwarzania w chmurze;
    b. planowanych zmianach w świadczonych usługach przetwarzania w chmurze, podejmowanych w rezultacie przeprowadzonych audytów i kontroli;
    c. wszelkich żądaniach kierowanych do Dostawcy dotyczących ujawnienia, udostępnienia bądź przekazania danych powierzonych przez Zamawiającego;
    d. wszelkich żądaniach kierowanych do Dostawcy przez osoby, których dane zostały przekazane Dostawcy przez Zamawiającego, dotyczące prawa dostępu lub sprostowania danych, prawa przenoszenia danych, prawa do zapomnienia (w takiej sytuacji Dostawca nie podejmuje żadnych działań bez polecenia ze strony Zamawiającego);
    e. poważnych incydentach naruszenia bezpieczeństwa informacji oraz o incydentach naruszenia ochrony powierzonych przez Zamawiającego danych osobowych[3] (informacja o incydencie powinna zostać przekazana Zamawiającemu nie później niż w terminie 36 godzin);
29. wskazanie przez Dostawcę punktu kontaktowego z zespołem realizującym zadania w zakresie bezpieczeństwa teleinformatycznego chmury obliczeniowej;
30. zasady zarządzania zmianami w świadczonych usługach;

[3] Informacja o incydencie musi co najmniej:
a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
c. opisywać środki zastosowane lub proponowane przez Dostawcę w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

31. obowiązek Dostawcy okresowego przekazywania Zamawiającemu dzienników zdarzeń systemowych (zakres oraz źródła logów powinny zostać wyspecyfikowane przez Zamawiającego) bądź obowiązek stworzenia technicznych możliwości wglądu Zamawiającego lub pobierania takich danych;
32. politykę wykonywania kopii zapasowych oraz zapewnienia ciągłości działania;
33. parametry odtworzenia po katastrofie, w tym parametry dotyczące ciągłości działania usług świadczonych przez Dostawcę (w tym parametry RTO[4] i RPO[5]);
34. zasady dotyczące korzystania przez Dostawcę ze wsparcia podwykonawców – korzystanie przez Dostawcę z usług podwykonawców, w tym przekazanie przez Dostawcę swojemu podwykonawcy realizacji poszczególnych czynności oraz przetwarzania danych osobowych jest możliwe wyłącznie po uzyskaniu pisemnej zgody Zamawiającego oraz pod warunkiem spełnienia przez ten podmiot wymogów analogicznych do nałożonych na Dostawcę;
35. listę podwykonawców Dostawcy z lokalizacjami wraz z określeniem zakresu czynności świadczonych przez podwykonawców;
36. zasady przekazywania, na żądanie Zamawiającego, listy upoważnionych osób zatrudnionych przez Dostawcę oraz przez podwykonawców Dostawcy, mających lub mogących mieć dostęp do danych Zamawiającego;
37. zasady odpowiedzialności Dostawcy za działania i zaniechania jego podwykonawców (za działania i zaniechania swoich podwykonawców Dostawca odpowiada jak za własne działania i zaniechania);
38. realizację przez Dostawcę wsparcia technicznego w zakresie świadczonych usług – w szczególności Zamawiający powinien wziąć pod uwagę, że umowy mogą nie uwzględniać stref czasowych lub uwzględniać je w sposób niekorzystny dla Zamawiającego, w związku z czym Zamawiający powinien zapewnić, by czas rozwiązywania incydentów i problemów objęty był poziomami SLA.

7. Realizacja umowy (dotyczącej wykorzystania publicznej chmury obliczeniowej)

1. W celu spełnienia wymagań dotyczących bezpieczeństwa informacji podczas transmisji danych w sieci internet należy zapewnić, że transmisja danych pomiędzy Zamawiającym a infrastrukturą Dostawcy, pomiędzy poszczególnymi zasobami w infrastrukturze Dostawcy oraz 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.
2. Zamawiający i Dostawca, w ramach swoich zakresów kompetencji, powinni zapewnić m.in.:

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

a. stosowne polityki i procedury w celu zarządzania potencjalnymi usługami i procesami wykorzystującymi przetwarzanie w publicznej chmurze obliczeniowej;

b. szyfrowanie i ochronę integralności transmitowanych i przechowywanych danych za pomocą nieskompromitowanych metod;

c. dostęp do usług zarówno z publicznej sieci internet, jak również z sieci wewnętrznej LAN Zamawiającego – dla każdego kanału dostępu, należy określić sposób ochrony transmisji danych w tym standardy szyfrowania (w szczególności algorytmy i długości klucza) lub też normę która transmisja musi spełniać;

d. silne uwierzytelnienie użytkowników uprzywilejowanych oraz uwierzytelnienie urządzeń w celu transmisji danych;

e. wysoką dostępność połączeń sieciowych i odpowiednią, wymaganą przepustowość;

