Uwagi Polskiej Izby Informatyki i Telekomunikacji
do projektu Rekomendacji Ministra Cyfryzacji dotyczących warunków technicznych
i organizacyjnych powierzenia danych administracji publicznej do przetwarzania
w publicznej chmurze obliczeniowej.

Polska Izba Informatyki i Telekomunikacji (PIIT) podczas tworzenia uwag do projektu Rekomendacji Ministra Cyfryzacji dotyczących warunków technicznych i organizacyjnych powierzenia danych administracji publicznej do przetwarzania w publicznej chmurze obliczeniowej (dalej: Rekomendacje) kierowała się zasadą neutralności technologicznej wyrażoną w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne (dalej: ustawa o informatyzacji) w art. 3 punkt 19):

> *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;*

Traktujemy projekt Rekomendacji jako krok w kierunku praktycznej realizacji tej zasady poprzez umożliwienie jednostkom sektora finansów publicznych skorzystania z prostych, a zarazem bezpiecznych i zgodnych z przepisami rozwiązań wykorzystujących przetwarzanie danych w publicznej chmurze obliczeniowej.

PIIT podczas prac nad projektem Rekomendacji przyjęła następujące Założenia kierunkowe.

Założenie 1. Rekomendacje dotyczą wyłącznie chmury publicznej
Przyjęte założenie oznacza, że chodzi o wykorzystanie standardowej oferty dostępnej u Dostawców usług chmurowych. W Rekomendacjach zatem nie powinny znajdować się zapisy dotyczące negocjacji z Dostawcą na temat zasad korzystania z chmury (usługi chmurowej) specjalnie przygotowanej dla Zamawiającego, ani problemy związane z funkcjonowaniem chmur prywatnych czy hybrydowych. Przy takim założeniu Rekomendacje mają – pomóc Zamawiającemu podjąć decyzję o wykorzystaniu chmury publicznej po sprawdzeniu dostępnych informacji.

Taka formuła Rekomendacji odpowiada funkcjonalnie zasadom zakupu i korzystania z oprogramowania „z półki” (tzw. model COTS, ang. Commercial Off The Shelf).

Założenie 2. Rekomendacje powinny być proste i napisane przystępnym językiem.
Przyjęte założenie wynika z tego, że Rekomendacje powinny znaleźć zastosowanie nawet w najmniejszych jednostkach sektora finansów publicznych, w szczególności w jednostkach samorządu terytorialnego (JST). Takie jednostki zazwyczaj nie dysponują ani licznym personelem technicznym, ani wsparciem prawnym w obszarze stosowania technologii. Natomiast chmura publiczna ze względu na koszty wdrożenia, prostotę wykorzystania oraz aspekty związane z cyberbezpieczeństwem może być brana pod uwagę jako jeden ze wskazanych sposobów realizowania zadań publicznych w takich jednostkach.

Zakładamy, że objętość Rekomendacji nie powinna przekraczać 8-10 stron.

Przyjmujemy przy tym, że Rekomendacje nie tworzą wymogów dodatkowych w stosunku do tych wynikających z przepisów prawa bądź potrzebnych dla zapewnienia zgodności z przepisami prawa. Do Rekomendacji może być przygotowany precyzyjny Aneks, tym razem napisany już językiem prawniczym i odwołujący się zarówno do definicji, jak i odpowiednich przepisów ustaw i rozporządzeń. Przygotowane przez PIIT uwagi mają wskazane odpowiednie umocowania w przepisach prawa.

Założenie 3. Wypełnienie wymogów Rekomendacji jest wystarczające dla zamówienia i stosowania chmury publicznej, także w przypadkach powierzenia przetwarzania danych osobowych.
Przyjęte założenie służyć ma ułatwieniu zamawiania i wykorzystania chmury nawet przez małe jednostki sektora finansów publicznych, które nie mają możliwości dokonywania złożonych analiz, zamawiania dodatkowych ekspertyz itp., natomiast zastosowanie chmury publicznej dostarczanej przez wiarygodnego Dostawcę może podnosić poziom cyberbezpieczeństwa, łatwość zarządzania i zmniejszenie kosztów utrzymania systemów.

Oczywiście każdy Zamawiający – jeśli uzna to za wskazane lub będzie to wynikało z rodzaju zastosowania publicznej chmury obliczeniowej – może dokonać dodatkowych analiz prawnych, organizacyjnych i technicznych dla przypadku swojego systemu teleinformatycznego.

Założenie 4. Dostawca przetwarza dane wyłącznie zgodnie z poleceniami i wymaganiami Zamawiającego (odpowiednik podmiotu przetwarzającego w RODO), w szczególności wynikającymi z treści umowy zawartej z Zamawiającym.
Przyjęte założenie pozwala uniknąć rozbudowy Rekomendacji o przypadki, kiedy np. Zamawiający nie jest administratorem i jedynym dysponentem przetwarzanych danych (por. Założenie 2 i Założenie 3). Mając na uwadze zapisy prawa związane z przetwarzaniem danych osobowych przyjmujemy, że Dostawca staje się podmiotem przetwarzającym zgodnie z zapisami RODO.. To powoduje znaczne uproszczenie wymagań, a także wprost odpowiada na pytania dotyczące przetwarzania danych osobowych w chmurze publicznej.

Założenie 5. Rekomendacje powinny dotyczyć wymagań właściwych jedynie dla przetwarzania danych w chmurze. Należy wykreślić punkty Rekomendacji, które w równej mierze dotyczą przetwarzania danych w ramach lokalnej infrastruktury Zamawiającego.
Przyjęte założenie jest związane z utrzymaniem prostoty i przystępności Rekomendacji (por. Założenie 2 i zasada neutralności technologicznej), ale także uniknięciu błędnej interpretacji, że wymagania wobec systemów we własnej infrastrukturze są niższe niż dla systemów w chmurze publicznej.

Porównaj np. Uwaga Szczegółowa do punkt 4.1 podpunkt k.

Wszystkie powyższe Założenia stosujemy w naszych dalszych uwagach **łącznie**.

Uwagi Ogólne

Uwaga 1. Planowanie, zamawianie i eksploatacja systemów informatycznych, realizujących zadania publiczne z wykorzystaniem chmury publicznej.
PIIT uważa, że z trzech etapów dotyczących chmury i wyróżnionych w Rekomendacjach (planowanie, zamawianie i eksploatacja) najtrudniejszy i w zasadzie niemożliwy do ujednolicenia w ramach Rekomendacji jest etap planowania (planowanie i szacowanie ryzyka). Każdy podmiot realizujący zadania publiczne ma swoją specyfikę, czy też właściwą tylko dla siebie infrastrukturę, historię oraz zasady eksploatacji. W takim kontekście każde wykorzystanie publicznej chmury obliczeniowej musi być dopasowane do charakterystyki tego podmiotu i wykonywanego zadania. Przyjmujemy, że Zamawiający powinien zadbać o spełnienie wymagań takich, jakie mają zastosowanie do przetwarzania we własnej infrastrukturze (*on-premise*), a dodatkowo wymagań specyficznych dla chmury, zawartych w Rekomendacjach.

Dlatego też proponujemy ograniczyć część Rekomendacji poświęconą planowaniu do niezbędnego minimum, pozostawiając podmiotom decyzję o zakresie i sposobach planowania wykorzystania przetwarzania w chmurze publicznej.

Uwaga 2. Wprowadzenie do Rekomendacji.
Proponujemy – na bazie przedstawionych powyżej Założeń – przygotowanie krótkiego tekstu wprowadzającego odbiorców Rekomendacji w cel i zakres ich stosowania.
Tekst wprowadzający może zastąpić Rozdział 1 „Zakres stosowania Rekomendacji".

