Cloud computing a przetwarzanie danych osobowych

MARLENA SAKOWSKA-BARYŁA, PIOTR SIEMIENIAK

Streszczenie

Przetwarzanie danych osobowych za pośrednictwem chmur obliczeniowych daje administratorom wiele korzyści odnoszących się do aspektów biznesowych oraz aspektów związanych z bezpieczeństwem i pewnością przetwarzania informacji, w tym danych osobowych. Niemniej jednak przetwarzanie danych osobowych z użyciem chmur obliczeniowych niesie za sobą liczne zagrożenia, które powinny być przez administratorów uwzględnione na etapie projektowania lub analizy zagrożeń dla praw i wolności osób, których dane dotyczą (analiza ryzyka).

Słowa-klucze: Cloud Computing, komputer, definiowanie chmury, modele usług chmurowych.

Zusammenfasung

Cloud Computing und Verabeitung personenbezogener Daten.

Die Verarbeitung personenbezogener Daten ueber Cloud Computing bietet Administratoren viele Vorteile in Bezug auf geschaeftliche Aspekte und Aspekte in Bezug auf die Sicherheit und Gewissheit der Informationsverarbeitung, einschliesslich personenbezogener Daten. Die Verarbeitung personenbezogener Daten unter Verwendung von Cloud Computing ist jedoch mit zahlreichen Bedrohungen verbunden, die von den fuer dieVerarbeitung Verantwortlichen in der Entwurfsphase oder in der Analyse der Bedrohung der Rechte und Freiheiten der betroffenen Personen beruecksichtigt werden sollten (Risikoanalyse).

Schluesselwoerter: Cloud Cmouting, Computer, Definition der Cloud, Modelle von Cloud-Diensten

Model biznesowy świadczenia usług IT określany jako *cloud computing* (CC), któremu to w języku polskim odpowiadają synonimiczne określenia: "przetwarzanie w chmurze", "przetwarzanie chmurowe" czy "chmura obliczeniowa" jest obecnie powszechnie wykorzystywany[1]. Nie sposób wskazać wyczerpującej definicji tego zjawiska, choć bez wątpienia zasadne jest uznawać, że *cloud computing* jest rodzajem swoistego outsourcingu w zakresie przetwarzania danych, w tym także danych osobowych. W uproszczeniu można powiedzieć, że *cloud computing* to grupy zasobów komputerowych, których nie widzimy i z którymi nie mamy bezpośredniej styczności, ponieważ są „w chmurach", a jednocześnie blisko nas, to model umożliwiający powszechny dostęp z każdego miejsca i na żądanie, dostęp sieciowy do określonych konfigurowanych zasobów obliczeniowych, np. sieci, nośników danych, aplikacji, czy usług, które mogą być wykorzystywane z minimalnym wysiłkiem użytkownika i interakcją dostawcy. Dlatego właśnie stają się tak wygodne, stosunkowo tanie i łatwo osiągalne[2].

DEFINIOWANIE CHMURY

Komisja Europejska w Komunikacie w sprawie wykorzystywania potencjału chmury obliczeniowej w Europie, zaproponowała, by pojęcie chmury definiowane było w uproszczeniu jako: przechowywanie, przetwarzanie i wykorzystywanie danych, do których dostęp uzyskuje się przez Internet na komputerach znajdujących się w innych lokalizacjach[3]. Chodzi tu o tzw. wirtualizację usług IT, gdzie - obrazowo rzecz ujmując - użytkownik otrzymuje usługi z zewnątrz, bo zasoby, czyli aplikacje, oprogramowanie, a także dane osobowe są przenoszone z dysku komputera użytkownika do tzw. chmury. Usługodawca może dostarczać użytkownikowi albo samo "miejsce w serwerowni", albo konkretne potrzebne mu aplikacje i oprogramowanie bez konieczności posiadania sprzętu, środowiska pracy, licencji, wyspecjalizowanego personelu[4]. *Cloud computing* pozwala na dostęp do aplikacji z dowolnego miejsca, innego niż znajduje się *hardware* użytkownika, to usługi oferowane przez zewnętrzne w stosunku do niego podmioty i dostępne na jego życzenie w dowolnym momencie, skalujące się dynamicznie w odpowiedzi na zapytanie.

[1] Zob. B. Fischer, *Podział odpowiedzialności a chmurowe przetwarzanie danych osobowych z uwzględnieniem kształtowania regulacji umownych*, [w:] *Aktualne problemy porwanej ochrony danych osobowych*, red. G. Sibiga, dodatek do "Monitora Prawniczego" 2014, nr 9, s. 12.

[2] Zob. A. Monarcha-Matlak, *Karta praw klientów chmury*, [w:] *Internet. Cloud computing. Przetwarzanie w* chmurach, red. G. Szpor, Warszawa 2013, s. 173 i 175.

[3]Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów "Wykorzystanie potencjału chmury obliczeniowej w Europie" z 27.09.2012 r., KOM(2012) 529, https://mac.gov.pl/files/wp-content/uploads/2012/10/Komunikat-Komisji-wersja-polska.pdf..

[4] Zob. M. Brzozowska, *Ochrona danych osobowych w sieci*, Wrocław 2012, s. 211.

