UWAGI

Polskiej Izby Informatyki i Telekomunikacji [PIIT]

do drugiego projektu Rekomendacji Ministra Cyfryzacji dotyczących warunków przetwarzania w chmurze publicznej danych podmiotów publicznych.

Polska Izba Informatyki i Telekomunikacji (PIIT) z zadowoleniem wita fakt, że wiele spośród naszych postulatów przedstawionych podczas pierwszego etapu konsultacji zostało wzięte pod uwagę i wykorzystane przy tworzeniu obecnego projektu. Mamy nadzieję, że poniższe uwagi również staną się podstawą do dalszego uproszczenia i ułatwienia stosowania publicznej chmury obliczeniowej w praktyce administracji w Polsce.

Ostatnie dni pokazały, że istnieje pilna potrzeba przygotowania Rekomendacji! Chmura publiczna w znaczący sposób może w znaczący sposób podnieść bezpieczeństwo informacji w jednostkach administracji, zwłaszcza tam, gdzie brakuje zasobów (ludzie, wiedza, budżet). Dosadnie pokazał to ostatnio opublikowany raport NIK po kontroli w JST w województwie podlaskim, https://www.nik.gov.pl/aktualnosci/bezpieczenstwo-informacji-woj-podlaskie.html:

> *Wszelkie informacje o obywatelach, w tym dane wrażliwe, przechowywane w formie elektronicznej przez jednostki samorządowe, nie są odpowiednio zabezpieczone przed nieuprawnionym dostępem - alarmuje NIK po kontroli na Podlasiu. Dane mogą w każdej chwili zostać przejrzane, przejęte lub zniszczone. Samorządy nie wiedzą nawet, kto ma do nich dostęp, gdyż nie monitorują tych kwestii. Większość skontrolowanych jednostek nawet nie podejmuje działań minimalizujących ryzyko utraty informacji. (…)* ***(Dane) Przechowywane były w miejscach ogólnodostępnych, bez możliwości zamknięcia. Instytucje nie sporządzały kopii bezpieczeństwa baz danych lub tworzyły je w niewłaściwy sposób (np. nie kopiując wszystkich danych). Zdarzało się, że nośniki, na których zapisywano kopie, przechowywano w tym samym pomieszczeniu co oryginały, co w żaden sposób nie gwarantuje im bezpieczeństwa.***

Każdy kto miał do czynienia z profesjonalnymi rozwiązaniami chmurowymi zauważy, jak łatwo pozbyć się słabości wskazywanych po ostatniej kontroli NIK! Dlatego też brak prostych i łatwych do zastosowania Rekomendacji (podkreślmy: prostych i łatwych do zastosowania! Pisaliśmy o tym w naszych uwagach z 31 sierpnia 2018 roku) w sposób bezpośredni konserwuje niski poziom bezpieczeństwa! W świetle obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa jakie spadają zarówno na administrację, jak i organy właściwe dla cyberbezpieczeństwa przygotowanie i przedstawienie Rekomendacji jest naprawdę pilne.

Oczywiście problemy o jakich mówi ostatni raport NIK nie są wyłącznie domeną samorządów – Naczelna Izba Kontroli w poprzednich latach przedstawiała raporty dotyczące jednostek administracji centralnej. Wnioski nie były optymistyczne.

Zanim przejdziemy do szczegółowych uwag chcielibyśmy przedstawić kilka ogólnych uwag do Rekomendacji:

Uwaga 1: Równoważność rozwiązań chmurowych i w infrastrukturze własnej.

Powtórnie chcemy podkreślić, że PIIT podczas tworzenia uwag do projektu Rekomendacji Ministra Cyfryzacji dotyczących warunków przetwarzania w chmurze publicznej danych podmiotów publicznych (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.

W szczególności chcemy podkreślić, że zasada neutralności technologicznej powinna odnosić się do równego traktowania rozwiązań chmurowych i rozwiązań stworzonych w infrastrukturze własnej (ang. on-premise). **Czas, wysiłek i zasoby jakie są poświęcone na sprawdzenie wymagań dotyczących rozwiązania chmurowego powinien być podobny jak dla rozwiązania on-premise.**

Uwaga 2: Konieczność opracowania klasyfikacji danych i odpowiadających im wymaganiom bezpieczeństwa.

W trakcie prac nad tekstem Rekomendacji wielokrotnie natrafialiśmy na barierę niedostatecznego opisu i klasyfikacji danych jakie przetwarzają jednostki administracji publicznej. Poddaliśmy krytyce zapisy w pierwszej wersji Rekomendacji dotyczące wyłączeń z możliwości stosowania chmury (np. wyłączające rejestry państwowe ustanowione ustawą) jako nieadekwatne do potrzeb.

PIIT chętnie włączy się w prace nad stworzeniem spójnego systemu klasyfikacji danych i odpowiadających im wymaganiom bezpieczeństwa. Niestety, nie potrafimy w tak krótkim czasie zaproponować satysfakcjonującego rozwiązania. W chwili obecnej rozpoczęliśmy kwerendę zbierając informacje w jaki sposób rozwiązano ten problem w innych krajach. Zakładamy przy tym, że niezależnie od dzielących kraje różnic, pewne fundamentalne zasady będą mogły być wprowadzone.
Przypominamy także, że pewne prace związane z klasyfikacją danych (wykorzystaniem metadanych) były już prowadzone i są dostępne na epuap.gov.pl na Portalu Interoperacyjności.