PIIT chciałby zaproponować główne elementy, które mogłyby być zawarte w preambule:

- Cel Rekomendacji: ułatwienie zamawiania i eksploatacji chmury publicznej;
- Zakres Rekomendacji:
    - minimalne wymagania przy zamówieniach i eksploatacji chmury publicznej;
    - zapisy dotyczące wyłącznie chmury publicznej jako funkcjonalnego odpowiednika zamówienia standardowego oprogramowania „z półki";
- Charakter Rekomendacji:
    - specyficzne wymagania dla zamawiania i eksploatacji chmury publicznej,
    - wskazanie, że usługi przetwarzania w chmurze publicznej powinny spełniać wymagania takie, jakie mają zastosowanie do przetwarzania danych we własnych zasobach technicznych

Uwagi Szczegółowe		
	Projekt Rekomendacji Ministerstwa Cyfryzacji	**Uwagi/Propozycje zmian PIIT**
0.1.	**Tytuł**: *Rekomendacje Ministra Cyfryzacji dotyczące warunków technicznych i organizacyjnych powierzenia danych administracji publicznej do przetwarzania w publicznej chmurze obliczeniowej.*	**Propozycja zmiany tytułu**: *Rekomendacje Ministra Cyfryzacji, dotyczące warunków przetwarzania w chmurze publicznej w jednostkach sektora finansów publicznych.* **Uzasadnienie**: W zmienionym tytule wykorzystujemy odwołanie do dwóch aktów prawnych – ustawy o finansach publicznych oraz ustawy o krajowym systemie cyberbezpieczeństwa (dalej: UKSC). Dzięki takiemu zapisowi tytułu wskazujemy, że Rekomendacje dotyczą każdego podmiotu z sektora finansów publicznych (co pozwala na uniknięcie dyskusji, jakie jednostki należą do administracji publicznej). Równocześnie proponujemy wykreślenie sformułowania „technicznych i organizacyjnych" ponieważ w Rekomendacjach jest m.in. mowa o wypełnianiu warunków wynikających z umów (warunków prawnych). Warto zatem pozostawić tytuł w jak najbardziej ogólnej wersji.

1. Zakres stosowania rekomendacji **Propozycja PIIT:** Patrz uwaga ogólna nr 2. Przenieść dwa zapisy z punktów 1.1. oraz 1.3. do tekstu wprowadzającego do Rekomendacji.		
1.1	*Rekomendacje powinny być stosowane podczas formułowania warunków zamówienia zawierających lub dopuszczających wykorzystanie przetwarzania danych w chmurze obliczeniowej poza zasobami technicznymi administracji publicznej.*	**Propozycja PIIT**: *Rekomendacje powinny być stosowane podczas formułowania warunków zamówienia, zawierających lub dopuszczających wykorzystanie przetwarzania danych w publicznej chmurze obliczeniowej.* **Uzasadnienie**: Uproszczenie tekstu, usunięcie części wynikającej z dalej przedstawionej definicji publicznej chmury obliczeniowej. Dopuszczających wykorzystanie - Zamawiający nie musi precyzować, że oferowane rozwiązania muszą zawierać wykorzystywanie przetwarzania danych w chmurze, ale może akceptować takie rozwiązania.
1.2	*Rekomendacje powinny być stosowane podczas formułowania klauzul w umowach zawieranych z Dostawcą usług dotyczących przetwarzania w chmurze obliczeniowej.*	**Propozycje PIIT**: Wykreślić ten punkt **Uzasadnienie:** Patrz Założenie 1. Rekomendacje miałyby dotyczyć zamawiania i eksploatacji standardowych usług chmury publicznej, co funkcjonalnie odpowiada zamówieniu i eksploatacji oprogramowania „z półki” w infrastrukturze własnej. W takim przypadku nie formułuje się klauzul, ale akceptuje lub odrzuca zapisy umowy, co skutkuje wykorzystaniem lub nie usługi chmurowej. Patrz także: zapisy związane z Wykonawcą

1.3	*Rekomendacje określają minimalny zakres obowiązków i koniecznych dostosowań organizacyjnych po stronie Zamawiającego w przypadku korzystania z usług świadczonych w chmurze obliczeniowej.*	**Propozycja PIIT**: *Rekomendacje określają minimalny zakres obowiązków po stronie Zamawiającego podczas przetwarzania danych w publicznej chmurze obliczeniowej.* **Uzasadnienie**: ujednolicenie określeń z punktem 1.1. Wskazanie, że zapisy rozdziałów 7 i 8 wprost odnoszą się do Zamawiającego
1.4	*W każdym z przypadków wymagane będzie po stronie Zamawiającego zastosowanie dodatkowych, adekwatnych do danej sytuacji, środków i mechanizmów wynikających z przeprowadzonej analizy ryzyka.*	**Propozycja PIIT:** Wykreślić ten punkt **Uzasadnienie**: Aby Rekomendacje spełniły zadanie ułatwienia wykorzystania chmury publicznej jednostkom sektora finansów publicznych, powinny stanowić zestaw minimalnych wymagań określających wymogi do utworzenia zamówienia i rozpoczęcia eksploatacji usługi w chmurze. Zapis znajdujący się w punkcie 1.4. oznacza coś przeciwnego.

2. Definicje		
2.2	*Dostawca – podmiot będący usługodawcą usług publicznej chmury obliczeniowej, odpowiedzialny za zapewnienie parametrów funkcjonalnych i technicznych, w tym poufności, integralności i dostępności oferowanego rozwiązania chmurowego.*	**Propozycja PIIT**: *Dostawca – podmiot będący usługodawcą publicznej chmury obliczeniowej.* **Uzasadnienie**: Całość rozwiązania chmurowego zależy nie tylko od Dostawcy, ale także Zamawiającego oraz dostawcy łącz do chmury (np. operatora telekomunikacyjnego). Enumeratywne wymienianie parametrów może spowodować pominięcie istotnego parametru.
2.2a		**Propozycja PIIT:** *Wykonawca – podmiot, który złożył ofertę lub zawarł umowę na zamówienie udzielane przez Zamawiającego obejmujące (także) przetwarzanie w publicznej chmurze obliczeniowej lub ubiega się o udzielenie takiego zamówienia* **Uzasadnienie**: Uważamy, że taka definicja, nawiązująca wprost do definicji znajdującej się pzp, jest potrzebna ze względu na uniknięcie rozbieżności interpretacyjnych. W wielu przypadkach usługa świadczona w chmurze będzie fragmentem większego systemu komputerowego?. Również ze względu na stosowane modele biznesowe przy niektórych chmurach relacja będzie pomiędzy partnerem Dostawcy (lokalną firmą) a Zamawiającym, a nie bezpośrednio z Dostawcą. Część z obowiązków wynikających z Rekomendacji może wówczas być wykonywana przez Wykonawcę, co powinno znaleźć jednoznaczne odzwierciedlenie w zapisach umów wskazujących podział obowiązków pomiędzy Zamawiającym, Dostawcą i Wykonawcą.
2.3	*Zamawiający – jednostka administracji publicznej.*	**Propozycja PIIT:** *Zamawiający – podmiot sektora finansów publicznych zamawiający lub wykorzystujący publiczną chmurę obliczeniową.* **Uzasadnienie**: patrz dyskusja dotycząca pełnego tytułu Rekomendacji.

2.3a		**Propozycja PIIT:** *Użytkownik – osoba fizyczna, korzystająca z systemów teleinformatycznych publicznej chmury obliczeniowej;* **Uzasadnienie**: odpowiada zapisowi art. 3 p. 22) ustawy o informatyzacji Definicja wprowadzona ze względu na to, że Użytkownikami systemów teleinformatycznych mogą być nie tylko pracownicy Zamawiającego, ale również inne osoby.
2.4	*Modele świadczenia usług w chmurze:* *a. IaaS (Infrastructure 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.*	**Propozycja PIIT**: Wykreślenie tego punktu. **Uzasadnienie**: Nie wnosi on nic poza powszechnie znane definicje. W dalszym ciągu Rekomendacji jest pojedyncze odniesienie do tej definicji.

3. Kryteria równoważności przetwarzania w chmurze		
3.0		**Propozycja PIIT:** *Dostawca będący operatorem usługi kluczowej będącej usługą cyfrową bądź spełniający obowiązki dostawców usługi cyfrowej przetwarzania w chmurze, w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa z 10 maja 2018 r., spełnia kryteria możliwości wykorzystania jego usług chmury publicznej w realizacji zadań publicznych.* **Uzasadnienie**: Celem zapisu jest uproszczenie sytuacji dla Zamawiających. Jeśli Dostawca usługi chmurowej spełnia wymagania dla usług kluczowych, to dla ogólnego zastosowania rozwiązania chmurowego w administracji w oczywisty sposób spełnia kryteria zapisane w Rekomendacjach. Nadzór i kontrolę nad dostawcami usług cyfrowych mają organy właściwe do spraw cyberbezpieczeństwa (UKSC, art. 53 i nast., także: Rozporządzeniu Wykonawczym 2018/151). Mogą oni również nakładać kary na dostawców usług cyfrowych. Dzięki takiemu zapisowi, Zamawiający nie musi prowadzić planowania (prócz sprawdzenia, czy wykorzystanie publicznej chmury obliczeniowej jest zgodne z wymogami prawa) i szacowania ryzyka wykorzystania chmury.