Cloud computing to dostarczanie zdolności komputerowych zdalnie przez dostawcę bez konieczności instalacji oprogramowania lub infrastruktury[5].
W literaturze wyróżnia się podstawowe cechy chmurowego modelu przetwarzania, kształtowane przez następujące elementy:

1) klienci chmury powinni mieć możliwość skorzystania z usług w chmurze, używając mechanizmu samoobsługi w taki sposób, by nabywanie usług nie wymagało interwencji przez usługodawcę chmury (*on-demand self-service*);
2) chmura powinna być dostępna z każdego miejsca na różnych urządzeniach - komputerach stacjonarnych, laptopach, tabletach, smartfonach itd. (*broad network access*);
3) chmury udzielają klientom chmury pule współdzielonych zasobów, takich jak: moc obliczeniowa, pamięć, sieć, dysk, które to zasoby są pobierane z aktualnej lokalizacji, której klienci nie są świadomi (*resource pooling*);
4) bez konieczności ingerencji człowieka, automatycznie chmury powinny zapewnić szybkie uwolnienie zasobów ze względu na zapotrzebowanie i ich zastrzeżenie, a odbiorcy chmury powinni odnosić wrażenie, że istnieje nieograniczona pula zasobów - usługa jest w stanie spełnić wymagania dla dowolnego scenariusza w przypadku użycia (*rapid elasticity*);
5) model chmury powinien umożliwiać ładowanie usług na podstawie rzeczywistego wykorzystania jej zasobów, przy czym wykorzystywanie zasobów jest monitorowane, zgłaszane i kontrolowane przez dostarczyciela usług CC i politykę serwisu, które zapewniają przejrzystość rozliczeń zarówno z dostarczycielem usług, jak i ich konsumentem (*metered services*)[6].

Definicja legalna odnoszącą się do usługi chmury obliczeniowej sformułowana została w art. 4 pkt 19 dyrektywy NIS[7], która wskazuje, że "usługa przetwarzania w chmurze" oznacza usługę cyfrową umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania. Jak wskazuje się w literaturze, koncepcja korzystania z zasobów teleinformatycznych na podstawie usługi ewoluowała i z czasem, co znajdowało przełożenie na terminologię, która posługiwano się w odniesieniu do tego konceptu – począwszy od *utility computing, grid computing, cluster computing*, aż do *cloud cmputing*[8].

[5] Zob. E. Molenda-Kropielnicka, *Cloud computing - zagadnienia prawne*, ZNUJ 2013, z. 119, s. 111.
[6] Zob. W.R. Wiewiórowski, *Prawne aspekty udostępniania usług administracji publicznej w modelu chmury*, [w:] *Internet. Cloud computing. Przetwarzanie w* chmurach, red. G. Szpor, Warszawa 2013, s. 86.
[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U.UE.L.2016.194.1).
[8] Szerzej zob. B.Fischer, *Cloud computing – globalny technologiczny paradygmat – zagrożeniem dla ochrony danych osobowych i prywatności,* Kraków 2013, s. 54, A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018, s. 36 i n.

MODELE USŁUG CHMUROWYCH

Chmura obliczeniowa nie jest kategorią jednorodną, ale stanowi szeroko zakreślony biznesowy typ przetwarzania oparty na użytkowaniu różnych usług dostarczanych przez podmioty zewnętrzne[9]. Usługi świadczone w chmurze występują w pewnych podstawowych modelach:

1) model usługi, w ramach której udostępniana jest infrastruktura informatyczna - *Infrastructure as a Service* (IaaS); klientowi dostarcza się np. sprzęt, oprogramowanie, serwisowanie, często polega na wynajmie sprzętu, na którym instaluje się oprogramowanie będące własnością usługobiorcy;
2) model usług, polegający na udostępnianiu klientom platformy umożliwiającej korzystanie klientom z pakietu aplikacji - *Platform as a Serwice* (PaaS) - mamy tu do czynienia ze sprzedażą gotowego, często dostosowanego do potrzeb użytkowników kompletu aplikacji udostępnianych klientowi przez serwer dostawcy;
3) model polegający na dostarczaniu klientowi oprogramowania - *Software as a Serwice* (SaaS) - udostępnia się konkretne oprogramowanie i funkcjonalności znajdujące się poza sprzętem należącym do klienta poprzez serwer dostawcy usługi;
4) udostępnianie komunikacji - *Communication as a Service* (CaaS) - to model polegający na udostępnieniu platformy pod komunikacyjne środowisko pracy[10].

Z punktu widzenia organizacji chmury dzieli się je zazwyczaj na:

1) chmurę prywatną, której infrastruktura przeznaczona jest dla pojedynczego klienta, pojedynczej organizacji, a jej zasoby sprzętowe są fizycznie izolowane od innych i przeznaczone dla jednego klienta;
2) chmurę publiczną, której infrastruktura przeznaczona jest do użytkowania bez ograniczeń dostępu; to zwirtualizowane, dostępne przez Internet zasoby pamięciowe i obliczeniowe udostępniane przez usługodawcę wielu klientom na życzenie, o takich cechach charakterystycznych, jak: skalowalność, płatność, współdzielenie fizycznych zasobów obliczeniowych z innymi użytkownikami, wykorzystanie Internetu, oparcie świadczeń na parametrach usługi (dostępność określonej pamięci i mocy obliczeniowej w czasie);
3) chmurę hybrydową, której infrastruktura składa się z dwóch bądź więcej infrastruktur chmury prywatnej lub publicznej, pozostających bytami samoistnymi powiązanymi dzięki technologii standaryzowanej lub firmowej;

[9] B. Fischer, *Ochrona prywatności i wykorzystanie instrumentów samoregulacji w modelu cloud computingu*, [w:] *Internet. Cloud computing. Przetwarzanie w* chmurach, red. G. Szpor, Warszawa 2013, s. 215.
[10] Zob. J. Kurek, *Prawne uwarunkowania świadczenia usług w chmurze w obrocie konsumenckim*, [w:] *Internet. Cloud computing. Przetwarzanie w* chmurach, red. G. Szpor, Warszawa 2013, s. 158; B.Fischer, *Cloud computing…*, s.51,52; A. Krasuski, *Chmura …*, s. 61-74

4) chmurę wspólnotową, którą udostępnia się kilku klientom spełniającym te same standardy, którą użytkuje w sposób wyłączny szczególna społeczność użytkowników mających wspólne cechy - misję, wymagania w zakresie bezpieczeństwa, względy polityczne[11].