Nasza bardzo wstępna analiza zagadnienia klasyfikacji danych wskazuje – oprócz dość oczywistego podziału na dane osobowe oraz dane nieosobowe – na rozpoczęcie prac poprzez rozważenie klasyfikacji danych w oparciu wykładni ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (**„uDIP”**); Dalej:

a. zgodnie z:
i. art. 1 ust. 1 uDIP:
Każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu na zasadach i w trybie określonych w niniejszej ustawie
ii. art. 5 ust. 1 uDIP:
Prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych
b. w oparciu o brzmienie zacytowanych w punkcie b. przepisów można dokonać podziału na:
i. informacje **publiczne dostępne**, oraz
ii. informacje **niedostępne publicznie**, wśród których należy dokonać **podpodziału** na:
— informacje niejawne w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (**„uOIN”**), które to informacje powinny podlegać **dalszemu podpodziałowi**, stosownie do uwagi w punkcie iii.;
— informacje ustawowo chronione, które nie stanowią informacji niejawnych w rozumieniu uOIN (np. podlegające ochronie na podstawie ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze, ustawy z dnia 6 lipca 1982 r. o radcach prawnych, ustawy z dnia 14 lutego 1991 r. Prawo o notariacie, ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe etc. I szereg innych tajemnic zawodowych);
— ewentualnie „dane osobowe” – jako dane, do których znajdują zastosowanie szczegółowe i dosyć rozbudowane regulacje prawne i wymogi
iii. w ramach informacji niejawnych w rozumieniu uOIN i stosownie do klasyfikacji zaproponowanej w rozdziale 2 uOIN, te informacje należy podzielić na:
— informacje o klauzuli „ściśle tajne” (por. art. 5 ust. 1 uOIN);
— informacje o klauzuli „tajne” (por. art. 5 ust. 2 uOIN);
— informacje o klauzuli „poufne” (por. art. 5 ust. 3 uOIN);
— informacje o klauzuli „zastrzeżone” (por. art. 5 ust. 4 uOIN), a ewentualnie także
— informacje przekazane przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych (por. art. 5 ust. 5 uOIN), przy czym te informacje oznacza się polskim odpowiednikiem posiadanej klauzuli tajności (przykładowo w przypadku klauzul NATO wyróżnia się:
a. COSMIC TOP SECRET (odpowiednik polski: ŚCIŚLE TAJNE);
b. NATO SECRET (odpowiednik polski: TAJNE);
c. NATO CONFIDENTIAL (odpowiednik polski: POUFNE);
d. NATO RESTRICTED (odpowiednik polski: ZASTRZEŻONE);

Proponujemy by rozwiązaniem zastosowanym w Rekomendacjach było wyłączenie ich bezpośredniego stosowania dla enumeratywnej lista specyficznych danych lub niektórych podmiotów administracji. Dzięki temu podmioty, które znalazły się na liście wyłączeń będą mogły stosować chmurę publiczną, ale po ich stronie pozostanie stworzenie własnej listy wymagań, zasad

stosowania itd. Co więcej, zakładamy również, że w ramach dalszego rozwoju usług chmurowych, ich certyfikacji i formalnych wymogów organizacyjno-technicznych lista ta może ulegać zmianie!
Uznajemy jednak, że brak klasyfikacji danych adekwatnej do dzisiejszych sposobów przetwarzania danych nie powinien w żadnym stopniu wstrzymać prac nad Rekomendacjami.

Uwaga 3: Rekomendacje a istniejące i wprowadzane przepisy prawa

Rekomendacje w sposób oczywisty są uzupełnieniem i praktycznymi wskazówkami dla stosowania istniejących przepisów prawa. Dlatego też uważamy, że nie powinny powtarzać zapisów aktów prawnych, a **tam, gdzie to niezbędne tylko wskazywać na odpowiednie zapisy**. Rozwiązanie takie pozwala utrzymać spójność i ułatwić pracę beneficjentom Rekomendacji. Unikamy też przypadku, w którym po nowelizacji aktu prawnego należałoby również zmieniać zapisy Rekomendacji.

W ramach naszych prac nad uwagami braliśmy pod uwagę przede wszystkim następujące akty prawne:

a. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005 roku z dalszymi zmianami (dalej: ustawa o informatyzacji)
    a. Rozporządzenia do ustawy o informatyzacji, w szczególności Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (dalej: KRI)
b. 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, dalej: RODO)
c. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
d. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
e. Projekt Rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie swobodnego przepływu danych nieosobowych w Unii Europejskiej
f. Ustawa Prawo zamówień publicznych

Uwaga 4: Wskazanie na potencjalną potrzebę nowelizacji aktów prawnych

W naszych uwagach szczegółowych przedstawiamy także propozycje przeniesienia niektórych zapisów projektu Rekomendacji do istniejących lub nowych aktów prawnych. W szczególności dotyczy to zapisów, które nakładają na Zamawiających obowiązki, które nie są precyzyjnie opisane w obecnym stanie prawnym. Wskazujemy na takie zapisy tam, gdzie ma sens wprowadzenie powszechnie stosowanych zasad bez względu na to czy rozwiązanie ma charakter chmurowy czy on-premise. Przykładem może być wspomniane wyżej (Uwaga 2) klasyfikowanie danych, ale także prowadzenie analizy ryzyka czy tworzenie dokumentacji projektowej dotyczącej wymagań organizacyjnych i technicznych dla systemów realizujących zamówienia publiczne.

