Projekt Rekomendacji Ministra Cyfryzacji dotyczących warunków przetwarzania w chmurze publicznej danych podmiotów publicznych

Spis treści

1. Zakres stosowania rekomendacji

1.1. Rekomendacje powinny być stosowane podczas formułowania warunków zamówienia, zawierających lub dopuszczających wykorzystanie przetwarzania danych w publicznej chmurze obliczeniowej.

1.2. Rekomendacje określają minimalny zakres obowiązków realizowanych po stronie Zamawiającego podczas przetwarzania danych w publicznej chmurze obliczeniowej.

1.3. Jeżeli z przeprowadzonej przez Zamawiającego analizy ryzyka wynika konieczność zastosowania dodatkowych zabezpieczeń nieopisanych w niniejszej rekomendacji, Zamawiający powinien również zastosować takie zabezpieczenia.

2. Definicje

2.1. Publiczna chmura obliczeniowa – usługa umożliwiająca dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników, charakteryzująca się następującymi cechami:

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 podmiotami publicznymi;

c. świadczenie usług opiera się na ustandaryzowanym katalogu skalowalnych usług infrastrukturalnych, platformowych lub oprogramowania, które mogą być oferowane podmiotom publicznym i komercyjnym oraz osobom fizycznym;

d. usługi udostępniane są zdalnie przez sieć Internet lub sieci dedykowane, 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.

2.2. Dostawca – podmiot będący usługodawcą usług publicznej chmury obliczeniowej.

2.3. Użytkownik – osoba fizyczna korzystająca z systemów teleinformatycznych publicznej chmury obliczeniowej.

2.4. Wykonawca – podmiot, który zawarł umowę z Zamawiającym obejmującą przetwarzanie w publicznej chmurze obliczeniowej lub ubiega się o udzielenie takiego zamówienia.

2.5. Zamawiający – podmiot publiczny zamawiający lub wykorzystujący publiczną chmurę obliczeniową.

2.6. Neutralność technologiczna – zasada równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji, w tym zapobiegania możliwości eliminacji technologii konkurencyjnych przy rozbudowie i modyfikacji eksploatowanych systemów teleinformatycznych lub przy tworzeniu konkurencyjnych produktów i rozwiązań.

2.7. Rozporządzenie RODO – 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).

3. Kryteria równoważności przetwarzania w chmurze

3.1. Przetwarzanie danych w chmurze publicznej jest równoważne przetwarzaniu w infrastrukturze własnej Zamawiającego, jeśli spełnione są następujące wymagania:

a. przetwarzanie danych w chmurze odbywa się na podstawie umowy z Dostawcą;

b. dane, które są przetwarzane w chmurze, mogą być przetwarzane wyłącznie na podstawie poleceń Zamawiającego, w tym wynikających z treści umowy;

c. Dostawca oraz jego rozwiązania techniczne i organizacyjne spełniają wymagania przewidziane dla systemu zarządzania bezpieczeństwem informacji zawarte 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) albo norm je zastępujących.

3.2. Niedopuszczalne jest:

a. korzystanie z usług publicznej chmury obliczeniowej bez umowy opisującej zobowiązania Dostawcy;

b. wyrażenie zgody na wykorzystanie danych Zamawiającego przez Dostawcę do celów niezwiązanych bezpośrednio z wykonaniem usług określonych w zawartej umowie;

c. korzystanie z usług publicznej chmury obliczeniowej bez weryfikacji dopuszczalności takiego działania w sektorowych i szczególnych przepisach prawa.

4. Planowanie przetwarzania w publicznej chmurze obliczeniowej

4.1. Przed rozpoczęciem przetwarzania danych w publicznej chmurze obliczeniowej, w ramach procesu planowania należy co najmniej:

a. określić wymagania biznesowe, funkcjonalne i techniczne biorąc pod uwagę obowiązujące przepisy prawa dotyczące planowanych usług, potrzeby Zamawiającego, obowiązujące u Zamawiającego standardy oraz oferowane na rynku warunki świadczenia usług chmurowych;