SPECYFIKA USŁUG CHMUROWYCH

Przetwarzanie chmurowe to rezultat ewolucji technologicznej w dziedzinie IT i kombinacja wielu technologii. Stało się ono możliwe dzięki rozwojowi sprzętu, bo komputery typu *mainframe* zostały zastąpione przez komputery osobiste, które obecnie ustępują miejsca urządzeniom mobilnym, rozwojowi połączeń internetowych poprzez zwiększenie przepustowości łączy i szerokopasmowemu Internetowi oraz rozwojowi usług świadczonych przez dostawców oferujących gotowe aplikacje, a nie tylko infrastrukturę, jak miało to miejsce wcześniej. Zmianie uległ także sposób przetwarzania danych od modelu klient - serwer, gdzie system klienta wysyłał żądanie na serwer, a odpowiedź otrzymywał za pośrednictwem sieci, poprzez technikę polegającą na łączeniu mocy obliczeniowej różnych systemów w wirtualny superkomputer przy wykorzystaniu nieużywanych zasobów sieciowych (*Grid Computing*), następnie model, w którym dzięki zastosowaniu wirtualizacji pracę wykonywała już tylko jedna maszyna, na której umieszczono kilka serwerów (*Utility Computing*) aż do technologii CC[12]. Jej cechą charakterystyczną jest to, że sprzęt, w tym komputery i urządzenia służące do przechowywania danych pozostają własnością dostawców usług chmurowych, nie zaś użytkowników, którzy uzyskują jedynie dostęp do chmury za pośrednictwem Internetu.

PRZETWARZANIE DANYCH OSOBOWYCH W CHMURZE

Klienci chmury niekoniecznie znają lokalizację danych lub procesów. Zasadniczo ta wiedza nie jest im potrzebna do realizacji usługi. Nie mają oni również wpływu na wykorzystywany sprzęt i zabezpieczenia, ponieważ o tę sferę zadbać musi dostawca chmury. To wszystko rodzi wątpliwości w sytuacji, gdy chmurowe przetwarzanie obejmuje dane osobowe[13]. Najpewniej wątpliwości te są słuszne, biorąc pod uwagę to, że usługi chmurowe są rynkiem dostawców, na którym klient ma niewielki wpływ na kształt umowy, bo możliwość negocjowania warunków świadczenia usług sprowadza się często do

[11] A. Monarcha-Matlak, *Karta praw ...*, s. 178-179.
[12] Zob. E. Molenda-Kropielnicka, *Cloud computing ...*, s. 110-111.
[13] Zob. J. Kurek, *Prawne uwarunkowania ...*, s. 157.

możliwości dokonywania wyboru pomiędzy poszczególnymi dostawcami i ich standardowymi propozycjami[14].

To powoduje konieczność zastanowienia się nad efektywnością dotychczasowych konstrukcji ochrony danych osobowych, skoro przypisywany dotąd administratorowi przymiot decydowania o celach i sposobach przetwarzania danych osobowych traci tu znaczenie, bo ów dysponent danych, korzystając z rozwiązań CC, już nie decyduje o sposobach i środkach przetwarzania, a wręcz faktycznie w tym zakresie traci nad nimi kontrolę[15]. Rzeczywiście z prawnego punktu widzenia najważniejsze, ale i najbardziej problematyczne, jest zapewnienie prywatności przy uwzględnieniu specyfiki przetwarzania i wymogów co do zlokalizowania danych. Trzeba bowiem znaleźć odpowiedzi na takie pytania, jak: kto może mieć dostęp do danych, w jaki sposób jest ukształtowana ochrona przed nieautoryzowanym dostępem, czy administrator uzyska informacje na temat ewentualnych incydentów bezpieczeństwa[16].

Niemniej ważne okazują się także pytania o to, jak w modelu CC określić lokalizację danych, zasady kontroli nad sposobem realizacji umowy, jak zapewnić administratorowi ingerencję w jej treść, czy da się jednoznacznie ustalić, kto w przypadku przetwarzania chmurowego jest administratorem, kto wyłącznie podmiotem przetwarzającym, jak kształtuje się odpowiedzialność użytkownika i dostawcy chmury względem osób, których dane dotyczą. Są to pytania mające duże znaczenie, zwłaszcza obecnie i dla podmiotów przetwarzających dane, które powinny być świadome zakresu swej odpowiedzialności i ciążących na nich obowiązków, jak i dla osób, których dane dotyczą, których autonomia informacyjna w dobie przewrotu informacyjnego, gdy „wszystko staje się dostępne dla wszystkich, wszędzie i natychmiast”[17] ulega uszczupleniu, bo coraz trudniej decydować jej kto, jakie informacje o niej i w jakim zakresie może przetwarzać[18].

WPŁYW CLOUD COMPUTING NA WYZNACZANIE SFERY INFORMACYJNEGO STATUSU JEDNOSTKI

Wraz z upowszechnianiem się nowych technologii, w tym tych, które dotyczą przetwarzania danych osobowych, środowisko informacyjne jednostki w coraz większym stopniu projektowane jest przez podmioty zewnętrzne względem jednostki.

[14] Zob. B. Fischer, *Podział odpowiedzialności ...*, s. 12.

[15] O sposobie rozumienia pojęcia „administrator” szerzej zob. M. Sakowska-Baryła, komentarz do art. 4 pkt 7, w: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 95 i n.

[16] Zob. Tenże, *Ochrona prywatności ...*, s. 215.

[17] K. Dobrzeniecki, *Konflikty wartości konstytucyjnych związane z funkcjonowaniem Internetu. Kazus przetwarzania danych w chmurze*, [w:] *Internet. Cloud computing. Przetwarzanie w* chmurach, red. G. Szpor, Warszawa 2013, s. 40.