3.1	*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).*	**Propozycja PIIT**: *Przetwarzanie danych w chmurze publicznej jest równoważne przetwarzaniu w infrastrukturze własnej podmiotu realizującego zadania publiczne, 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 zgodnie z poleceniami Zamawiającego, w tym wynikającymi z treści umowy; w przypadku przetwarzania danych osobowych Dostawca pełni rolę podmiotu przetwarzającego,* *c. Dostawca może wykazać się certyfikatami norm przewidzianych dla zarządzania bezpieczeństwem informacji* *d. Spełnione są minimalne wymagania zapisane w niniejszych rekomendacjach.* **Uzasadnienie**: Podkreślamy pojęcie „infrastruktury własnej”, gdyż wykorzystanie infrastruktury innych podmiotów nie zwalnia Zamawiającego z zachowania zgodności z wymaganiami prawa, jak i stosowania się do zapisów Rekomendacji. Upraszczamy brzmienie punktu a. z projektu, tworząc krótsze punkty a. i b. Podkreślamy całkowitą decyzyjność Zamawiającego nad danymi. Punkt c. uważamy, że enumeratywne wymienianie norm ISO może być niewystarczające ze względu na charakter przetwarzania danych, rodzaj jednostki sektora finansów publicznych oraz zmiany w przepisach prawa, np. Rozporządzeniu KRI. Dla określonych sektorów mogą mieć zastosowanie szczegółowe normy związane z przetwarzaniem szczególnych rodzajów danych – patrz także zapis punktu 3.2., który

		wskazuje na niedopuszczalność wykorzystania chmury jeśli zakazują tego przepisy prawa.
3.2	*Niedopuszczalne jest:* *a. korzystanie z usług w publicznej chmurze obliczeniowej na podstawie nieuregulowanych kontraktowo opcji umów licencyjnych;* *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.*	**Propozycja PIIT:** *Niedopuszczalne jest:* *a. W zakresie wskazanym rekomendacjach korzystanie z usług publicznej chmury obliczeniowej bez umowy opisującej zobowiązania Dostawcy* *b. Zawarcie umowy nie może być warunkowane przez wykorzystanie danych Zamawiającego przez Dostawcę do celów niezwiązanych bezpośrednio z wykonaniem usług publicznej chmury obliczeniowej lub zapewnieniem ich bezpieczeństwa* *c. Korzystanie z usług chmury publicznej, gdy zakazują tego przepisy prawa.* **Uzasadnienie:** Punkt a. Proponujemy inny zapis, oddający ten sam zamysł; Punkt b. Dane, jakie są powierzone Dostawcy nie mogą być wykorzystywane do celów innych niż określił to Zamawiający; wyjątkiem jest bezpieczeństwo, np. ochrona antywirusowa Punkt c. Zamiast wymieniania jednej ustawy nasza propozycja wprost odnosi się do tego, że niektóre przepisy prawa mogą uniemożliwiać stosowanie chmury publicznej. Oznacza także, że Zamawiający nie może odrzucić rozwiązania bazującego na chmurze publicznej bez podania podstawy prawnej;

3.3	*Niniejsze Rekomendacje nie wyłączają stosowania przepisów regulujących dopuszczalność przetwarzania w chmurze szczególnych kategorii danych, w tym danych medycznych i innych danych wrażliwych.*	**Propozycja PIIT:** Wykreślić ten punkt **Uzasadnienie**: jego zakres został przeniesiony do punktu 3.2. b.

4. Planowanie przetwarzania w chmurze obliczeniowej **Poprawka PIIT: 4. Planowanie przetwarzania w publicznej chmurze obliczeniowej**		
	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;	**Propozycja PIIT:** wykreślić ten punkt **Propozycja alternatywna:** *a. Dokonać sprawdzenia, czy obowiązujące przepisy prawa nie wykluczają możliwości wykorzystania publicznej chmury obliczeniowej* **Uzasadnienie:** Całkowite wykreślenie wynika z faktu, że bez względu na rodzaj wdrażanego systemu Zamawiający dokonuje takiej analizy, jaka została zapisana w tym punkcie – dlaczego zatem taki punkt powinien pojawić się tylko w Rekomendacjach dotyczących chmury? Propozycja alternatywna wynika z faktu, że jeśli Zamawiający sprawdził przepisy prawa, które w efekcie wykluczają wykorzystanie publicznej chmury obliczeniowej dla planowanego systemu, to rzeczywiście jest to właściwa chwila, aby zatrzymać proces wdrażania rozwiązania chmurowego. Jednocześnie chcielibyśmy tutaj zredukować zapis do jasnego umocowania przeciwskazania wdrożenia chmury wyłącznie w przepisach prawa (obejmującego także wiążące rekomendacje tworzone przez regulatorów), bez powoływania się na niejasne określenie „regulacje zewnętrzne” lub nawet „regulacje wewnętrzne”, które są w pełnej gestii Zamawiającego i mogą być dowolnie zmieniane. Proponowane rozwiązanie daje możliwość łatwej odpowiedzi: Tak/Nie Można pominąć ten punkt mając na uwadze punkt 3.2.

	b. przeprowadzić analizę kosztów i korzyści związanych z korzystaniem z usług publicznej chmury obliczeniowej;	**Propozycja PIIT**: wykreślić ten punkt **Uzasadnienie**: Nie ma żadnych wytycznych, ani narzędzi dostępnych dla Zamawiających, które pozwoliłyby im dokonać takiej analizy szybko, sprawnie, bez dodatkowych kosztów, a jednocześnie w konsystentny sposób dla wszystkich Zamawiających. W chwili obecnej jest to punkt, który tylko dodaje pracy Zamawiającemu, natomiast nie przynosi żadnej korzyści. Analiza – nie poddana ujednoliceniu przez organ zewnętrzny – będzie zawsze wykazywać to, co zechce osoba ją wykonująca.
	c. przeprowadzić analizę mającą na celu porównanie pełnych kosztów rozwiązań chmurowych oraz pełnych kosztów uruchomienia rozwiązania we własnych zasobach Zamawiającego;	**Propozycja PIIT**: wykreślić ten punkt **Uzasadnienie**: j.w.
	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;	**Propozycja PIIT**: wykreślić ten punkt **Uzasadnienie:** Kto miałby wystawić wiążące prawnie potwierdzenie opisane w tym punkcie? Podkreślamy „wiążące prawnie” ponieważ zakładamy, że rozwiązanie chmurowe może dotyczyć takich zadań jednostki sektora finansów publicznych, za które bierze odpowiedzialność. W szczególności, zapis dotyczy także usług jakie potencjalnie mogą być świadczone w przyszłości (kto bierze odpowiedzialność, jeśli takie usługi nie będą świadczone w przyszłości lub ich funkcjonalność bądź inne wymagania nie będą wystarczające?)

	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);	**Propozycja PIIT:** wykreślić ten punkt **Uzasadnienie:** Uproszczenie a. takie działania, jak określenie poziomu ryzyka dla określania odpowiedzialności Dostawcy, dotyczą procesu szacowania ryzyka i zamawiania, a nie planowania (por. p. 5.1 i zapisy rozdziału 6). b. szacowanie ryzyka (por. rozdział 5) powinno mieć miejsce dla każdego rodzaju systemu, a zatem nie ma potrzeby wymieniania go w szczególny sposób dla rozwiązań chmurowych c. brak jest ujednoliconych wytycznych i narzędzi, które pozwalałyby na miarodajne oceny oraz szybką i kosztowo efektywną metodę d. nie jest możliwe zrobienie takiej analizy dla ogółu rynku Dostawców – jakakolwiek analiza możliwa tylko dla konkretnego Dostawcy!

