Dziesięć zasad stosowania usług chmurowych przez administrację publiczną

1. Podmiot publiczny decydujący się na przekazanie choćby części swoich zasobów do chmury musi zobowiązać dostarczyciela usługi chmurowej do przekazania pełnej informacji o wszystkich fizycznych lokalizacjach serwerów na których przetwarzane są lub mogą być przetwarzane dane. Informacja o zmianie lokalizacji powinna być przekazywana podmiotowi publicznemu z rozsądnym wyprzedzeniem, tak by podmiot ten mógł rozważyć nie tylko wymagania wynikające z zasad ochrony danych osobowych ale również z zasad ochrony tajemnic prawnie chronionych oraz ewentualnych wymagań co do infrastruktury krytycznej Państwa. Wymaganie to dotyczy tym samym nie tylko przekazywania zasobów do tak zwanych państw trzecich w rozumieniu przepisów o ochronie danych osobowych, ale również do przekazywania zasobów do państw należących do EOG, a nawet do konkretnych centrów przetwarzania danych.
2. Dostarczyciel usługi chmurowej powinien umożliwić podmiotowi publicznemu pełny dostęp do dokumentacji dotyczącej zasad bezpieczeństwa oraz środków technicznych przyjmowanych w poszczególnych centrach przetwarzania danych. Informacja taka stanowi oczywiście tajemnice przedsiębiorcy dostarczającego usługi chmurowe, jest jednak niezbędna dla zapewnienia bezpieczeństwa usług publicznych.
3. Dostarczyciel usługi chmurowej jest zobowiązany przekazać pełną informację dotyczącą podwykonawców i współpracujących instytucji mających udział w realizacji usługi chmurowej. Przekazana informacja powinna umożliwić podmiotowi publicznemu ocenę wszystkich podwykonawców w „stosie chmur" oraz umożliwić mu ocenę roli każdego z tych podmiotów jako przetwarzającego dane osobowe.
4. Każdy z podwykonawców traktowany jako podprzetwarzający dane osobowe powinien być związany takimi samymi klauzulami umownymi jak dostarczyciel usług chmurowych. Dostarczyciel usług chmurowych powinien zaś zarządzać całym łańcuchem podwykonawców i ich uprawnieniami zgodnie z instrukcjami przekazanymi przez podmiot publiczny.
5. Podmiot publiczny powinien pozostawać wyłącznym administratorem danych osobowych przekazanych do chmury. Niedopuszczalna jest sytuacja, w której jakikolwiek dostarczyciel chmury – nawet jeśli sam jest podmiotem publicznym – decydowałby o celach i sposobach przetwarzania danych niezależnie od instrukcji ze strony administratora danych osobowych.
6. Dostarczyciel usługi chmurowej jest zobowiązany informować podmiot publiczny o wszelkich zobowiązaniach publicznych w stosunku do policji i organów ścigania oraz służ specjalnych w zakresie przekazywania im dostępu do danych zamieszczonych w chmurze przez podmiot publiczny będący jej użytkownikiem. Odmowa przekazania takich informacji powinna stanowić przeszkodę dla realizacji usługi chmurowej u danego dostarczyciela. Wymaganie to dotyczy oczywiście również wszystkich podwykonawców w „stosie chmur". Jeśli podmiot publiczny podejmie decyzję, że może godzić się na taki dostęp do danych instytucji publicznych (krajowych lub zagranicznych), dostarczyciel usługi chmurowej powinien niezwłocznie informować użytkownika o wszystkich wnioskach o udostępnienie danych z jego zasobu.

7. Dostarczyciel usługi chmurowej powinien określić wspólnie z podmiotem publicznym zasady przeszukiwania, retencji i usuwania danych dostarczonych przez podmiot publiczny.

8. Dostarczyciel usługi chmurowej powinien być zobowiązany do raportowania wszystkich incydentów bezpieczeństwa danych, ze szczególnym uwzględnieniem tych, które dotyczyć mogą danych osobowych przetwarzanych przez podmiot publiczny w chmurze. Powinien również udzielić podmiotowi publicznemu wszelkiej możliwej pomocy przy zwalczaniu skutków takich incydentów bezpieczeństwa.

9. Podmiot publiczny powinien w procesie negocjacji umowy z dostarczycielem usługi chmurowej ustalić, jakie zasady wyłączenia lub ograniczenia odpowiedzialności dostarczyciela usługi mogą być zastosowane przy realizacji usługi. Powinno to w szczególności dotyczyć wyłączeń, o których mowa w dyrektywie o handlu elektronicznym, czyli mere conduit, cachingu i przede wszystkim hostingu.

10. Podmiot publiczny musi wszelkimi środkami unikać przywiązania do pojedynczego dostarczyciela usług chmurowych i jego rozwiązań technicznych. Interoperacyjność i przenaszalność danych jest podstawą dla uniknięcia „syndromu jednego dostawcy", który musi niekorzystnie wpływać na całość realizacji zadania publicznego w chmurze[1].

Wszystkie rozważania dotyczące chmur dedykowanych i prowadzenia negocjacji, mających na celu zawarcie umowy o usługę chmurową, zakładają, że przy umowach dotyczących usług innych niż przetwarzanie informacji publicznej nie można wykorzystywać umów adhezyjnych. Musi istnieć przynajmniej możliwość dedykowania usługi do potrzeb i wymagań prawnych administracji. Angażowanie się administracji publicznej w jakiekolwiek umowy adhezyjne, nie uwzględniające instrukcji ze strony organu administracji publicznej, który podejmuje się przetwarzania „swych" danych w chmurze, należy traktować jednoznacznie jako naruszenie podstawowych wymagań działania władzy publicznej na podstawie prawa i w jego granicach.

Na podst.: *B. Segalis*, Cloud Computing Legal Risk and Liability, InfoLawGroup 2011, prezentacja s. 21-30.