[18] Szerzej zob. M. Sakowska-Baryła, *Cloud computing a autonomia informacyjna jednostki*, [w:] *Internet. Cloud computing. Przetwarzanie w chmurach*, red. G. Szpor, Warszawa 2013, s. 145.

Dodatkowo – co istotne – coraz większy wpływ na kształt informacyjnego statusu jednostki mają podmioty prywatne z tej racji, że w obrębie infrastruktury Internetu, w zakresie urządzeń i oprogramowania, to one mają przewagę własnościową. Tym samym to te podmioty właśnie mają wpływ na kształt zasobów informacyjnych dotyczących jednostki umiejscawianych dziś nie tylko w komputerze osobistym, ale i korzystających z mocy obliczeniowej urządzeń zewnętrznych. Tu zaciera się granica pomiędzy sferą prywatną a sferą publiczną, pomiędzy sektorem publicznym i prywatnym. Tymczasem wyznaczanie granic między sferą publiczną i prywatną było tradycyjna funkcją prawa stanowionego przez władzę publiczną. Dotyczy to między innymi ewentualnego limitowania autonomii informacyjnej jednostki, które w Polsce dokonywane być powinno tylko przez ustawodawcę, tylko w ustawie i tylko z uwzględnieniem przesłanek określonych w art. 31 ust. 3 oraz w art. 51 ust. 2 Konstytucji RP. Nie idzie tu jednak o uwarunkowania formalnoprawne, bo te wydają się być spełnione, ale o stan faktyczny i rzeczywiste potrzeby obrotu gospodarczego i prawnego. Obecnie uzasadnione jest pytanie o status jednostki czyli podmiotu prawa, który coraz bardziej uzależnia się od dostępności zasobów informacyjnych w formie elektronicznej, które to z kolei coraz częściej przetwarzane są z wykorzystaniem technologii CC, co może zdezintegrować spójność informacyjną tego podmiotu i służyć do tworzenia nowych metod jego kontroli i inwigilacji[19].

Pojawiające się aktualnie dylematy dotyczące prywatności informacyjnej w kontekście *cloud computing* przywodzą na myśl dyskurs, który towarzyszył kształtowaniu się prawa ochrony danych osobowych w latach 60-tych i 70-tych XX w., kiedy to automatyzacja procesów przetwarzania danych powodowała obawy o prywatność jednostki. Dziś podobne obawy powracają w związku z przetwarzaniem danych w chmurze obliczeniowej. Przy CC problematyczne jest samodzielne określenie przez jednostkę sfery dostępności dla innych wiedzy o sobie, a nadto wręcz niemożliwe jest kontrolowanie przez nią treści i obiegu informacji, które jej dotyczą, a to przecież są podstawowe założenia koncepcji autonomii informacyjnej. Nie wydaje się, by dzisiaj prawdziwe było stwierdzenie, że jednostka ma możliwość kontrolowania treści i obiegu informacji, które jej dotyczą oraz możliwość wyznaczania sfery dostępności informacji o sobie, nie tylko z uwagi na wykorzystywanie do przetwarzania jej danych osobowych technologii CC, ale miedzy innymi z uwagi na nią. Przetwarzanie w chmurze polega przecież na oferowaniu przez dostarczyciela chmury usług dostępnych *on-line* dla klienta - także administratora w rozumieniu przepisów o ochronie danych osobowych, który nie zna szczegółów korzystania z chmury obliczeniowej i przetwarzania danych za jej pomocą, bo nie musi ich znać, a często wręcz znać ich nie może.

[19] Zob. K. Dobrzeniecki, *Konflikty wartości* …, s. 43-46.

PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH W CHMURZE

Wśród wątpliwości prawnych związanych z przetwarzaniem chmurowym pojawiają się te, które dotyczą samych podstaw prawnych przetwarzania danych, odpowiedzialności za przetwarzanie danych, niejednoznacznością ról klienta chmury i jej dostarczyciela z punktu widzenia zasad ochrony danych osobowych, bo trudno określić, kto jest administratorem, a kto jedynie je przetwarza. Wątpliwości może budzić kwestia dopuszczalności i podstaw prawnych podwykonawstwa, a także dopuszczalności stosowania CC przez władze publiczne, choć korzystanie przez podmioty publiczne z usług chmurowych jest faktem.
Przetwarzanie danych w technologii chmurowej może odbywać się w różnych miejscach na świecie, w tym poza Europą. W modelu CC podstawowe wątpliwości może budzić właśnie aspekt geograficzny - lokalizacja serwerów poza Europejskim Obszarem Gospodarczym (EOG). W tym przypadku trzeba pamiętać o obostrzeniach w przekazywaniu danych osobowych do państw trzecich. Podstawową przesłanką umożliwiającą przekazanie danych na serwer umiejscowiony poza EOG jest zapewnienie, że państwo docelowe daje gwarancje ochrony przynajmniej analogiczne z istniejącymi w obrębie EOG[20]. Uprzednio aktami, na podstawie których oceniało się właściwy standard ochrony była dyrektywa 95/46/WE oraz w Polsce art. 47 i 48 poprzedniej ustawy o ochronie danych osobowych z 1997 r. uodo. Natomiast od dnia 25 maja 2018 r. standardy przetwarzania danych osobowych także w odniesieniu do przetwarzania chmurowego wyznaczają przepisy RODO.