	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;	**Propozycja PIIT**: wykreślić ten punkt **Uzasadnienie**: Nie ma żadnego uzasadnienia nakładanie takiego obowiązku w przypadku rozwiązania chmurowego przy braku takich wymagań wobec rozwiązań w infrastrukturze własnej. Przykładowo: kontrole, jakie przeprowadził w ostatnich latach NIK pokazały, że sektor finansów publicznych nie jest idealnie przygotowany pod względem bezpieczeństwa. Wszystkie badane systemy były w infrastrukturze własnej Zamawiających. Podobnie byłoby przy dokonaniu audytu ze względu na zgodność systemów w administracji publicznej z rozporządzeniem KRI. Uznajemy ten punkt w aktualnym brzmieniu za dyskryminujący rozwiązania z wykorzystaniem publicznej chmury obliczeniowej. Taki zapis, jak ten nie bierze pod uwagę możliwości skorzystania z usług Wykonawcy, a nie tylko 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;*	**Propozycja PIIT**: usunąć ten punkt **Uzasadnienie:** Takie działania, jak zabezpieczenie przed nagłym zakończeniem usługi dotyczą procesu zamawiania, a nie planowania. Taką analizę można dokonać znając Dostawcę, natomiast jest praktycznie niemożliwa do wykonania dla ogółu rynku Dostawców.

	h. przeprowadzić inwentaryzację i klasyfikację informacji, które planuje się powierzyć Dostawcy;	**Propozycja PIIT:** usunąć ten punkt **Uzasadnienie:** W punkcie tym występuje także niespójność terminologiczna – czy informacja to dane? Czego w zasadzie miałaby dotyczyć inwentaryzacja? Zakładając, że chodzi o inwentaryzację i klasyfikację danych: a. brak jednolitych wytycznych i narzędzi pozwalających dokonać takiej inwentaryzacji (patrz także poniżej p. i); w zasadzie jedynymi danymi, które są poddane dobrze znanym regułom zapisanym w przepisach prawa to dane niejawne oraz dane osobowe (wraz z danymi szczególnie chronionymi) Porównaj: uwaga do punktu 4.1. a. b. obciążenie Zamawiającego dodatkowym zadaniem
	i. określić wymagania w zakresie bezpieczeństwa i ochrony danych w odniesieniu do każdego poziomu bezpieczeństwa występującego w klasyfikacji;	**Propozycja PIIT**: Usunąć ten punkt **Uzasadnienie**: to wymaganie dotyczy każdego systemu, bez względu na to, czy jest to rozwiązanie umiejscowione w chmurze, czy też w infrastrukturze własnej Odnosi się do nieznanej 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;	**Propozycja PIIT**: usunąć ten punkt **Uzasadnienie**: punkt niejasny i spekulatywny – zakłada wprowadzanie przez Zamawiającego w przyszłości (?) nowych (?) mechanizmów kontrolnych (?) przy jednocześnie ograniczonych możliwościach (?) Zamawiającego. Praktycznie niewykonalne dla ogółu Dostawców.

	***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;*	**Propozycja PIIT:** Usunąć ten punkt **Uzasadnienie**: Analizę wpływu na ochronę danych osobowych (ocena skutków dla ochrony danych, art.35 i nast. RODO) należy przeprowadzić, kiedy jest to wymagane przez prawo bez względu na rodzaj technologii, sposobu jej wykorzystywania. A zatem także dla systemów tworzonych na własnej infrastrukturze. Dlatego też nie ma potrzeby dodatkowo wpisywać tego wymagania do Rekomendacji. Patrz także: Komunikat Prezesa UODO z 24 sierpnia 2018 wskazujący w jakich sytuacjach należy bezwzględnie dokonać oceny skutków dla ochrony danych. W ogólnym przypadku ocena jest wymagana jedynie, gdy dany rodzaj przetwarzania może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (osób, których dane dotyczą).
	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);	**Propozycja PIIT**: usunąć ten punkt **Uzasadnienie:** Takie działania, jak ocena potencjału Dostawcy i Wykonawcy, dotyczą procesu zamawiania, a nie planowania. Zamawiający w postępowaniu może wprowadzić takie wymagania wobec Dostawcy i Wykonawcy jakie uzna za adekwatne w stosunku do planowanego zadania. Niemożliwe do wykonania dla ogółu Dostawców
	m. dokonać analizy zasad funkcjonowania wsparcia technicznego ze strony Dostawcy dla świadczonych usług publicznej chmury obliczeniowej.	**Propozycja PIIT**: usunąć ten punkt **Uzasadnienie:** Takie działania, jak ocena potencjału Dostawcy i Wykonawcy, dotyczą procesu zamawiania, a nie planowania Niemożliwe do wykonania dla ogółu Dostawców

4.2	*Potwierdzenie przeprowadzenia weryfikacji powyższych punktów powinno zostać udokumentowane.*	**Uwaga PIIT**: do zachowania, jeśli faza planowania nie będzie znacząco skrócona. Punkt warty zachowania dla celów rozliczalności przy jednoczesnym wykreśleniu p. 4.3.
4.3	*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).*	**Propozycja PIIT**: punkt do usunięcia **Uzasadnienie:** • W każdej jednostce sektora publicznego istnieją procedury dopuszczające rozpoczęcie procesu zamawiania oraz późniejszej eksploatacji systemów teleinformatycznych – nie ma potrzeby tworzenia dodatkowego procesu • Nie ma równoważności pomiędzy wymaganiami wobec rozwiązania w infrastrukturze własnej, gdzie nie ma postawionych podobnych wymagań, a rozwiązaniem w publicznej chmurze obliczeniowej. Dlaczego analogiczne wymogi związane z weryfikacją i akceptacją nie powinny być nałożone na wdrożenia w infrastrukturze własnej. • Obowiązki osób odpowiedzialnych za bezpieczeństwo informacji, jak i Inspektorów Danych Osobowych są opisane w oddzielnych przepisach. Nie jest oczywiste, że do obowiązków IOD należy weryfikacja i akceptacja np. finansowej strony procesu w chmurze obliczeniowej.

5. Zarządzanie ryzykiem		
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:*	**Propozycja PIIT**: *W analizie ryzyka w szczególności należy uwzględnić:* Uwaga: patrz Propozycja alternatywna dla punktu 5.1.
	a. zakresem oraz ilością i kategoriami przetwarzanych danych osobowych (w szczególności przetwarzanie dużych ilości danych pociąga za sobą wyższe poziomy ryzyka);	**Propozycja PIIT**: wykreślić ten punkt **Uzasadnienie**: Punkt ten dotyczy ochrony danych osobowych (patrz także punkty 5.2. c, d, i), a ograniczenie tego ryzyka można uzyskać w prosty sposób poprzez wymaganie by Dostawca spełniał wymagania nakładane przez RODO na podmiot przetwarzający (patrz Rozdział 6). Nie ma zatem potrzeby wykonywania takiej analizy, gdyż przepisy prawa jednoznacznie określają jakie warunki powinien spełniać taki podmiot. Dodatkowo: taka analiza ryzyka w żaden sposób nie jest punktem specyficznym dla rozwiązań w publicznej chmurze obliczeniowej, a zatem dlaczego tylko w tym przypadku miałaby być wykonywana?
	b. rozproszeniem geograficznym przetwarzanych danych w kontekście zapewnienia zgodności z przepisami prawa obowiązującymi w Polsce, regulacjami zewnętrznymi oraz regulacjami wewnętrznymi Zamawiającego;	**Propozycja PIIT**: Wykreślenie tego punktu Patrz: punkt także 5.2.i.
	c. bezpieczeństwem danych osobowych, w tym ryzyka mające wpływ na prawa i wolności osób, których te dane dotyczą (ocena skutków na ochronę danych);	**Propozycja PIIT:** wykreślić ten punkt **Uzasadnienie**: patrz dyskusja przy punkcie 5.2.a

	d. poszczególnymi czynnościami przetwarzania danych osobowych (w szczególności czynności związane z „profilowaniem" danych osobowych pociągają za sobą wyższe poziomy ryzyka);	**Propozycja PIIT:** wykreślić ten punkt **Uzasadnienie**: patrz dyskusja przy punkcie 5.2.a
	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);	**Propozycja PIIT:** Wykreślenie tego punktu **Uzasadnienie**: ten punkt jest zapisem wymagań jakie powinny znaleźć się przy zamówieniach (Rozdział 6)
	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;	**Propozycja PIIT**: *ocenę jakości i bezpieczeństwa połączenia Użytkowników z publiczną chmurą obliczeniową* **Uzasadnienie**: • zasadnicze uproszczenie tekstu Rekomendacji, • możliwość łatwego określenia poziomu ryzyka (np. wystarczająca, dopuszczalna czy też nieakceptowalna, nieadekwatna) • pozwala na ocenę także wtedy jeśli Użytkownicy będą łączyli się z chmurą z różnych lokalizacji i z pomocą różnych mediów i urządzeń (por. p.5.2.q) • nie jest możliwe enumeratywne wyliczenie wszystkich potencjalnych ryzyk w tekście Rekomendacji bez obawy o pominięcie jakiegoś istotnego punktu