f. spójne wprowadzanie wymagań dotyczących bezpieczeństwa danych w zakresie posiadanych kompetencji;

g. opracowanie i przetestowanie integracji rozwiązania chmurowego Dostawcy z systemami Zamawiającego, takimi jak system autoryzacji użytkowników, systemy komunikacji, itp.;

h. zdefiniowanie parametrów dostępności danych zgodnych z parametrami RTO[6] i RPO[7] procesów biznesowych korzystających z publicznej chmury obliczeniowej;

i. plany działania Dostawcy zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową, rozwiązania w zakresie Disaster Recovery, metody zapewnienia wysokiej dostępności świadczonych usług;

j. odpowiedni plan działania na wypadek wystąpienia błędów lub niewłaściwego funkcjonowania usług świadczonych przez Dostawcę;

k. uzgodnienie sposobów bezpiecznego usuwania przetwarzanych danych (łącznie z kopiami zapasowymi i danymi zgromadzonymi w archiwach, kopiach i snapshotach maszyn wirtualnych, itp.) oraz zobowiązanie Dostawcy, na wniosek Zamawiającego, do udokumentowania powyższych czynności;

l. procedury wykonywania, przechowywania i archiwizacji kopii zapasowych;

m. niezależną od oferowanej w ramach publicznej chmury obliczeniowej lokalizację składowania zapasowych kopii danych uznanych za krytyczne oraz określenie trybu i zakresu przekazywania kopii zapasowych oraz format przechowywanych danych;

n. spójny proces zarządzania incydentami, w tym zasady rejestrowania incydentów, odpowiednie procedury reakcji na te zdarzenia, zasady rozwiązywania i raportowania incydentów, procedury informowania o incydentach, zasady gromadzenia i zabezpieczania dowodów związanych z incydentami, które będą mogły zostać wykorzystane w ewentualnych postępowaniach sądowych, zasady przekazywania na żądanie Zamawiającego dokumentacji incydentów.

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

8. Zakończenie współpracy Zamawiającego z Dostawcą

1. Zamawiający powinien posiadać strategię dotyczącą zakończenia korzystania z publicznej chmury obliczeniowej dostarczanej przez Dostawcę oraz plan działań minimalizujących takie ryzyko. Strategia zakończenia współpracy powinna uwzględniać m.in. następujące kwestie:
    a. wpływ zakończenia współpracy z Dostawcą na funkcjonowanie procesów biznesowych Zamawiającego wykorzystujących publiczną chmurę obliczeniową na wypadek przerwania świadczenia usług przez Dostawcę;
    b. warunki umowy z Dostawcą powinny umożliwiać Zamawiającemu bezpieczne zakończenie korzystania z publicznej chmury obliczeniowej, w tym zwrot oprogramowania (w tym kodów źródłowych), konfiguracji oraz danych w odpowiednim formacie, zakresie, trybie i czasie (w szczególności umożliwiających przeniesienie usług do innego Dostawcy);
    c. sposób migracji oprogramowania (w tym kodów źródłowych), konfiguracji i danych, łącznie z harmonogramem, specyfikacją wymagań środowiska teleinformatycznego i bezpieczeństwa oraz potrzebnych narzędzi, wpływ na strukturę organizacyjną Zamawiającego, procesy zarządzania środowiskiem teleinformatycznym i jego bezpieczeństwem.
2. W celu ograniczenia ryzyka związanego z zakończeniem współpracy z Dostawcą Zamawiający powinien zapewnić potrzebny personel, środki techniczne i technologie, w szczególności:
    a. zespół projektowy niezbędny do przeprowadzenia procesu zakończenia współpracy z Dostawcą i kontynuowania powierzonych wcześniej czynności samodzielnie lub powierzenia ich innemu Dostawcy;
    b. szczegółowy plan działań związanych z zaprzestaniem korzystania z usług świadczonych przez Dostawcę, 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 Zamawiającego lub przekazanych innemu Dostawcy.
3. Zamawiający powinien opracować i przetestować plan odstąpienia od umowy z Dostawcą (exit-plan) polegający na przeniesieniu całości danych Zamawiającego do innej infrastruktury przetwarzania bez utraty wartości informacyjnej danych. Wymogi techniczne exit-planu powinny być uzależnione od specyfiki usługi chmurowej, użytego modelu świadczenia usług chmurowych i struktury przetwarzanych informacji i powinny zostać określone przez Zamawiającego w sposób zapewniający mu ciągłość działania w razie decyzji o zaprzestaniu korzystania z usług danego Dostawcy. Zapewnienie alternatywnych lokalizacji infrastruktury lub alternatywnych usług chmurowych jest koniecznym elementem exit-planu. Przez zapewnienie infrastruktury alternatywnej rozumie się jej posiadanie, prawo dysponowania, lub potwierdzenie możliwości jej pozyskania w czasie i na warunkach określonych w exit-planie.