W kontekście *cloud computingu* warto wziąć pod uwagę także opinię 8/2010 w sprawie prawa właściwego[21], która przedstawia zakres stosowania dyrektywy 95/46/WE, w szczególności jej art. 4 dotyczącego wyboru przepisów w przypadku transgraniczności usług. Próbę zmierzenia się z problematyką przetwarzania chmurowego i zgłaszanych co do niej zastrzeżeń są działania podejmowane w obrębie Komisji Europejskiej. Trzeba wspomnieć tu choćby o opublikowanym 27.09.2012 r. komunikacie Komisji Europejskiej "Wykorzystanie potencjału chmury obliczeniowej w Europie"[22].
Wciąż można zastanawiać się czy obecne unormowania prawa powszechnie obowiązującego były przystające do potrzeb i odpowiednio zabezpieczały prywatność informacyjną jednostki. Chmura nie zna granic i zasady terytorializmu, która cechowała dotychczasowe regulacje. Odnoszą się one do zapewnienia ochrony przetwarzania danych na poziomie państw – państw UE, państw trzecich zapewniających adekwatną ochronę.

[20] Zob. B. Fischer, *Ochrona prywatności ...*, s. 221. Szerzej też zob. B.Fischer, *Transgraniczność prawa administracyjnego na przykładzie regulacji przekazywania danych osobowych z Polski do państw trzecich*, Warszawa 2010, s. 183.
[21] Opinia 8/2010 w sprawie prawa właściwego Grupy Roboczej art. 29 przyjęta 16 grudnia 2010 r., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_pl.pdf.
[22] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów "Wykorzystanie potencjału chmury obliczeniowej w Europie" z 27.09.2012 r., KOM(2012) 529, https://mac.gov.pl/files/wp-content/uploads/2012/10/Komunikat-Komisji-wersja-polska.pdf.

Przy CC niewystarczające wydają się także zabezpieczenia oferowane poprzez sformułowanie standardowych klauzul umownych w drodze decyzji Komisji Europejskiej[23]. Istotniejsze natomiast jest potraktowanie dostarczyciela chmury jako zaufanego obszaru przetwarzania danych, dzięki wiążącym regułom korporacyjnym – *Binding Corporate Rules* (BCR)[24]. Uzasadnionym rozwiązaniem jest traktowanie korporacji, które wprowadziły takie BCR dotyczące przetwarzania danych osobowych jako czegoś w rodzaju odpowiednika państw. Instytucja BCR pojawiła się także w poprzedniej ustawie o ochronie danych osobowych z 1997 r. znowelizowanej w listopadzie 2014 r.[25]. W RODO natomiast instytucja wiążących reguł korporacyjnych uregulowana została w art. 47[26]. niemniej w dalszym ciągu brak jest wyodrębnionych ram prawnych dotyczących podejmowania i wykonywania działalności w chmurze obliczeniowej, a jako pojedynczą regulację, która wskazuje wprost na usługi chmurowe, jednak wyłącznie w kontekście bezpieczeństwa teleinformatycznego należy wskazać dyrektywę NIS. Stąd – jak wskazuje się w literaturze – w celu wyznaczenia źródeł prawa dotyczących chmury obliczeniowej należy oprzeć się na cechach wspólnych wynikających z rożnego definiowania tej konstrukcji. W zależności bowiem od charakteru zasobu, który stanowi element łącznej konstrukcji chmury obliczeniowej różnie kształtuje się podstawa prawna począwszy od aktów normatywnych regulujących dostęp do sieci Internet, prawa do oprogramowania i baz danych, infrastruktury sprzętowej, poprzez kwestię samego świadczenia usług i umowne ustalenia w tym zakresie[27].

Bez wątpienia jednak problematyczny pozostaje charakter norm, które powinny regulować zagadnienie przetwarzania chmurowego, o czym już wcześniej pośrednio wspomniano poprzez wskazanie na "prywatyzowanie się" sfery regulowanej zwykle przez publicznego prawodawcę. Rzecz jasna, w rachubę wchodzą tu przepisy prawa międzynarodowego, europejskiego, krajowego, czy wspomniane normy wiążących reguł korporacyjnych. Niemniej jednak zważywszy na niezbędność ochrony prywatności i danych osobowych jednostki, gwarantowanych jako jej prawa podstawowe, zasadne jest postulować, by zasady tworzenia BCR, kryteria, jakie owe normy powinny spełniać i mechanizmy ich weryfikacji określały przepisy prawa powszechnie obowiązującego. Przepisy te powinny znaleźć się w aktach dotyczących ochrony danych osobowych.

[23] Szerzej zob. X. Konarski, G. Sibiga, *Zasady przekazywania danych osobowych do państwa trzeciego w prawie polskim i Unii Europejskiej*, [w:] *Ochrona danych osobowych. Aktualne problemy i nowe* wyzwania, pod. Red. G. Sibigi i X. Konarskiego, s. 87 i n., B.Fischer, *Cloud computing*…, 207-231

[24] Szerzej zob. J. Byrski, X. Konarski, *Wiążące reguły korporacyjne jako podstawa przekazywania danych osobowych do państwa trzeciego*, [w] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. A. Mednis, s. 91; B.Fischer, *Cloud computing*… s.231 i n.; B.Fischer, *Transgraniczność prawa ...*, s. 270 i n.

[25] Zob. ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. poz. 1662), weszła w życie 01.01.2015 r. między innymi nowelizując uodo.

[26] Szerzej zob. B. Fischer, komentarz do art. 47, w: *Ogólne* rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Warszawa 2018, s. 480 i n.

[27] Zob. A. Krasuski, *Chmura …*,, s. 99 oraz 104-212.

Zaznaczyć należy przy tym, że obecnie przetwarzanie danych w chmurach jest prawnie dopuszczalne. W przypadku polskich przepisów *outsourcing* danych osobowych następuje na podstawie art. 31 uodo, w sytuacji przekazywania danych osobowych do państwa trzeciego - na podstawie art. 47 i art. 48 uodo z uwzględnieniem wiążących reguł korporacyjnych i standardowych klauzul umownych określonych w decyzjach Komisji Europejskiej[28]. Tyle tylko, że stosowanie tych przepisów w przypadku technologii CC nie wydaje sie efektywne[29].