	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);	**Propozycja PIIT:** Wykreślenie tego punktu **Uzasadnienie**: ten punkt jest zapisem wymagań jakie powinny znaleźć się przy zamówieniach (Rozdział 6) także: wymagania wobec podwykonawców nakłada wprost RODO, a potwierdza m.in. ISO 27018
	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;	**Propozycja PIIT**: ocenę procesu integracji z systemami teleinformatycznymi Zamawiającego **Uzasadnienie**: • zasadnicze uproszczenie tekstu Rekomendacji, • możliwość łatwego określenia poziomu ryzyka (np. prosta, dopuszczalna czy też nieakceptowalna kosztowo, nieadekwatna ze względów bezpieczeństwa) • pozwala na ocenę także wtedy jeśli Użytkownicy będą łączyli się z chmurą z różnych lokalizacji i z pomocą różnych mediów i urządzeń • nie jest możliwe enumeratywne wyliczenie wszystkich potencjalnych ryzyk w tekście Rekomendacji bez obawy o pominięcie jakiegoś istotnego punktu

	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;	**Propozycja PIIT:** wykreślić ten punkt **Uzasadnienie**: patrz także 5.2.a Także: • część z zapisanych w tym punkcie wymagań powinna znajdować się w części poświęconej zamówieniom – proponujemy w takim przypadku wyjść od wymagań nakładanych przez RODO na podmiot przetwarzający (patrz Rozdział 6). • uważamy za praktycznie niemożliwe wykonywanie przez niewielkie jednostki sektora finansów publicznych rzetelnej analizy niektórych wskazanych punktów np. oceny ryzyka związane z systemami prawnymi w innych krajach czy sprawdzanie czy jest zapewniony przez Dostawcę zakaz ujawniania danych organom innych państw. • Nie ma możliwości oszacowania ryzyka dla ogółu Dostawców

	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;	**Propozycja PIIT**: *ocenę łatwości stworzenia planu przeniesienia danych do innego Dostawcy lub własnej infrastruktury Zamawiającego* **Uzasadnienie**: • znaczące uproszczenie tekstu Rekomendacji • możliwość dokonywania analiz adekwatnych do złożoności rozwiązań przez każdego Zamawiającego • łatwość odpowiedzi na proponowane pytanie • trudne do opracowania w zakresie opisanym w projektcie ponieważ w procesie zamówień publicznych nie jest znany ostateczny Dostawca (Dostawcy mogą mieć różne warunki migracji)
	k. ograniczoną możliwością sprawowania kontroli nad działalnością Dostawcy w zakresie świadczonych przez niego usług;	**Propozycja PIIT**: wykreślenie tego punktu **Uzasadnienie**: nie jest możliwa rzetelna ocena przed rozstrzygnięciem postępowania o zamówienie i określenie takiego ryzyka dla ogółu Dostawców
	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;	**Propozycja PIIT**: wykreślenie tego punktu **Uzasadnienie**: ten punkt jest zapisem wymagań jakie powinny znaleźć się przy zamówieniach (Rozdział 6) Także: zagadnienia związane z tymi zagadnieniami są przede wszystkim rozwiązywane przez certyfikacje ISO i mogą być analizowane dopiero po wyborze konkretnego Dostawcy

	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;	**Propozycja PIIT**: wykreślenie tego punktu **Uzasadnienie**: zagadnienie nie jest charakterystyczne dla wykorzystania publicznej chmury obliczeniowej
	n. procesem usuwania powierzonych danych oraz brakiem bezpośredniej kontroli nad jego przebiegiem;	**Propozycja PIIT**: wykreślenie tego punktu **Uzasadnienie**: ten punkt jest zapisem wymagań jakie powinny znaleźć się przy zamówieniach (Rozdział 6) Także: zagadnienie to omawia m.in. ISO 27018 oraz NIST 800-88, a zatem łatwo można użyć ich przy formułowaniu wymagań zamówienia; patrz także uwagi w p. 7.2.
	o. możliwością jednostronnego kształtowania i zmiany warunków świadczenia usługi przez Dostawcę w powiązaniu z długością okresu wypowiedzenia umowy;	**Propozycja PIIT**: wykreślenie tego punktu **Uzasadnienie:** • możliwość rzetelnej oceny jest znana dopiero po wyłonieniu konkretnego Dostawcy • zagadnienie to jest omówione w p. 5.2.j.
	p. pogorszeniem jakości świadczenia usług w trybach lub zakresach nieuwzględnianych w parametrach SLA ;	**Propozycja PIIT**: *określenie dopuszczalnego czasu całkowitej lub niepełnej dostępności systemu teleinformatycznego wynikające z przyczyn leżących po stronie Dostawcy* **Uzasadnienie**: taka ocena ryzyka przygotowana przez Zamawiającego pozwoli na lepsze określenie oczekiwań wobec Dostawcy przy procesie zamówienia; istnieje możliwość szacowania ryzyka bez względu na Dostawcę

	q. dostępem z urządzeń mobilnych do systemów przetwarzających dane Zamawiającego;	**Propozycja PIIT**: wykreślenie tego punktu **Uzasadnienie**: czym różniłoby się ryzyko dostępu z urządzeń mobilnych od dostępu z jakichkolwiek innych urządzeń? Dlaczego zostało wyróżnione w szczególny sposób?
	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.	**Propozycja PIIT**: usunięcie tego punktu **Uzasadnienie**: zakres szacowania tego ryzyka jest omówiony w p. 5.2.j. Nie jest możliwe oszacowanie ryzyka dla ogółu Dostawców
5.3	*Po przeprowadzonej ocenie ryzyka powinna zostać opracowana lista mechanizmów niezbędnych do wdrożenia w celu zminimalizowania poziomu zidentyfikowanych ryzyk.*	**Propozycja PIIT:** wykreślenie punktu i przeniesienie merytorycznej zawartości do 5.1 – patrz propozycja 5.1
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.*	**Propozycja PIIT**: połączenie p. 5.4 i 5.6. – patrz poniżej

5.5	*Proces szacowania ryzyka powinien być dokumentowany – w szczególności dokumentowane powinny być zidentyfikowane ryzyka, ich ocena oraz plan minimalizacji zidentyfikowanych ryzyk.*	**Propozycja PIIT:** wykreślenie punktu i przeniesienie merytorycznej zawartości do 5.1. – patrz propozycja 5.1
5.6	*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 potencjalnie mogąca przesądzać o wdrożeniu lub odstąpieniu od wdrożenia bądź o zaprzestaniu korzystania z publicznej chmury obliczeniowej.*	**Propozycja PIIT**: Oszacowane poziomy ryzyka powinny być przedmiotem porównania z poziomami ryzyka rozwiązań niewykorzystujących przetwarzania w publicznej chmurze obliczeniowej. Wynik porównania powinien być uwzględniany jako istotna przesłanka potencjalnie mogąca przesądzać o wdrożeniu lub odstąpieniu od wdrożenia, bądź o zaprzestaniu korzystania z publicznej chmury obliczeniowej. Proces taki należy powtarzać w przypadku zidentyfikowania nowego, istotnego ryzyka lub zmian w zakresie lub trybie wykorzystywania publicznej chmury obliczeniowej. **Uzasadnienie**: uproszczenie zapisów projektu z p. 5.4. i 5.6 Nie ma uzasadnienia dlaczego przegląd ryzyk powinien być robiony co roku.