b. przeprowadzić analizę mającą na celu porównanie pełnych kosztów rozwiązań chmurowych oraz pełnych kosztów uruchomienia i utrzymywania rozwiązania we własnych zasobach Zamawiającego. Analiza powinna zostać przeprowadzona przy założeniu, że rozwiązania mają takie same standardy bezpieczeństwa (w tym bezpieczeństwa przechowywanych danych), niezawodności i dostępności. Przedmiotem analizy powinno być również określenie i zbadanie liczby obowiązków po stronie Zamawiającego związanych z zapewnieniem prawidłowego funkcjonowania danego rozwiązania;

c. ocenić przygotowanie 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 oraz nad zapewnieniem bezpieczeństwa przekazanych danych, a także zdolności personelu do analizy dzienników zdarzeń i innych informacji otrzymanych od Dostawcy. Zamawiający może korzystać w tym celu z personelu zewnętrznego lub innych usługodawców;

d. 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;

e. przeprowadzić inwentaryzację i klasyfikację danych, które planuje się powierzyć do przetwarzania przez Dostawcę;

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

g. 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;

h. w przypadku gdy przeprowadzenie analizy wpływu na ochronę danych osobowych (oceny skutków na ochronę danych) wymagane jest na podstawie art. 35 Rozporządzenia RODO, przeprowadzić ocenę 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[1];

i. dokonać oceny potencjału Dostawców pod kątem możliwości realizacji powierzanych czynności.

4.2. Potwierdzenie przeprowadzenia weryfikacji powyższych punktów powinno zostać udokumentowane.

4.3. Przed rozpoczęciem przetwarzania danych w publicznej chmurze obliczeniowej planowane rozwiązanie powinno zostać, w zakresie bezpieczeństwa informacji, zweryfikowane i zaakceptowane przez osoby (świadczące pracę lub usługi na rzecz Zamawiającego) odpowiedzialne za bezpieczeństwo informacji oraz zaopiniowane przez Inspektora Ochrony Danych Zamawiającego w zakresie przetwarzania danych osobowych.

5. Zarządzanie ryzykiem

5.1. 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.

5.2. 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 informacji oraz danych osobowych (w szczególności przetwarzanie dużych ilości danych pociąga za sobą wyższe poziomy ryzyka);

b. bezpieczeństwem danych osobowych, w tym ryzyka mające wpływ na prawa i wolności osób, których te dane dotyczą;

c. poszczególnymi czynnościami przetwarzania danych osobowych (w szczególności czynności związane z „profilowaniem" danych osobowych oraz automatycznym podejmowaniem decyzji pociągają za sobą wyższe poziomy ryzyka);

d. 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);

e. ocenę jakości i bezpieczeństwa połączenia z publiczną chmurą obliczeniową (ryzyka związane z ograniczeniem komunikacji, np. wskutek błędnego zaplanowania wymaganej przepustowości, przeciążenia lub awarii po stronie operatora telekomunikacyjnego, ataków typu DDoS, itp.);

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

f. kontrolą dostępu i zarządzaniem uprawnieniami użytkowników, w tym ryzyka 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);

g. ocenę procesu i możliwości integracji planowanego rozwiązania z systemami teleinformatycznymi Zamawiającego;

h. przetwarzaniem danych na terytorium państw, które nie zapewniają należytego poziomu ochrony danych lub których systemy prawne nie dają gwarancji należytej ochrony praw i wolności osób, których dane dotyczą – 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;

i. neutralnością technologiczną (vendor lockingiem) - nieuzasadnionym uzależnieniem od konkretnego Dostawcy usług bądź od konkretnego producenta sprzętu lub oprogramowania;

j. możliwościami i procedurami sprawowania kontroli nad działalnością Dostawcy w zakresie usług świadczonych przez niego na rzecz Zamawiającego;

k. stosowanymi przez Dostawcę mechanizmami izolacji danych poszczególnych Klientów Dostawcy, zapobiegającym przypadkowemu ujawnieniu danych Zamawiającego innemu Klientowi Dostawcy;

l. 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;

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

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

o. pogorszeniem jakości świadczenia usług w trybach lub zakresach nieuwzględnianych w parametrach SLA[2] mających wpływ na bezpieczeństwo świadczenia usługi lub jej dostępność;

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

q. zakończeniem współpracy z Dostawcą, w szczególności mając na uwadze możliwość nieoczekiwanego i nieplanowanego wycofania się Dostawcy ze współpracy, np. w wyniku likwidacji przedsiębiorstwa Dostawcy lub zaprzestania przez niego świadczenia usług dotyczących publicznej chmury obliczeniowej lub w wyniku decyzji Zamawiającego.