ADMINISTRATOR A PRZETWARZAJĄCY PRZY PRZETWARZANIU DANYCH OSOBOWYCH W CHMURZE

W przypadku technologii *cloud* traci aktualność modelowe rozróżnienie administratora (*data controller*) oraz podmiotu, któremu powierzono przetwarzanie danych (*data processor*). Wprawdzie Grupa Robocza Art. 29 przyjęła 16 lutego 2010 r. opinię 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"[30], ale ponieważ nie rozstrzyga ona wszystkich wątpliwości, konieczne jest każdorazowe analizowanie statusu podmiotów uczestniczących w przetwarzaniu danych. Klasyfikacja podmiotu odpowiednio, jako administrator lub podmiot, któremu powierzono przetwarzanie danych osobowych, powinna zostać uzależniona od zakresu i sposobu przetwarzania danych osobowych. Dostawca usługi chmury obliczeniowej jest podmiotem, który może wystąpić jednocześnie w dwóch rolach – pierwsza rola, jako ten, komu administrator powierzył przetwarzanie danych osobowych – oraz druga rola, jako administrator w zakresie decydowania i implementacji określonych celów i środków przetwarzania informacji. Podział zaciera się, bo to dostawca chmury, udostępniając oprogramowanie i infrastrukturę, *de facto* określa środki przetwarzania, a także może wpływać na jego cel dzięki oferowanym usługom i funkcjonalnościom. Usługi oferowane przez dostawców chmury mogą być na tyle specjalistycznymi usługami i jednocześnie prostymi w użyciu, że administratorzy będą musieli brać pod uwagę możliwości zastosowania nowych metod przetwarzania danych osobowych, które wpływają na możliwości związane z określaniem nowych, innowacyjnych celów przetwarzania. Zatem stosując taką interpretację należy uznać dostawcę usługi chmury obliczeniowej jednocześnie jako administratora lub procesora w zależności od kontekstu przetwarzania.

Powierzenie przetwarzania danych osobowych przez administratora powinno być zgodne z wymaganiami wynikającymi z art. 28 RODO[31]. Powierzenie przetwarzania danych osobowych powinno zostać określone na zasadzie równości stron.

[28] O standardowych klauzulach umownych szerzej zob. B. Fischer, *Transgraniczność prawa ...*, s. 229 i n.
[29] Szerzej zob. B. Fischer, *Ochrona prywatności ...*, s. 218 i n.; W.R. Wiewiórowski, *Prawne aspekty ...*, s. 90.
[30] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_pl.pdf.
[31] Szerzej zob. M. Sakowska-Baryła, komentarz do art. 28, w: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018. s. 315 i n.

Często silniejsza pozycja dostawcy chmury obliczeniowej może doprowadzić do sytuacji, w której administrator nie będzie miał możliwości przeprowadzenia audytów lub inspekcji u dostawcy, z którym zawiera umowę. Innym aspektem istotnym z punktu widzenia administratora jest weryfikacja tego, czy dostawca usług CC przetwarza dane osobowe w państwach trzecich oraz czy istnieją w związku z tym odpowiednie mechanizmy prawne, które dadzą administratorowi właściwą ochronę prawną[32].

PRZETWARZANIE DANYCH W CHMURZE PRZEZ ORGANY WŁADZY PUBLICZNEJ

Przetwarzanie chmurowe to zagadnienie interesujące także władze publiczne, ponieważ staje się ono ważnym elementem strategii rozwoju podmiotów realizujących zadania publiczne. Ponadto technologia CC okazuje się tą, która zwiększenie wydolności publicznych usług, od których oczekuje się sprawności i które także podlegają procesom "wirtualizacji". Wraz z postępującą informatyzacją usług publicznych, wzrasta potrzeba sięgania po usługi chmurowe. W tym stanie rzeczy organ administracji publicznej narażony jest na nieznane mu zagrożenia, bo np. akceptacja standardowych klauzul umownych, jakimi posługuje się dostarczyciel chmury, może oznaczać, że ten publiczny administrator godzi się na zmianę sposobu przetwarzania danych, bądź na to, by dostarczyciel usług CC i jego podwykonawcy używali danych osobowych pochodzących od organu do innych celów, niż realizacja zadań publicznych. Pozbawia to organ kontroli nad danymi osobowymi. Dlatego też znacznie bezpieczniejszym z punktu widzenia tej kontroli wydaje się przetwarzanie danych w chmurze dedykowanej, w odniesieniu do której możliwe jest wynegocjowanie z dostawcą chmury umowy eliminującej tego rodzaju niebezpieczeństwo[33].

W przypadku podmiotów publicznych przetwarzanie chmurowe może jednocześnie pociągać za sobą powstanie pokusy uzyskania dostępu do danych w szerszym zakresie, niż to niezbędne w demokratycznym państwie prawnym. Można bowiem wyobrazić sobie sytuację, w której dostarczyciel chmury jest obciążony obowiązkiem ujawniania danych organom publicznym (policji, służbom specjalnym), choć przetwarzania tego nie sposób uznać za niezbędne w demokratycznym państwie prawnym (art. 51 ust. 2 Konstytucji RP). Wątpliwości tego rodzaju odnoszą się zresztą i do władz publicznych państw dostarczycieli chmury. Trudno ograniczyć zakres podmiotów, które będą miały dostęp do danych w chmurze wyłącznie na zasadzie umownej, ale obecnie właśnie tak się to odbywa. Centra CC twierdzą, że dane pozostają wyłącznie pod kontrolą zamawiającego, jednak nie ma możliwości ustalenia, czy dostarczyciele chmury nie ingerują w dane osobowe oraz czy nie ciążą na nich obowiązki sprowadzające się do ujawnienia danych organom publicznym.