Uznajemy, że wprowadzanie takich zapisów w Rekomendacji – zapisów nie zawsze jasnych, ale zawsze obciążających Zamawiającego – stanowi **brak równoważności dla rozwiązań chmurowych i w infrastrukturze własnej, a tym samym może stanowić naruszenie ustawowej zasady neutralności technologicznej.**

Uwaga 5: Wypełnienie wymogów Rekomendacji jest wystarczające dla zamówienia i stosowania chmury publicznej.

Chcieliśmy ponownie – tak jak w sierpniu br. – podkreślić, że Rekomendacje mają służyć ułatwieniu zamawiania i wykorzystania chmury nawet przez małe jednostki administracji, 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.

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.

Tam, gdzie dzisiaj granice nie są jasno postawione należy zastosować wprost zasadę, że dozwolone jest to co nie jest zabronione! Takie podejście powinno być wprost wskazane przez Rekomendacje!

Podsumowanie Części I

Podsumowując pierwszą część naszych uwag Polska Izba Informatyki i Telekomunikacji chcieliśmy powtórzyć

- **Zasada neutralności technologicznej**, czyli brak dyskryminacji i brak preferencji dla rozwiązań informatycznych ma zastosowanie dla rozwiązań chmurowych. Zasada ta jest zapisana zarówno w ustawie o informatyzacji, jak i dokumentach europejskich (Europejskie Ramy Interoperacyjności[1]). Nakładanie nierównych warunków na rozwiązania chmurowe w porównaniu z rozwiązaniami w infrastrukturze własnej jest naruszeniem tej zasady
- Ze względu na trudność z opracowaniem odpowiadających potrzebom zasad klasyfikacji danych bazujących na aktualnym stanie prawnym **proponujemy zastosowanie zapisu, że Rekomendacje nie mają bezpośredniego zastosowania do wymienionych enumeratywnie rodzajów danych**. Takie rozwiązanie nie zamyka drogi rozwiązaniom chmurowym, a jedynie nakłada na potencjalnego Zamawiającego konieczność opracowania własnych reguł stosowania chmury. Natomiast Ministra Cyfryzacji chroni przed zarzutem nakładania ograniczeń nie mających podstawy prawnej.
- Rekomendacje powinny tylko przywoływać definicje i zapisy aktów prawnych, aby ułatwić Zamawiającym szybką orientację w poruszanych zagadnieniach. Tam gdzie to możliwe zapis Rekomendacji powinien wprost wskazywać z jakiego aktu prawnego wynika.
- **Rekomendacje powinny wypełniać postulat minimalnych wymagań dla zastosowania chmury w ogólnym przypadku**.
- Proponujemy wydzielenie i usunięcie części zapisów Rekomendacji ze względu na to, że powinny one znaleźć się w innych aktach prawnych, dotyczą zarówno systemów w publicznej chmurze obliczeniowej, jak i systemów on-premise - zaś ich obecność w Rekomendacjach może naruszać neutralność technologiczną i preferować jedne rozwiązania względem innych.

[1] https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf , str. 14 i nast.

Proponujemy rozważenie konsultacji Rekomendacji z Urzędem Zamówień Publicznych pod względem zgodności proponowanych zapisów z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych, podobnie jak to nastąpiło w przygotowanych przez Ministerstwo Cyfryzacji wzorcowych klauzulach umownych w wersji 2.0, tym bardziej, że:

a) z uwagi na to, iż Rekomendacje dotyczą podmiotów publicznych, to zamówienia na usługi chmurowe tych podmiotów z reguły będą następować w reżimie zamówień publicznych;
b) Urząd Zamówień Publicznych w przeszłości (w 2009 r., por. punkt I. 2. c. powyżej) przygotowywał rekomendacje w zakresie zakupu systemów informatycznych, a te rekomendacje – z uwagi na upływ aż 9 lat od czasów ich powstania i istotny postęp technologicznych oraz dosyć duże zmiany w zakresie prawa zamówień publicznych – powinny zostać zaktualizowane stosownie do zmian, które nastąpiły od 2009 r.;

PIIT deklaruje włączenie się do dalszych prac mających na celu:

- ułatwienie procesów planowania i zarządzania ryzykiem – w tym przypadku chcielibyśmy zaproponować stworzenie narzędzi informatycznych, które pozwolą w sposób łatwy, szybki i prosty dokonywać odpowiednich analiz
- konsultację społeczną przy nowelizacji istniejących i nowych aktów prawnych
- prace przy zadaniach szczególnych jak np. nowy system klasyfikacji danych

Chcielibyśmy zaproponować by prace jakie rozpoczęły się przy tekście Rekomendacji były kontynuowane z udziałem wszystkich interesariuszy oraz zewnętrznych ekspertów. Uznajemy, że rozwiązania w chmurze obliczeniowej mają ogromny potencjał oraz pomagają w rozwiązaniu wielu problemów polskiej administracji jak np. cyberbezpieczeństwo.