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

5.4. 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.

[2] SLA – ang. Service Level Agreement.

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

5.6. Oszacowane poziomy ryzyka powinny być przedmiotem porównania z właściwymi poziomami ryzyka rozwiązań niewykorzystujących przetwarzania w publicznej chmurze obliczeniowej, uwzględniając wszystkie aspekty zapewniające możliwie najpełniejszą porównywalność takich rozwiązań. Wynik tego porównania powinien być uwzględniany jako istotna przesłanka 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 usług świadczonych na rzecz Zamawiającego, w szczególności powinna zawierać zapisy określające:

6.1. zakresy praw, obowiązków i odpowiedzialności obu stron umowy;

6.2. zapewnienie, że świadczenie usług przez Dostawcę odbywać się będzie zgodnie z wymaganiami obowiązujących przepisów prawa dotyczących świadczenia usług objętych umową (w szczególności Dostawca zapewni, że przetwarzanie danych osobowych spełnia wymogi Rozporządzenia RODO i chroni prawa osób, których dane dotyczą), regulacji zewnętrznych oraz regulacji wewnętrznych Zamawiającego udostępnionych Dostawcy;

6.3. zasady opracowania i wdrożenia stosownych polityk i procedur zapewniających prawidłową realizację zleconych czynności oraz bezpieczeństwo danych przekazanych przez Zamawiającego;

6.4. postanowienia / klauzule o powierzeniu przetwarzania przez Dostawcę danych osobowych (zgodnie z przepisami o ochronie danych osobowych) – w przypadku przetwarzania danych osobowych Dostawca pełni rolę podmiotu przetwarzającego;

6.5. w przypadku gdy powołanie inspektora ochrony danych jest wymagane na podstawie przepisów rozporządzenia RODO, powołanie inspektora ochrony danych bądź zapewnienie korzystania z usług osoby zewnętrznej pełniącej taką funkcję;

6.6. 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), w przypadku gdy dane przetwarzane będą poza terytorium Unii Europejskiej Dostawca zobowiąże się do przestrzegania przepisów Rozdziału V Rozporządzenia RODO;

6.7. zapewnienie aktywnego wsparcia i pomocy w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;

6.8. sposób komunikacji pomiędzy Zamawiającym i Dostawcą w sprawach dotyczących bezpieczeństwa informacji, w tym zachowania poufności i ochrony danych osobowych;

6.9. 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;

6.10. zobowiązanie Dostawcy do zapewnienia poufności, integralności i dostępności 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;

6.11. zobowiązanie Dostawcy do poinformowania i wyegzekwowania obowiązku zachowania poufności danych przekazanych przez Zamawiającego, zgodnie z warunkami zawartej umowy, od osób mających w imieniu i na rzecz Dostawcy dostęp do danych Zamawiającego;

6.12. zasady uzyskiwania dostępu do danych Zamawiającego przez przedstawicieli Dostawcy i osoby upoważnione przez Dostawcę;

6.13. procedury zarządzania dostępem w sposób wykluczający uzyskanie dostępu przez osoby nieuprawnione;

6.14. kary umowne z tytułu naruszenia zasad bezpieczeństwa oraz ochrony danych przekazanych przez Zamawiającego, w tym danych osobowych;

6.15. obowiązek Dostawcy zapewnienia skutecznego niszczenia danych z uszkodzonych komponentów infrastruktury w przypadku ich wymiany;

6.16. warunki rozwiązania umowy;

6.17. w przypadku umów zawartych na okres dłuższy niż rok, zasady wypowiedzenia relacji kontraktowej z Dostawcą bez obowiązku zapłaty kar umownych za przedterminowe wypowiedzenie umowy;

6.18. 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;

6.19. opracowanie i okresowe testowanie planu związanego z rozwiązaniem lub zakończeniem obowiązywania umowy z Dostawcą (exit-plan);

6.20. prawo do przeprowadzania audytu lub kontroli przez Zamawiającego i upoważnione przez niego podmioty i osoby trzecie, w szczególności poprzez prawo do żądania od Dostawcy udostępnienia raportów z niezależnych audytów potwierdzających spełnianie przez Dostawcę wymaganych norm bezpieczeństwa;

6.21. możliwość wykonywania obowiązków kontrolnych przez organ nadzorczy;