[32] Należy zwrócić uwagę na to, że nie każdy mechanizm prawny jest w pełni skuteczny. Mechanizm tzw. Bezpiecznej Przystani (ang. Safe Harbour) został w dniu 6 października 2015 roku podważony. Następcą Safe Harbour jest EU-US Privacy Shield wobec, którego również istnieje ryzyko związane z możliwością podważenia przez właściwe organy.

[33] Zob. W.R. Wiewiórowski, *Prawne aspekty ...*, s. 89-91.

Tymczasem zapewnienie ochrony danym osobowym oznacza także przewidywalność tego, kto legalnie będzie mógł mieć do nich dostęp.

W związku z rozwojem i popularnością przetwarzania chmurowego oraz licznymi wątpliwościami dotyczącymi ochrony danych osobowych Generalny Inspektor Ochrony Danych Osobowych (GIODO) kilka lat temu przygotował "dekalog chmuroluba", który wskazuje, na co zwracać uwagę przy wyborze usługi CC, zwłaszcza, gdy wyboru tego dokonują podmioty publiczne, do których owe dziesięć zasad zostało skierowane[34]. Z uwagi na ich doniosłość i uniwersalność warto wprost wskazać na te zasady:

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 .

[34] http://www.giodo.gov.pl/259/id_art/6271/j/pl.

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"[35].

Formułując tak określone zasady, GIODO zaznaczył jednocześnie, że "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"[36].

[35] http://www.giodo.gov.pl/259/id_art/6271/j/pl.
[36] Tamże.

BEZPIECZEŃSTWO PRZETWARZANIA W CHMURACH OBLICZENIOWYCH

Usługi dostarczane przez dostawców CC zwykle oferują wysoki poziom bezpieczeństwa na każdej płaszczyźnie przetwarzania informacji, np. bezpieczeństwa fizycznego, kontroli dostępu, odporności na awarie, czy ochronie przed atakami polegającymi na przeciążeniu aplikacji (blokadzie usług)[37].

W celu zagwarantowania odpowiedniego poziomu bezpieczeństwa dla świadczonych usług dostawcy rozwiązań w modelu chmury obliczeniowej podejmują działania w celu przeprowadzenia wewnętrznych oraz zewnętrznych audytów w odniesieniu do powszechnie stosowanych wzorców i wytycznych w zakresie bezpieczeństwa, np. PCI DSS[38], normy z serii ISO, NIST 800-53, HIPAA[39], SOC2. Przeprowadzone audyty obejmują przykładowo aspekty takie jak poufność, integralność, dostępność oraz możliwość zapewnienia odpowiedniego poziomu prywatności w kontekście środków zarówno organizacyjnych, jak i technicznych dla świadczonej usługi CC. Następstwem podejmowanych działań może być certyfikacja na zgodność z określonymi normami, a uzyskanie certyfikacji przez dostawcę usług chmury obliczeniowej może być sposobem wykazania rozliczalności, zarówno przez dostawcę, jak i administratora, którego celem jest wykazanie tego, że stosuje wyłącznie usług spełniające ściśle określone standardy.

Prawne regulacje, które dotyczą mechanizmów certyfikacji, zostały wprowadzone przez art. 42 RODO. Administrator może dobrowolnie poddać się certyfikacji na mocy wskazanego przepisu zgodnie z przepisami określonymi na poziomie prawa krajowego. Treść zawarta w motywie 81 rodo stanowi, że certyfikacja może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora. Następnie, prawodawca odnosi się do mechanizmów certyfikacji w ogólnym rozporządzeniu w ramach przepisów dotyczących przede wszystkim obowiązków administratora (art. 24 ust. 3), ochrony danych w fazie projektowania (art. 25 ust. 3), podmiotów przetwarzających (art. 28 ust. 5 i 6), bezpieczeństwa przetwarzania (art. 32 ust. 3) oraz przekazywania danych do państw trzecich z zastrzeżeniem odpowiednich zabezpieczeń (art. 47 ust. 2 lit. f). Prawodawca odnosząc się w wymienionych normach prawnych do stosowania mechanizmów certyfikacji jasno wskazuje, że wywiązywanie się z obowiązków nakładanych na dostawców CC może być wykazane przez zastosowanie zatwierdzonego mechanizmu certyfikacji[40].

W związku z powyższym wysoki poziom bezpieczeństwa, który jest udokumentowany przez dostawcę CC i często weryfikowany przez niezależne podmioty jest argumentem dla administratorów danych, aby właśnie z tego powodu wybrać model przetwarzania oparty o usługi CC.

---

[37] Denial of Service (ang) – atak przeprowadzony na rozwiązanie teleinformatyczne, którego celem jest uniemożliwienie działania elementów infrastruktury teleinformatycznej

[38] Payment Card Industry Data Security Standard

[39] Health Insurance Portability and Accountability Act

[40] Szerzej zob. B. Fischer, komentarz do art. 42, w: *Ogólne rozporządzenie o ochronie dnaych osobowych. Komentarz,* Warszawa 2018, s. 446 i n.

Administrator może wówczas w prosty sposób wykazać stosowanie odpowiednich środków bezpieczeństwa, co może być szczególnie istotne z punktu widzenia zasady rozliczalności (art. 5 ust. 2 rodo)[41], zwłaszcza w kontekście przepisów dotyczących bezpieczeństwa przetwarzania (art. 32 rodo). Samodzielne wdrożenie mechanizmów bezpieczeństwa przez administratorów o podobnym standardzie i zakresie, jak w modelu CC w wielu przypadkach mogłoby być dla nich nieosiągalne z uwagi na wysokie koszty, potrzebę posiadania odpowiedniego know-how oraz czas niezbędny na wdrożenie i ciągłe utrzymywanie całej infrastruktury teleinformatycznej.