Uwagi Szczegółowe

	Projekt Rekomendacji Ministerstwa Cyfryzacji	Uwagi/Propozycje zmian PIIT
0.1.	**Tytuł**: *"Rekomendacje Ministra Cyfryzacji dotyczące warunków przetwarzania w chmurze publicznej danych podmiotów publicznych."*	**Propozycja zmiany tytułu**: *Rekomendacje Ministra Cyfryzacji, dotyczące warunków przetwarzania w chmurze publicznej w jednostkach sektora finansów publicznych.* **Uzasadnienie**: Podtrzymujemy naszą poprzednią propozycję. Prócz uzasadnienia jakie przedstawiliśmy w uwaga z 31 sierpnia 2018 (patrz niżej) chcielibyśmy zwrócić uwagę, że określenie „dane podmiotów publicznych" może spowodować poważny chaos. Czy każdy podmiot, w tym także podmiot komercyjny lub obywatel, który zamierza przetwarzać w chmurze dane podmiotów publicznych powinien stosować te rekomendacje np. firma budowlana, która otrzymała drogą elektroniczną decyzję administracyjną? Czy informacja publiczna, np. serwer BIP hostowany u lokalnego dostawcy, podlega tym samym rygorom jak złożone rozwiązanie dla centralnego resortu? Patrz także: uwaga ogólna nr 2 Uwagi z 31 sierpnia: 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).

1. Zakres stosowania rekomendacji		
1.3a		**Propozycja PIIT:** *1.3.a Rekomendacje nie mają zastosowania dla:* • *przetwarzania informacji niejawnych* • *…* *W wymienionych wyżej przypadkach, kiedy podmiot sektora finansów publicznych zamierza zastosować publiczną chmury obliczeniowej powinien samodzielnie przygotować analizę wymagań, ryzyk oraz potencjalnych ograniczeń prawnych stosowania chmury obliczeniowej.* **Uzasadnienie:** Ze względu na trudność z opracowaniem odpowiadających potrzebom zasad klasyfikacji danych bazujących na aktualnym stanie prawnym proponujemy zastosowanie zapisu, że Rekomendacje nie mają zastosowania do wymienionych enumeratywnie sytuacji, rodzajów danych czy wręcz podmiotów. Takie rozwiązanie nie zamyka drogi rozwiązaniom chmurowym, a jedynie nakłada na potencjalnego Zamawiającego konieczność opracowania własnych reguł stosowania chmury. Natomiast Ministra Cyfryzacji chroni przed zarzutem nakładania ograniczeń niemających podstawy prawnej. Taki zapis będzie także bardzo pomocny dla Zamawiających oraz spełni postulat, że co nie jest zabronione jest dozwolone W chwili obecnej – ze względu na brak czasu i konieczność szerszej dyskusji – pozostawiamy listę pustą, a jako przykład podajemy przetwarzanie informacji niejawnych. Wprawdzie dzisiaj nie jest możliwe przetwarzanie w chmurze publicznej informacji niejawnych, ale należałoby się zastanowić czy nie można – oczywiście pod dodatkowymi warunkami! – dopuścić do przetwarzania informacji opatrzonych klauzulą ZASTRZEŻONE!

2. Definicje		
1.5. a		**Propozycja PIIT:** *Dostawca Usługi Cyfrowej – podmiot będący dostawcą usługi przetwarzania w chmurze w rozumieniu ustawy z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa.* **Uzasadnienie**: Wdrożenie ustawy o krajowym systemie cyberbezpieczeństwa (UKSC) stworzyło Dostawców Usługi Cyfrowej, nową kategorię podmiotów świadczących usługi cyfrowe, które mogą być wykorzystane również do wykonywania usług kluczowych. Na podmioty te zostały nałożone dodatkowe specjalne wymagania, zaś nadzór i kontrolę sprawuje nad nimi – jako organ właściwy ds. cyberbezpieczeństwa – minister właściwy ds. informatyzacji. PIIT spodziewa się, że wiele firm będzie dążyło i osiągnie status Dostawcy Usługi Cyfrowej, a zatem jeśli będą one zweryfikowane i przygotowane do świadczenia przetwarzania w chmurze dla usługi kluczowej to tym bardziej będzie to właściwy Dostawca w ogólnym przypadku stosowania chmury. Pozostawiamy decyzji resortu czy przy stosowaniu w Rekomendacjach pojęcia Dostawcy Usługi Cyfrowej ograniczyć ją tylko do dostawcy usługi przetwarzania w chmurze czy rozciągnąć także na pozostałe dwa typy DUC wymienione w Załączniku nr 2. Patrz UKSC: art.2 p15) – definicja usługi kluczowej Rozdział 4, art. 17-20 „Obowiązki dostawców usług cyfrowych” Rozdział 11, art. 53 i nast. „Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa” Załącznik nr 2 do ustawy Oraz Rozporządzenie Wykonawcze Komisji (UE) 2016/1148 z 30 stycznia 2018 r.

1.9.	*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.* .	**Propozycja PIIT**: *Neutralność technologiczna – definicja równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji zapisana w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005 roku z dalszymi zmianami, art. 3, p.19)* **Uzasadnienie**: wprowadzenie podstawy prawnej stosowanej w Rekomendacjach definicji.

3. Kryteria równoważności przetwarzania w chmurze		
1.11	*Przetwarzanie danych w chmurze publicznej jest równoważne przetwarzaniu w infrastrukturze własnej Zamawiającego, jeśli spełnione są następujące wymagania:*	**Propozycja PIIT:** *Przetwarzanie danych w chmurze publicznej jest zgodnie z zasadą neutralności technologicznej równoważne przetwarzaniu w infrastrukturze własnej Zamawiającego, jeśli spełnione są następujące wymagania:* **Uzasadnienie:** Wskazanie zasady neutralności technologicznej podkreśla brak preferencji i brak dyskryminacji rozwiązania chmurowego względem rozwiązania on-premise.