Uwaga końcowa: Proponujemy połączenie rozdziałów 4 i 5 w jeden „Przygotowanie do wykorzystania przetwarzania w publicznej chmurze obliczeniowej”

6. Wymagania dotyczące umowy z Dostawcą		
6	*Umowa z Dostawcą powinna zapewniać możliwość sprawowania kontroli nad działaniami Dostawcy w zakresie świadczonych przez niego usług, w szczególności powinna zawierać zapisy określające:*	**Propozycja PIIT**: *Warunkiem wykorzystania publicznej chmury obliczeniowej jest zawarcie umowy pomiędzy Zamawiającym a Dostawcą zawierającej:* **Uzasadnienie**: uproszczenie tekstu Rekomendacji oraz wskazanie na wystarczający charakter Rekomendacji dla ogólnego stosowania chmury publicznej w jednostkach sektora finansów publicznych Także: nawiązanie do p. 3.2. mówiącego, że niedopuszczalne jest przetwarzanie w chmurze bez umowy
6.1	*zakresy praw, obowiązków i odpowiedzialności obu stron umowy, w tym podział ról pomiędzy osobami / rolami po stronie Zamawiającego i Dostawcy;*	**Propozycja PIIT:** *zapis wskazujący, że administratorem danych jest Zamawiający, a Dostawca przetwarza dane zgodnie z poleceniami Zamawiającego,* **Uzasadnienie**: wskazujemy na fundamentalną zasadę, że Zamawiający ma całkowite panowanie nad danymi, zaś Dostawca tylko przetwarza dane zgodnie z poleceniami administratora
6.2	*zapewnienie, że świadczenie usług przez Dostawcę odbywać się będzie zgodnie z wymaganiami obowiązujących przepisów prawa, regulacji zewnętrznych oraz regulacji wewnętrznych Zamawiającego;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: jeżeli przyjmujemy zasadę opisaną w p. 6.1. tzn. pełną decyzyjność Zamawiającego to znaczy, że Zamawiający decyduje co robić z danymi. Dostawca nie wie jakie dane przetwarza Zamawiający, ani jaki jest cel przetwarzania i nie ma na to wpływu. To Zamawiający sprawdza (patrz rozdział Planowanie) czy dopuszczalne jest wykorzystanie chmury. W szczególności Dostawca nie zna regulacji wewnętrznych Zamawiającego.

6.3	*zasady opracowania i wdrożenia stosownych polityk i procedur zapewniających prawidłową realizację zleconych czynności oraz bezpieczeństwo danych przekazanych przez Zamawiającego;*	**Propozycja PIIT:** *zapis wskazujący na zapewnienie przez Dostawcę odpowiednich zabezpieczeń technicznych i organizacyjnych w celu ochrony danych Zamawiającego i procesów przetwarzania* **Uzasadnienie**: taki zapis wskazuje na konieczność obecności zapisów dotyczących zabezpieczenia danych i procesu przetwarzania; ocena czy jest to zabezpieczenie „odpowiednie" należy do Zamawiającego i rodzaju wykorzystania chmury.
6.4	*postanowienia / klauzule o powierzeniu przetwarzania przez Dostawcę danych osobowych zgodnie z przepisami o ochronie danych osobowych);*	**Propozycja PIIT**: *zapis wskazujący, że Dostawca w rozumieniu RODO jest podmiotem przetwarzającym* **Uzasadnienie**: najprostszy możliwy zapis dotyczący obowiązków Dostawcy ze względu na przetwarzanie danych osobowych! Jeśli taki zapis istnieje nakłada to na Dostawcę obowiązki ściśle opisane w przepisach, od zapewniania bezpieczeństwa, wsparcia administratora danych osobowych w realizacji żądań osób, których dane dotyczą itd.itp. Dostawca nie wie jakie dane będzie przetwarzał Zamawiający, dlatego też wskazanie, że Dostawca jest podmiotem przetwarzającym w rozumieniu RODO rozwiązuje problem ze sprawdzaniem czy w chmurze są przetwarzane dane osobowe. Dzięki takiemu zapisowi można zrezygnować z wielu kolejnych zapisów w Rekomendacji, gdyż wynikają one wprost z obowiązków podmiotu przetwarzającego!
6.5	*wymóg powołania przez Dostawcę, zgodnie z przepisami o ochronie danych osobowych, inspektora ochrony danych bądź zapewnienie korzystania z usług osoby zewnętrznej pełniącej taką funkcję;*	**Propozycja PIIT**: wykreślić **Uzasadnienie**: zapewnione przez propozycję zapisu w p.6.4

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);*	**Propozycja PIIT:** *zapis wskazujący na lokalizację przechowywania danych Zamawiającego lub możliwość wyboru lokalizacji przechowywania danych przez Zamawiającego, przy czym w obu przypadkach zalecana jest lokalizacja na terenie Europejskiego Obszaru Gospodarczego* **Uzasadnienie**: • Uproszczenie zapisu Rekomendacji • Wskazanie EOG zamiast EU – dla zachowania konsystencji z RODO • Nie jest możliwy zapis, by całość przetwarzania, bez wyjątku, była realizowana na terenie EOG, bo oznaczałoby że dowolny Użytkownik jaki opuścił teren EOG (np. użytkownik maila podczas delegacji w Szwajcarii) byłby całkowicie odcięty od usługi; • Jeśli Zamawiający ma swobodę wyboru lokalizacji to zalecenie lokalizacji na terenie EOG, ale Dostawca – realizujący wyłącznie polecenia Zamawiającego, patrz p. 6.1. - nie ma możliwości zabronienia Zamawiającemu innego wyboru
6.7	*zasady realizacji żądań osób fizycznych oraz sposób współpracy w przypadku wniosków osób fizycznych o realizację praw określonych w przepisach o ochronie danych osobowych;*	**Propozycja PIIT**: wykreślić **Uzasadnienie**: zapewnione przez propozycję zapisu w p.6.4

6.8	*sposób komunikacji pomiędzy Zamawiającym i Dostawcą w sprawach dotyczących bezpieczeństwa informacji, w tym zachowania poufności i ochrony danych osobowych;*	**Propozycja PIIT:** *zapis wskazujący na sposób komunikacji z Dostawcą* **Uzasadnienie**: nie można z góry enumeratywnie określić w jakich sprawach Zamawiający może kontaktować się z Dostawcą, dlatego niezbędny jest tylko ogólny zapis Zapis p.6.4. także nakłada odpowiednie obowiązki na Dostawcę w zakresie komunikacji dotyczącej bezpieczeństwa i naruszeń
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;*	**Propozycja PIIT:** *zapis dotyczący nieujawniania danych Zamawiającego bez polecenia, lub jeśli inne zapisy umowy nie przewidują takich przypadków, oraz o ile obowiązek nie wynika z przepisów prawa* **Uzasadnienie**: • Znaczne uproszczenie zapisu • Wskazanie na „polecenie Zamawiającego" – realizacja zapisu z 6.1. • „Inne zapisy umowy" dotyczą przede wszystkim podwykonawców (podprzetwarzających), którzy mogą mieć dostęp do danych wykonując zlecone czynności przetwarzania np. sprawdzenie ze względów bezpieczeństwa - tu także wystarczający jest zapis z p. 6.4 wskazujący na całkowitą odpowiedzialność podmiotu przetwarzającego za swoich podprzetwarzających • Oczywisty obowiązek wynikający z przepisów prawa Patrz także 6.28

6.10	*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;*	**Propozycja PIIT:** wykreślić w przedstawionej postaci **Uzasadnienie**: zagadnienie zapisane w 6.3. oraz w 6.9 = = = **Alternatywnie (tylko w jednej części odpowiadający pierwotnej propozycji):** *zapis dotyczący zachowania integralności i dostępności danych Zamawiającego w określonym umową okresie po jej wygaśnięciu* Patrz także propozycje uwag przedstawione w p. 7.2
6.11	*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;*	**Propozycja PIIT**: *zapis zobowiązujący personel Dostawcy do ochrony poufności przez, także po zakończeniu zatrudnienia* **Uzasadnienie**: uproszczenie zapisu

6.12	*zasady przekazywania, na żądanie Zamawiającego, listy upoważnionych osób mających dostęp do środowiska przetwarzania wraz z pełnioną przez nie funkcją w organizacji Dostawcy;*	**Propozycja PIIT:** do wykreślenia **Uzasadnienie**: • W przypadku świadczenia usług standardowych takie wymaganie będzie nie do zrealizowania ponieważ ze względów bezpieczeństwa takie dane nie powinny być w ogóle przekazywane, bo przekazanie takiej listy osób – bez ścisłych reguł bezpieczeństwa jest wręcz zaproszeniem do szantażu! = = = **Propozycja alternatywna:** *zapisy dotyczące adekwatnej kontroli dostępu personelu Dostawcy do środowiska przetwarzania*
6.13	*procedury zarządzania dostępem w sposób wykluczający uzyskanie dostępu przez osoby nieuprawnione;*	**Propozycja PIIT**: wykreślić **Uzasadnienie**: zapewnione przez propozycję zapisu w p.6.3., 6.4 oraz 6.12
6.14	*kary umowne z tytułu naruszenia zasad bezpieczeństwa oraz ochrony informacji i danych przekazanych przez Zamawiającego, w tym danych osobowych;*	**Propozycja PIIT**: wykreślić **Uzasadnienie**: zapewnione przez propozycję zapisu w p.6.4
6.15	*obowiązek Dostawcy zapewnienia skutecznego niszczenia danych z uszkodzonych komponentów infrastruktury w przypadku ich wymiany;*	**Propozycja PIIT:** *zapis dotyczący skutecznego usuwania danych* **Uzasadnienie**: • powyższy zapis dotyczy każdej sytuacji usuwania danych, zarówno z zasobów ciągle dostępnych, jak i ze sprzętu przeznaczonego do zniszczenia patrz uwagi w p. 7.2
6.16	*warunki rozwiązania umowy;*	Patrz p. 6.18