Administrator musi mieć również świadomość tego, że wybór modelu chmury obliczeniowej wiąże się z istnieniem ryzyka odnoszącego się do różnych płaszczyzn przetwarzania informacji. Pomimo tego, że dostawca usług chmurowych podejmuje wszelkie środki, aby przetwarzane dane były bezpieczne to zawsze istnieje ryzyko utraty danych choćby z uwagi na błąd dostawcy usługi, który może być spowodowanym uszkodzeniem lub przypadkowym usunięciem danych[42].

W związku z istniejącym ryzykiem utraty danych spowodowanej wyborem jednego dostawcy administrator powinien ocenić, czy ewentualne konsekwencje utraty danych będą dla niego dotkliwe i następnie rozważyć stosowanie korzystania z usług dodatkowego dostawcy usług, np. w celu przechowywania kopii zapasowych danych. Ponadto, administrator danych powinien zabezpieczyć się przed tzw. uzależnieniem od jednego dostawcy (ang. *vendor lock-in*), co wiąże się z dostosowaniem swoich rozwiązań, np. własnego oprogramowania, w taki sposób, aby możliwe było uruchomienie oprogramowania oraz przeniesienie danych z infrastruktury jednego dostawcy do zasobów drugiego dostawcy.

Kolejnym aspektem związanym z bezpieczeństwem korzystania z chmur obliczeniowych jest to, że incydenty bezpieczeństwa lub naruszenia ochrony danych mogą być wynikiem braku odpowiedniej wiedzy samego administratora. Administratorzy często popełniają błędy związane z samą konfiguracją chmury obliczeniowej, co może doprowadzić do publicznego udostępnienia danych osobowych. Dla przykładu zamieszczony poniżej fragment polityki bezpieczeństwa w zakresie dostępu do usługi Simple Storage Service (S3) udostępnianej w ramach chmury AWS daje każdemu m.in. uprawnienia do odczytu informacji zapisanych w ramach wydzielonych i zamieszczonych tam zasobów przez administratora[43]

[41] O zasadach rozliczalności przetwarzania szerzej zob. A. Nerka, komentarz do art. 5, w: *Ogólne rozporządzenie o ochronie dnaych osobowych. Komentarz,* Warszawa 2018, s. 141 i n.

[42] Utrata danych użytkowników programu Evernote w wersji na Mac - https://techcrunch.com/2016/10/13/evernote-confirms-a-serious-bug-caused-data-loss-for-some-mac-users/ ; Utrata danych użytkownika Dropbox - https://petapixel.com/2014/07/31/cautionary-tale-bug-dropbox-permanently-deleted-8000-photos/;

[43] Incydent bezpieczeństwa związany z błędną konfiguracją usługi chmury w ramach rozwiązani Amazon S3 będący wynikiem błędnej konfiguracji- https://www.esecurityplanet.com/cloud/cloud-security-fail-classified-u.s.-military-data-exposed-in-amazon-s3-bucket.html [dostęp04.04.2019]

{
"Statement": [
{
"Effect": "Allow",
"Action": "s3:*",
"Resource": "*",
"Principal":"*"
}
]
}

Minimalizowanie ryzyka związanego z brakiem wiedzy odnośnie konfiguracji i zarzadzania chmurą obliczeniową może być przeprowadzone przez certyfikację pracowników i egzaminy w zakresie wytwarzania oprogramowania w chmurze, projektowania rozwiązań chmurowych lub zarządzania usługami chmurowymi.

Innym ryzykiem związanym z bezpieczeństwem przetwarzania danych osobowych w modelu chmury obliczeniowej jest zagrożenie wiążące się ściśle z aspektami finansowymi, zarówno po stronie dostawcy chmury, jak i administratora, który chce korzystać z usług CC. Prawidłowe wyliczenie kosztów po stronie administratora jest szczególnie istotne, ponieważ błędy w kalkulacjach wynikające z niedoszacowania tego, jakie zasoby będą niezbędne administratorowi mogą doprowadzić do stanu, gdzie administrator przekroczy zakładane budżety i utraci płynność finansową. Natomiast z drugiej strony administrator musi zwrócić uwagę na ewentualność utraty płynności finansowej po stronie dostawcy usług CC i przygotować odpowiedni plan postępowania odnoszący się do aspektów prawnych, jak i technologicznych w związku z taką ewentualnością.

PODSUMOWANIE

Przetwarzanie danych osobowych za pośrednictwem chmur obliczeniowych daje administratorom wiele korzyści odnoszących się do aspektów biznesowych oraz aspektów związanych z bezpieczeństwem i pewnością przetwarzania informacji, w tym danych osobowych. Niemniej jednak przetwarzanie danych osobowych z użyciem chmur obliczeniowych niesie za sobą liczne zagrożenia, które powinny być przez administratorów uwzględnione na etapie projektowania lub analizy zagrożeń dla praw i wolności osób, których dane dotyczą (analiza ryzyka).

Nie jest wykluczone, że w przyszłości możliwości chmur obliczeniowych będą wykorzystywane praktycznie w każdym procesie przetwarzania informacji ze względu na prostotę wykorzystywania, coraz niższe koszty i niższe wymagania w zakresie wiedzy administratora w obszarze obsługi takich usług.

Należy przyjąć, że każdy administrator osobowych lub wyznaczony przez administratora procesor powinien mieć możliwość negocjowania umów w zakresie powierzenia przetwarzania danych osobowych w relacji z dostawcą usługi chmury obliczeniowej. Nie wykluczone, że w najbliższej przyszłości powstaną szczególne regulacje prawne dotyczące oferowania usług w chmurze, których celem będzie zapewnienie odpowiedniego poziomu równowagi pomiędzy dostawcą, a klientami usługi chmurowej. Aktualnie dostrzega się znaczną dysproporcję pomiędzy dostawcami usług chmury obliczeniowej a klientami. Stan taki jest niepożądany ze względu na kształtowanie się podmiotów o pozycji dominującej.