1.11	*Przetwarzanie danych w chmurze publicznej jest równoważne przetwarzaniu w infrastrukturze własnej Zamawiającego, jeśli spełnione są następujące wymagania: (..)* *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.*	**Propozycja PIIT**: *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 lub Dostawca jest Dostawcą Usługi Cyfrowej.* **Uzasadnienie**: Wymagania wobec Dostawcy Usługi Cyfrowej (DUC) są ściśle określone, nadzór i kontrolę nad Dostawcami Usług Cyfrowych sprawuje minister właściwy ds. informatyzacji, a także mogą być na nich nakładane kary. Skoro usługa DUC może mieć zastosowanie do usług kluczowych to znaczy, że musi także spełniać warunki dla ogólnego zastosowania chmury. Patrz także uwaga 1.5.a.

4. Planowanie przetwarzania w publicznej chmurze obliczeniowej **5. Zarządzanie ryzykiem**		
1.13 – 1.15		**Propozycja PIIT:** Proponujemy radykalną zmianę Rozdziału 4 i Rozdziału 5.

		Uzasadnienie: 1. W znacznej części wymagania stawiane przed Zamawiającym dotyczą w równym stopniu systemów w publicznej chmurze obliczeniowej i systemów w infrastrukturze własnej. Nie ma powodu by tylko systemy chmurowe podlegały zasadom opisanym w Rekomendacjach przy braku podobnych wymagań dla systemów on-premise 2. Niektóre zapisy w obu Rozdziałach wynikają z przepisów prawa i mają zastosowanie wprost niezależnie od obecności w Rekomendacjach czy też nie. Problematyczne natomiast staje się utrzymanie integralności Rekomendacji w przypadku zmian w prawie. Przykładem niech będą częste odwołania do RODO, które mogą być modyfikowane ze względu na zatwierdzone kodeksy postępowania czy nowelizacje innych aktów prawnych związanych z RODO, a dotyczących określonego typu danych. 3. Część wymagań związana jest z działaniami na nieokreślonych prawem obszarach – w części I zwracaliśmy uwagę na niewystarczający sposób klasyfikacji danych, podobnie z metodykami oceny ryzyka itd. Bardzo trudno oczekiwać by ktoś odpowiedzialnie chciał się podpisać pod dokumentacją projektową bazującą na tak niepewnym gruncie (por. punkt 1.15) 4. Wymagania w rozdziale 4 i 5 są bardzo rozległe i wymagające bardzo dużych zasobów (projekt Rekomendacji mówi np. wprost o „kompleksowym szacowaniu ryzyka”). To z kolei będzie oznaczało, że wykorzystanie chmury obliczeniowej tam, gdzie byłoby najbardziej wskazane np. w niedoinwestowanych jednostkach samorządu terytorialnego będzie jeszcze bardziej utrudnione.

		Dlatego proponujemy: Oba rozdziały połączyć w jeden pn. „Planowanie przetwarzania w publicznej chmurze obliczeniowej”. Rozdział ten dotyczyć powinien wyłącznie działań po stronie Zamawiającego – kolejne rozdziały zaś definiują zadania Dostawcy. Zapisy tych rozdziałów przedstawić następująco: *1.13. Planowanie systemu realizującego zadania publiczne z zastosowaniem przetwarzania w publicznej chmurze obliczeniowej podlega tym samym przepisom jak planowanie dla systemu w infrastrukturze własnej Zamawiającego, w szczególności winny być spełnione wymagania nakładane przez Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.* *1.14. Planowanie przetwarzania w publicznej chmurze obliczeniowej, w tym oszacowanie ryzyk, winno być udokumentowane.* *1.15. Dokumentacja planowania powinna zawierać w szczególności:* *a. brak znanych przeciwwskazań dla przetwarzania w publicznej chmurze obliczeniowej zgodnie z zasadami przedstawionymi w niniejszych Rekomendacjach, w szczególności w Rozdziałach 1 i 3,* *b. nałożenie w procesie zamówienia wymagań wobec Dostawcy przedstawionych w niniejszych Rekomendacjach lub potwierdzenie, że przetwarzanie w publicznej chmurze obliczeniowej jest realizowane przez Dostawcę Usługi Cyfrowej,* *c. wykaz korzyści związanych z bezpieczeństwem, niezawodnością, integralnością i dostępnością w stosunku do rozwiązania w infrastrukturze własnej Zamawiającego, w tym porównanie podstawowych ryzyk dla obu rozwiązań i sposobów ich minimalizacji,*

		d. wskazanie korzyści finansowych w stosunku do rozwiązania w infrastrukturze własnej Zamawiającego, e. *sprawdzenie, 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.* Uzasadnienie: • Proponowane zapisy w pełni respektują zasadę neutralności technologicznej w jednakowy sposób traktując rozwiązania chmurowe i on-premise. Podkreślona jest szczególnie rola KRI jako aktu wykonawczego dla ustawy o informatyzacji • Nałożonym wymaganiem jest udokumentowanie procesu planowania • Przeniesiony został punkt 1.57 z Rozdziału 7 – to jest właściwe miejsce! • Dokumentacja powinna zawierać podstawowe elementy. Wielkość dokumentacji, zakres porównania ryzyk czy wskazanie korzyści pozostawione jest decyzji Zamawiających, gdyż będzie zależało od wielkości, rodzaju systemu i typu danych. • Ministerstwo Cyfryzacji w przyszłości może stworzyć narzędzia pomagające Zamawiającym w przygotowaniu takiej dokumentacji. PIIT deklaruje pomoc w ich tworzeniu