6.17	*w przypadku umów zawartych na okres dłuższy niż rok, możliwość bezkosztowego rozwiązania relacji kontraktowej z Dostawcą, z wyprzedzeniem nie dłuższym niż roczne;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: • decyzję czy takie rozwiązanie powinno być zastosowane winna być pozostawiona Zamawiającemu • nie ma możliwości określenia jakie warunki mogą być najbardziej korzystne dla Zamawiających, w tym także dla okresów dłuższych niż rok (przykład: obsługa dwuletniego projektu w ramach zarządzania funduszami europejskimi – wszystkie zasoby są dedykowane tylko na okres projektu) - zapis o bezkosztowym rozwiązaniu może podnosić cenę rozwiązania chmurowego • jeśli umowa jest zawarta na czas określony to rozwiązanie takiej umowy jest możliwe tylko w wyjątkowych wypadkach
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;*	**Propozycja PIIT:** *zapisy dotyczące wypowiedzenia umowy i zasad zwrotu lub usunięcia danych* **Uzasadnienie**: • uproszczenie zapisu • wybór zwrot czy usunięcie danych przez Zamawiającego wynika z zapisu 6.1 • przenoszenie danych pomiędzy Dostawcami nie jest obecnie regulowane żadnymi przepisami (jedynie RODO wskazuje na możliwość takiego przeniesienia, ale dotyczy to realizacji żądania osoby, której dane dotyczą i tylko wtedy jeśli to jest możliwe); w chwili obecnej najwięksi dostawcy usług chmurowych nawiązali porozumienie dotyczące przenoszenia danych, ale nie ma to jeszcze fizycznej realizacji patrz także uwagi do p. 7.2

6.19	*opracowanie i regularne testowanie planu odstąpienia od umowy z Dostawcą (exit-plan);*	**Propozycja PIIT**: wykreślić **Uzasadnienie**: ten punkt należy do części poświęconej eksploatacji chmury obliczeniowej; patrz uwagi do punktu 7.2
6.20	*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;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: to zagadnienie jest rozwiązane poprzez wskazanie, że Dostawca jest podmiotem przetwarzającym w rozumieniu RODO, patrz p. 6.4
6.21	*możliwość wykonywania obowiązków kontrolnych przez organ nadzorczy;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: • taka możliwość wynika z ogólnych przepisów prawa, a nie z umowy pomiędzy Dostawcą i Zamawiającym • w przypadku kiedy Dostawca jest dostawcą usługi cyfrowej w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa takie uprawnienia są wykonywane przez organ właściwy do spraw cyberbezpieczeństwa właśnie z tej ustawy (patrz propozycja w p. 3.0)
6.22	*zgodne z przepisami prawa zakres odpowiedzialności Dostawcy za szkody wyrządzone osobom trzecim;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: ten zapis wynika z powszechnie obowiązujących przepisów i nie ma potrzeby przywoływania go dodatkowo

6.23	*przeniesienie na Zamawiającego prawa do własności intelektualnej;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: • zapis niezrozumiały co do intencji i treści • w zakresie dotyczącym danych odpowiednie zabezpieczenie interesów Zamawiającego znajduje się z propozycji do p. 6.1.
6.24	*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);*	**Propozycja PIIT:** *zapis dotyczący zasad odpowiedniej obsługi incydentów przez Dostawcę* **Uzasadnienie**: • zasady obsługi incydentów mogą być różne w zależności od zadania wykonywanego w publicznej chmurze obliczeniowej • rola podmiotu przetwarzającego dla Dostawcy w rozumieniu RODO nakłada wysokie obowiązki powiadamiania o naruszeniach • Dostawcy, którzy są lub będą dostawcami usług cyfrowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa będą musieli spełniać bardzo wysokie kryteria informowania o incydentach oraz komunikacji z odpowiednimi służbami w kraju

6.25	*okresowe i incydentalne raportowanie z zakresu zagrożeń i zdarzeń bezpieczeństwa w środowisku teleinformatycznym Dostawcy;*	**Propozycja PIIT:** *zapis dotyczący prowadzenia rejestru naruszeń i prowadzenia działań korygujących* **Uzasadnienie**: • Nie ma pewności czy raporty będą adekwatnym sposobem komunikacji w najbardziej ogólnym przypadku np. dla niewielkich JST, szkół itp. • Istotna jest rozliczalność procesu ochrony danych i to zapewnia propozycja zapisu powyżej Patrz także zapisy p. 6.31
6.26	*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;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: zapisy dotyczące wskazanych w tym punkcie zagadnień zostały omówione wcześniej w p.6.6 oraz wynikają z propozycji zapisu p. 6.4

6.27	*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;*	**Propozycja PIIT:** *zapisy dotyczące odpowiednich warunków świadczenia usługi przetwarzania w publicznej chmurze obliczeniowej (SLA), w tym w szczególności ciągłości świadczenia usługi, zasady odpowiedzialności za niedotrzymanie warunków opisanych w SLA, posiadane przez Dostawcę certyfikaty* **Uzasadnienie**: • Zdecydowane skrócenie i uproszczenie zapisu • Część z zapisanych wymogów wynika z tego, że Dostawca jest podmiotem przetwarzającym w rozumieniu RODO – propozycja zapisu p. 6.4 • Zapisy SLA mogą stanowić oddzielną umowę

6.28	*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 (informacja o*	**Propozycja PIIT***: zapisy dotyczące informowania o zmianach dotyczących świadczenia przetwarzania w publicznej chmurze obliczeniowej* **Uzasadnienie**: • Zasadnicze uproszczenie zapisu • W pierwotnej wersji ten punkt dotyczył kilku odmiennych spraw • Propozycja adresuje p. a i b. • Punkt c. jest opisany w 6.9. • Punkty d. i e. wynikają z faktu, że Dostawca jest podmiotem pretwarzającym w rozumieniu RODO Patrz także p. 6.30 oraz propozycja zapisu p. 7.2

	incydencie powinna zostać przekazana Zamawiającemu nie później niż w terminie 36 godzin);	
6.29	*wskazanie przez Dostawcę punktu kontaktowego z zespołem realizującym zadania w zakresie bezpieczeństwa teleinformatycznego chmury obliczeniowej;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: • Temat ujęty w p. 6.8. • Dla przypadków związanych z naruszeniami danych osobowych lub wymogami dla dostawcy usług cyfrowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa obowiązują oddzielne przepisy
6.30	*zasady zarządzania zmianami w świadczonych usługach;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: patrz p. 6.28
6.31	*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;*	**Propozycja PIIT***: zapis o obowiązku rejestrowania zdarzeń przez Dostawcę i umożliwieniu Zamawiającemu dostępu do takiego rejestru* **Uzasadnienie**: • Uproszczenie zapisu • Dla dużej części Zamawiających uzyskiwanie raportów będzie nadmiarowe (patrz uwagi do p. 6.25) • Zamawiający mając dostęp do rejestru zdarzeń może swobodnie kształtować swój zakres pozyskiwanych informacji
6.32	*politykę wykonywania kopii zapasowych oraz zapewnienia ciągłości działania;*	**Propozycja PIIT**: wykreślić **Uzasadnienie**: temat zapisany w 6.27