6.22. zgodne z przepisami prawa zakres odpowiedzialności Dostawcy za szkody wyrządzone osobom trzecim;

6.23. zasady i tryb obsługi zgłoszeń dotyczących incydentów i problemów w zakresie usług świadczonych przez Dostawcę i dotyczących Zamawiającego, w tym obowiązek zgłaszania zidentyfikowanych incydentów związanych z bezpieczeństwem informacji i danych osobowych powierzonych dostawcy przez Zamawiającego zgodnie z wymaganiami przepisów o ochronie danych osobowych;

6.24. okresowe i incydentalne raportowanie z zakresu zagrożeń i zdarzeń bezpieczeństwa w środowisku teleinformatycznym Dostawcy, które dotyczą bezpośrednio danych Zamawiającego;

6.25. parametry 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;

6.26. w zakresie dotyczącym usług świadczonych dla Zamawiającego zasady informowania przez Dostawcę 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, niezwłocznie, nie później jednak niż w **terminie 36 godzin);**

6.27. wskazanie przez Dostawcę punktu kontaktowego z zespołem realizującym zadania w zakresie bezpieczeństwa teleinformatycznego chmury obliczeniowej;

6.28. w zakresie dotyczącym usług świadczonych dla Zamawiającego zasady zarządzania zmianami w świadczonych usługach;

6.29. obowiązek Dostawcy okresowego przekazywania na żądanie Zamawiającego dzienników zdarzeń systemowych dotyczących usług świadczonych na rzecz Zamawiającego (zakres oraz źródła logów powinny zostać wyspecyfikowane przez Zamawiającego) bądź obowiązek stworzenia technicznych możliwości wglądu Zamawiającego lub pobierania takich danych;

6.30. politykę wykonywania kopii zapasowych oraz zapewnienia ciągłości działania;

6.31. parametry odtworzenia po katastrofie, w tym parametry dotyczące ciągłości działania usług świadczonych przez Dostawcę na rzecz Zamawiającego;

6.32. 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 zgody Zamawiającego oraz pod warunkiem spełnienia przez ten podmiot wymogów analogicznych do nałożonych na Dostawcę;

---

[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.

6.33. listę podwykonawców Dostawcy mających dostęp do danych przekazanych przez Zamawiającego wraz z określeniem zakresu czynności związanych z przetwarzaniem danych Zamawiającego;

6.34. zasady odpowiedzialności Dostawcy za działania i zaniechania jego podwykonawców (za działania i zaniechania swoich podwykonawców Dostawca odpowiada jak za własne działania i zaniechania);

6.35. 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)

7.1. W celu spełnienia wymagań dotyczących bezpieczeństwa 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.

7.2. Zamawiający i Dostawca, w ramach swoich zakresów odpowiedzialności, powinni zapewnić m.in.:

a. stosowne polityki i procedury zarządzania 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. opracowanie i przetestowanie integracji rozwiązania chmurowego Dostawcy z systemami Zamawiającego, takimi jak system autoryzacji użytkowników, systemy komunikacji, itp.;

g. zdefiniowanie parametrów dostępności danych zgodnych z parametrami RTO[4] i RPO[5] procesów biznesowych korzystających z publicznej chmury obliczeniowej;

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

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

j. uzgodnienie sposobów bezpiecznego usuwania przetwarzanych danych (łącznie z kopiami zapasowymi i danymi zgromadzonymi w archiwach, kopiach i snapshotach maszyn

[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.

wirtualnych, itp.) oraz zobowiązanie Dostawcy, na wniosek Zamawiającego, do udokumentowania powyższych czynności;

k. procedury wykonywania, przechowywania i archiwizacji kopii zapasowych, w tym w zasobach niezależnych od publicznej chmury obliczeniowej;

l. 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.

8. Zakończenie współpracy Zamawiającego z Dostawcą

8.1. 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 przetwarzanych danych w określonym czasie w formacie umożliwiającym przeniesienie usług do innego Dostawcy;

c. sposób migracji oprogramowania, 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.

8.2. W celu ograniczenia ryzyka związanego z zakończeniem współpracy z Dostawcą Zamawiający powinien określić (zapewnić lub wskazać sposób pozyskania i organizacji) 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.

8.3. Zamawiający powinien opracować, przeglądać i testować plan związany z rozwiązaniem lub zakończeniem obowiązywania 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 danych 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.