6. Wymagania dotyczące umowy z Dostawcą		
	Umowa z Dostawcą powinna zapewniać możliwość sprawowania kontroli nad działaniami Dostawcy w zakresie świadczonych przez niego usług, w szczególności powinna zawierać zapisy określające:	**Propozycja PIIT**: *Warunkiem wykorzystania publicznej chmury obliczeniowej jest zawarcie umowy pomiędzy Zamawiającym a Dostawcą zawierającej:* **Uzasadnienie**: Podtrzymujemy naszą poprzednią propozycję. Umowy – porównajmy je z zapisami umów licencyjnych dla oprogramowania on-premise! – nie dają kontroli nad działaniami Dostawcy, ale określają warunki, w ramach których działa Dostawca. Nasza propozycja lepiej oddaje świadczenie usług w chmurze. Uproszczenie tekstu Rekomendacji oraz wskazanie na wystarczający charakter Rekomendacji dla ogólnego stosowania chmury publicznej w jednostkach sektora finansów publicznych Chcieliśmy zwrócić uwagę, że w dalszej części zapisów dotyczących wymagań dotyczących umowy z Dostawcą zamiast zapewnienie, zobowiązanie, uzgodnienia itp. o których mówi projekt stosujemy konsekwentnie „zapisy" (w sensie „zapisy umowy"), ponieważ zasadą wykorzystania usługi chmurowej jest bezobsługowe zamówienie usługi on-line
1.23	*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;*	**Propozycja PIIT:** *zapisy pozwalające Zamawiającemu ocenić, że dopuszczalne jest przetwarzanie w publicznej chmurze obliczeniowej* **Uzasadnienie**: nawiązujemy do propozycji zapisów dopuszczalności znajdujących się w Rekomendacjach oraz do wymagań związanych z planowaniem. Uproszczenie zapisu. Wyszczególnienie RODO nie wskazuje, że inne akty prawne są równie istotne!

1.24	*zasady opracowania i wdrożenia stosownych polityk i procedur zapewniających prawidłową realizację zleconych czynności oraz bezpieczeństwo danych przekazanych przez Zamawiającego;*	**Propozycja PIIT:** *zapisy wskazujące na zapewnienie przez Dostawcę odpowiednich zabezpieczeń technicznych i organizacyjnych w celu ochrony danych Zamawiającego i realizacji procesów przetwarzania* **Uzasadnienie**: taki zapis wskazuje na konieczność obecności zapisów dotyczących zabezpieczenia danych i procesu przetwarzania; ocena czy jest to zabezpieczenie „stosowne" należy do Zamawiającego, rodzaju wykorzystania chmury i wynika z procesu planowania.
1.26	*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;*	**Propozycja PIIT**: wykreślić **Uzasadnienie**: wynika wprost z RODO i nie ma potrzeby powtarzania tego w Rekomendacjach

1.27	*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;*	**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. Przetwarzanie poza terytorium EOG musi nakładać na Dostawcę takie same obowiązki jakby dla przetwarzania w EOG.* **Uzasadnienie**: Podtrzymujemy poprzednią propozycję (uzupełnioną). • Uproszczenie zapisu Rekomendacji – aktualny zapis jest praktycznie nieczytelny • Brak jest wskazania czy wymaganie dotyczy tylko danych osobowych czy też wszelkich danych. Można się domyślać, że chodzi o dane osobowe, ale nie jest to wprost wskazane. • W propozycji PIIT dotyczy to wszekich danych – co idzie także w zgodzie z Rozporządzeniem Free Flow of Data • Wskazanie EOG zamiast EU – dla zachowania konsystencji z RODO • **Podkreślamy ponownie:** 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 - nie ma możliwości zabronienia Zamawiającemu innego wyboru, • Dostawca na różne sposoby może realizować odpowiednią ochronę danych poza EOG i może to się odnosić do różnych typów danych, nie tylko danych osobowych.

1.29	*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**: Podtrzymujemy naszą poprzednią propozycję - nie można z góry określić w jakich sprawach Zamawiający może kontaktować się z Dostawcą oraz w jaki sposób będzie realizowany (od bezpośredniego kontaktu do informacji przesyłanym przez Pojedynczy Punkt Kontaktowy zgodnie z UKSC), dlatego niezbędny jest tylko ogólny zapis.
1.31	*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:** *zapis dotyczący zachowania integralności i dostępności danych Zamawiającego w trakcie umowy oraz w określonym umową okresie po jej wygaśnięciu*
1.32	*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 w czasie realizacji i po zakończeniu umowy, a także po zakończeniu zatrudnienia* **Uzasadnienie**: uproszczenie zapisu