6.33	*parametry odtworzenia po katastrofie, w tym parametry dotyczące ciągłości działania usług świadczonych przez Dostawcę (w tym parametry RTO i RPO);*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: temat zapisany w 6.27
6.34	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;	**Propozycja PIIT**: wykreślić **Uzasadnienie**: zapewnione przez propozycję zapisu w p. 6.4.
6.35	listę podwykonawców Dostawcy z lokalizacjami wraz z określeniem zakresu czynności świadczonych przez podwykonawców;	**Propozycja PIIT**: wykreślić **Uzasadnienie**: zapewnione przez propozycję zapisu w p.6.4
6.36	zasady przekazywania, na żądanie Zamawiającego, listy upoważnionych osób zatrudnionych przez Dostawcę oraz przez podwykonawców Dostawcy, mających lub mogących mieć dostęp do danych Zamawiającego;	**Propozycja PIIT**: wykreślić **Uzasadnienie**: zapewnione przez propozycję zapisu w p.6.4

6.37	zasady odpowiedzialności Dostawcy za działania i zaniechania jego podwykonawców (za działania i zaniechania swoich podwykonawców Dostawca odpowiada jak za własne działania i zaniechania);	**Propozycja PIIT**: wykreślić **Uzasadnienie**: zapewnione przez propozycję zapisu w p.6.4
6.38	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.	**Propozycja PIIT:** wykreślić **Uzasadnienie**: • Jeśli wsparcie techniczne wychodzi poza zapisy SLA to jest opisane oddzielnymi umowami, zróżnicowanymi pod względem zasad i kosztów dla różnych podmiotów • Pozostałe elementy zapisane w p. 6.27

7. Realizacja umowy (dotyczącej wykorzystania publicznej chmury obliczeniowej) **Propozycja PIIT: Połączenie rozdziału 7 i 8 w jeden pn. „Zasady eksploatacji systemów teleinformatycznych wykorzystujących przetwarzanie w publicznej chmurze obliczeniowej”**		
7.0.		**Propozycja PIIT:** *Zamawiający, samodzielnie lub w porozumieniu z Dostawcą lub/i Wykonawcą, powinien mieć przygotowane rozwiązania techniczne, polityki i oceny ryzyk zgodnie z przyjętymi w tej jednostce zasadami eksploatacji systemów teleinformatycznych poszerzone o wymienione niżej dotyczące przetwarzania w publicznej chmurze obliczeniowej.* **Uzasadnienie:** • Wykorzystanie przetwarzania w publicznej chmurze obliczeniowej wymaga pewnych dodatkowych działań w trakcie eksploatacji – ten punkt jest wprowadzeniem do listy niezbędnych działań. • Podczas eksploatacji znany jest już konkretny Dostawca, także można oceniać ryzyka poszczególnych działań w chmurze na podstawie konkretnych zapisów umów (patrz uwagi do Rozdziału 5 „Zarządzanie ryzykiem”) • Część z zagadnień należy do Zamawiającego, a część może być elementem umów z Dostawcą i Wykonawcą. Zakres tych umów może być bardzo różnorodny w zależności od rozwiązań

7.1	*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.*	**Propozycja PIIT:** skreślić jako oddzielny punkt. **Uzasadnienie**: tematyka omówiona w p.7.2.b

7.2	*Zamawiający i Dostawca, w ramach swoich zakresów kompetencji, powinni zapewnić m.in.:* *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;*	**Propozycja PIIT:** *Zamawiający zgodnie z przyjętymi w jednostce zasadami dokumentuje przyjęte zasady eksploatacji systemu teleinformatycznego, a w szczególności dla systemu zawierającego przetwarzanie w publicznej chmurze obliczeniowej:* a. **Skreślić** – opis tej tematyki we wprowadzającej propozycji p. 7.0 b. *Zasady i polityki bezpieczeństwa informacji związane z szyfrowaniem przesyłu i przechowywania danych* **Uzasadnienie**: taki zapis pozwala na przygotowanie zasad i ich zróżnicowania (patrz p. c.) zgodnie z potrzebami konkretnego systemu i jego Użytkowników, ich kanałów dostępu do usług, a także sprawdzenie nie tylko integralności, ale i innych cech bezpieczeństwa informacji Patrz także zapisy p. 5.2.e. c. **Skreślić** – ogólny zapis punktu b. obejmuje także ten punkt *d. Zasady i polityki uwierzytelniania Użytkowników (jeśli inne niż dla systemów w infrastrukturze własnej)* e. *Ocenę ryzyka związaną z dostępnością usług chmurowych lub ich niewystarczającą jakością* **Uzasadnienie**: Zamawiający ocenia ryzyko nie tylko związane z SLA Dostawcy, ale także z możliwością przerwania połączenia z usługą chmurową, co zależy od dostępności usług telekomunikacyjnych (ten punkt obejmuje także zapisy z p. h., i. oraz j.– patrz także zapisy p. 5.2 f); zakres oceny będzie zależał od tego jaka jednostka, do jakich danych i do jakich celów będzie przygotowywać tę ocenę, a także od przyjętej w tej jednostce metodyce oceny

	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 i RPO 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*	**f. Skreślić –** zapisane w punkcie b. g. **Skreślić** – część tematyki (uwierzytelnianie) jest w omówione w punkcie d., natomiast integracja z innymi systemami dotyczy w takim samym stopniu rozwiązań chmurowych, jak i rozwiązań w infrastrukturze własnej h. **Skreślić** - zapisane w punkcie e. i. **Skreślić** – zapisane w punkcie e. j. **Skreślić** – zapisane w punkcie e. k. Przesunięte do punktu 7.2.o. *l. Zasady i polityki związane z archiwizacją danych i tworzenia kopii zapasowych w zasobach niezależnych od wykorzytywanej publicznej chmury obliczeniowej* m. **Skreślić** – zbyt szczegółowe, klasyfikacja danych (jeśli jest zrobiona) zależy od specyfiki Zamawiającego, a pozostałe elementy zapisane w punkcie l. *n. Zasady i polityki związane z obsługą incydentów bezpieczeństwa i naruszeń związanych z ochroną danych osobowych* Dodatkowo proponujemy poszerzenie tego punktu o treści zapisane w Rozdziale 8. lub stworzenie oddzielnego punktu w Rozdziale 7 o. *Ocenę ryzyka związaną z zakończeniem korzystania z usługi przetwarzania w publicznej chmurze obliczeniowej obejmującą co najmniej* a. *Ryzyko zaprzestania korzystania z usług świadczonych przez Dostawcę,*

	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.*	*b. Ryzyko związane z wykonaniem niezbędnych procesów pomiędzy zakończeniem korzystania z usługi a usunięciem przez Dostawcę danych Zamawiającego,* c. *Ryzyko związane z usuwaniem danych Zamawiającego po zakończeniu przetwarzania, w tym także związaną z fizycznym niszczeniem nośników.* **Uzasadnienie**: Uproszczenie zapisu Rekomendacji Zaadresowanie tematyki z p. 8 oraz z p. 7.k. Zakres i objętość oceny ryzyka zależy od Zamawiającego. Ryzyko zaprzestania korzystania z usług może wynikać z wielu przyczyn: zmian w oferowanej usłudze, problemami ze zgodnością z prawem, zbyt niskim poziomem świadczonego SLA, nieakceptowalnymi podatnościami, praktykami Dostawcy, również sytuacją rynkową Dostawcy (bankructwo, przejęcie) itd. itp. Ryzyko związane z wykonaniem niezbędnych procesów to sprawy związane zarówno ze stroną techniczną (przeniesienie danych, migracje), rozliczenia, warunków prawnych, ale także ryzyka związane z możliwością wznowienia lub kontynuacji usługi Ryzyko związane z usuwaniem danych to zagadnienie związane z bezpieczeństwem w trakcie (dynamiczne przydzielanie zasobów np. pamięci masowych) i po zakończeniu korzystania z usług chmurowych Dostawcy, a także zasady przyjęte przez Dostawcę związane z niszczeniem fizycznych zasobów.

		p. Plan działań związanych z zakończeniem wykorzystywania przetwarzania w publicznej chmurze obliczeniowej **Uzasadnienie**: jak dokładny i szczegółowy ma być ten plan, czy powinien obejmować wydarzenia nagłe czy tylko planowe zakończenie – to zależy od oceny ryzyka zapisanej w punkcie. o. oraz zasad przyjętych w konkretnej jednostce sektora finansów publicznych Ten zapis odpowiada tematyce z p. 8.3.

8. Realizacja umowy (dotyczącej wykorzystania publicznej chmury obliczeniowej)		
8.1	Zamawiający powinien posiadać (..)	**Propozycja PIIT**: zagadnienia przeniesione do p. 7.2
8.2	W celu ograniczenia ryzyka (..)	
8.3	Zamawiający powinien opracować i przetestować plan (..)	