1.34	*procedury zarządzania dostępem w sposób wykluczający uzyskanie dostępu przez osoby nieuprawnione;*	**Propozycja PIIT:** *zapisy dotyczące adekwatnej kontroli dostępu personelu Dostawcy do środowiska przetwarzania* **Uzasadnienie**: • Jednym z wymagań dopuszczających przetwarzanie w chmurze jest stosowanie norm serii ISO 27000, które m.in. wykluczają dostęp osób niepowołanych. Zapis o stosowaniu takiej normy np. 27001, może nie znajdować się w umowie, ale być oddzielnym zobowiązaniem Dostawcy. Dodatkowo normy te mogą się zmieniać, nowelizować. • Proponujemy uproszczony, ale zapis w swoim sensie pozostaje bez zmian.
1.35	*kary umowne z tytułu naruszenia zasad bezpieczeństwa oraz ochrony informacji i danych przekazanych przez Zamawiającego, w tym danych osobowych;*	**Propozycja PIIT**: wykreślić **Uzasadnienie**: • wynika z oddzielnych przepisów prawa, w szczególności z odpowiedzialności przed regulatorem • brak wskazania o jakie zasady bezpieczeństwa chodzi, więc w najbardziej generalnym przypadku wystarczy by w umowie były jakiekolwiek kary za cokolwiek? • Porównując z licencjami na oprogramowanie z półki w instalacji on-premise – czy znane są zapisy o podobnych karach umownych?
1.36	*obowiązek Dostawcy zapewnienia skutecznego niszczenia danych z uszkodzonych komponentów infrastruktury w przypadku ich wymiany;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: • weryfikacją tego jest ISO 27001 (patrz dopuszczalność przetwarzania w chmurze)

1.40	*opracowanie i okresowe testowanie planu związanego z rozwiązaniem lub zakończeniem obowiązywania umowy z Dostawcą (exit-plan);*	Propozycja PIIT: wykreślić **Uzasadnienie**: to nie jest obowiązek Dostawcy! Patrz także Rozdział 8, gdzie jest zapis o konieczności exit-planu przygotowanego przez Zamawiającego.
1.41	*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;*	**Propozycja PIIT:** *zapis dotyczący możliwości wymagania od Dostawcy udostępnienia raportów z niezależnych audytów potwierdzających spełnianie przez Dostawcę wymaganych norm bezpieczeństwa lub prawo do przeprowadzenia audytu lub kontroli przez Zamawiającego i upoważnione przez niego podmioty i osoby trzecie* **Uzasadnienie**: • Prawo to regulują oddzielne przepisy (RODO, UKSC), np. to zagadnienie jest rozwiązane poprzez wskazanie, że Dostawca jest podmiotem przetwarzającym w rozumieniu RODO, • Odwrócenie kolejności – pierwszym wymaganiem jest przedstawienie przez Dostawcę raportów od niezależnych audytorów, a gdyby nie był w stanie wypełnić takiego żądania to możliwość przeprowadzenia audytu.
1.42	*możliwość wykonywania obowiązków kontrolnych przez organ nadzorczy;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: Podtrzymujemy poprzednią uwagę. • taka możliwość wynika z ogólnych przepisów prawa, a nie z umowy pomiędzy Dostawcą i Zamawiającym, a dla Dostawcy Usług Cyfrowych wynika to z nadzoru i kontroli regulatora • nie wiadomo o jakim organie nadzorczym jest mowa, zwłaszcza jeśli jest użyta liczba pojedyncza. Czy jeśli UODO wykonuje czynności wobec Dostawcy Usług Cyfrowych to organ właściwy ds. cyberbezpieczeństwa już takich obowiązków wykonać nie może?...

1.43	*zgodne z przepisami prawa zakres odpowiedzialności Dostawcy za szkody wyrządzone osobom trzecim;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: Podtrzymujemy poprzednią uwagę. Ten zapis wynika z powszechnie obowiązujących przepisów prawa (np. RODO) i nie ma potrzeby przywoływania go dodatkowo.
1.44	*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**: Podtrzymujemy poprzednią propozycję • zasady obsługi incydentów mogą być różne w zależności od zadania wykonywanego w publicznej chmurze obliczeniowej • rola podmiotu przetwarzającego dla Dostawcy w rozumieniu RODO nakłada stosowne obowiązki powiadamiania o naruszeniach • Dostawcy Usług Cyfrowych będą musieli spełniać bardzo wysokie kryteria informowania o incydentach oraz komunikacji z odpowiednimi służbami w kraju.

1.46	*Parametry usług świadczonych przez Dostawcę, w tym: (..)* *d. mierniki w zakresie bezpieczeństwa IT;* *e. sposób komunikacji;* *f. (..)* *h. zasady przeglądów i aktualizacji parametrów SLA;*	**Propozycja PIIT:** Wskazane w tym punkcie elementy nie są parametrami usług świadczonym przez Dostawcę. Część wymagań wynika z przepisów prawa np. z faktu, że jest podmiotem przetwarzającym w rozumieniu RODO lub Dostawcą Usług Cyfrowych. Część zapisanych w propozycji parametrów z nich nie znajduje się w umowach o świadczenie usługi, a w oddzielnych umowach. Chcielibyśmy podtrzymać naszą poprzednią propozycję, zwłaszcza że część z nich znajduje się w procesie planowania. **Propozycja:** *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 dotyczące jakości świadczonych usług*

1.47	*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 incydencie powinna zostać przekazana Zamawiającemu nie później niż w terminie 36 godzin);*	**Propozycja PIIT***: zapisy dotyczące informowania o zmianach dotyczących świadczenia przetwarzania w publicznej chmurze obliczeniowej* **Uzasadnienie**: • Zasadnicze uproszczenie zapisu • Punkt dotyczy wielu odmiennych zagadnień • Propozycja adresuje p. a i b. • Punkt c. jest opisany w propozycji w punkcie 1.30, do którego nie zgłaszamy uwag – powtarzanie w różny sposób zapisanego tego samego wymagania prowadzi do braku integralności dokumentu! • Punkty d. i e. wynikają z faktu, że Dostawca jest podmiotem przetwarzającym w rozumieniu RODO (p.1.25) i nie ma potrzeby ich przywoływać.

1.49	*zasady zarządzania zmianami w świadczonych usługach;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: patrz p. 1.47;
1.50	*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**: Podtrzymujemy poprzednią wersję. • Uproszczenie zapisu i zapewnienie Zamawiającemu odpowiedniej kontroli nad swoimi danymi • Dla dużej części Zamawiających uzyskiwanie raportów będzie nadmiarowe, co dobitnie pokazuje raport NIK z województwa podlaskiego • Żądanie by Zamawiający specyfikował jaki jest zakres i źródła logów jest mało prawdopodobne dla mniejszych odbiorców ponieważ wymaga dużej wiedzy • Zamawiający mając dostęp do rejestru zdarzeń może swobodnie kształtować swój zakres pozyskiwanych informacji • Również: wynika z innych zapisów prawa, np. wymagań wobec Dostawcy Usług Cyfrowych.
1.51	*politykę wykonywania kopii zapasowych oraz zapewnienia ciągłości działania;*	**Propozycja PIIT**: wykreślić (podtrzymujemy poprzednią opinię) **Uzasadnienie**: temat zapisany w 1.46;
1.52	*parametry odtworzenia po katastrofie, w tym parametry dotyczące ciągłości działania usług świadczonych przez Dostawcę na rzecz Zamawiającego;*	**Propozycja PIIT:** wykreślić **Uzasadnienie**: temat zapisany propozycji p. 1.46

1.53	*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**: jeśli dotyczy zasad związanych z przetwarzaniem danych osobowych to wynika to wprost z przepisów prawa oraz z faktu, że Dostawca jest podmiotem przetwarzającym w rozumieniu RODO (patrz p. 1.25).
1.54	*listę podwykonawców Dostawcy z lokalizacjami wraz z określeniem zakresu czynności świadczonych przez podwykonawców;*	**Propozycja PIIT**: wykreślić **Uzasadnienie**: wynika wprost z zapisu p.1.25 wskazującego, że Dostawca jest podmiotem przetwarzającym w rozumieniu RODO.
1.55	*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**: wynika wprost z zapisu p.1.25 wskazującego, że Dostawca jest podmiotem przetwarzającym w rozumieniu RODO.
1.56	*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 – zakres ten pozostaje w gestii Zamawiającego i nie musi być regulowany • Pozostałe elementy zapisane w propozycji p. 1.46 • Dla Dostawcy Usług Cyfrowych realizacja takich zgłoszeń wynikać będzie m.in. z wymagań regulatora

1.56 a		**Propozycja PIIT:** *Jeśli Dostawca jest Dostawcą Usługi Cyfrowej uznaje się, że spełnione są wymagania dotyczące umowy z Dostawcą opisane powyżej.* Uzasadnienie: • Zakładamy, że wiele podmiotów będzie starało się i uzyska status Dostawcy Usług Cyfrowych, stąd znaczące uproszczenie procesu dla tych, którzy zechcą skorzystać z ich usług • Dostawca Usługi Cyfrowej znajduje się pod kontrolą i nadzorem organów właściwych dla cyberbezpieczeństwa, a usługi chmurowe świadczone przez DUC mogą być wykorzystane dla realizacji usług kluczowych (art. 17 ust. 2 UKSC). • Oznacza to bardzo wysokie wymagania, zdecydowanie większe niż w przypadku zastosowań typowych a jednocześnie nadzór nad takimi dostawcami. • Jeśli Zamawiający chce dokonać dodatkowego sprawdzenia lub wymaga to wyższych wymagań niż nakładają rekomendacje – to daje mu to zapis punktu 1.3 • Jeśli Zamawiający uzna, że rekomendacje zostaną wyłączone (propozycja punktu 1.3a) to może dokonać zupełnie oddzielnej analizy wymagań.

7. Realizacja umowy (dotyczącej wykorzystania publicznej chmury obliczeniowej)		
		Proponujemy wykreślenie tego Rozdziału! **Uzasadnienie:** • Punkt 1.57 jest przeniesiony do Rozdziału poświęconego planowaniu, gdyż sprawdzenie wskazanego w nim parametru powinno nastąpić zanim podjęta zostanie decyzja o rozważeniu modelu chmurowego • (opcja) Ministerstwo powinno opracować oddzielne rekomendacje dotyczące korzystania z usług operatorów telekomunikacyjnych lub wskazać odpowiednie zapisy prawa • Wszystkie pozostałe zapisy tego rozdziału powinny zostać uwzględnione nie w Rekomendacjach, ale w takich aktach prawnych jak Rozporządzenie KRI lub oddzielne Rekomendacje dotyczące Zasad Eksploatacji Systemów Informatycznych! • Ani jedno z wymagań zapisanych w p. 1.58 nie jest specyficzne dla rozwiązania chmurowego! W równym stopniu dotyczy rozwiązań on-premise! Dlaczego zatem należałoby stosować je tylko do chmury?
1.57	*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**: przeniesione do propozycji p. 1.15