Grupa Robocza Artykułu 29 ds. Ochrony Danych

01037/12/PL
WP 196

Opinia 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej

Przyjęta w dniu 1 lipca 2012 r.

Niniejsza Grupa Robocza została powołana na mocy artykułu 29 Dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy w sprawach ochrony danych i prywatności. Jego zadania opisane zostały w artykule 30 Dyrektywy 95/46/WE i artykule 15 Dyrektywy 2002/58/WE.

Obsługę Sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, Biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Streszczenie

W niniejszej opinii Grupa Robocza Artykułu 29 analizuje wszystkie kwestie istotne dla dostawców usług przetwarzania danych w chmurze działających w Europejskim Obszarze Gospodarczym (EOG) oraz ich klientów, określając wszystkie mające zastosowanie zasady z Dyrektywy o ochronie danych UE (95/46/WE) oraz Dyrektywy o prywatności i łączności elektronicznej 2002/58/WE (zrewidowanej dyrektywą 2009/136/WE), gdy to właściwe.

Mimo uznanych korzyści płynących z przetwarzania danych w chmurze (tzw. cloud computingu) zarówno pod względem ekonomicznym, jak i społecznym, w niniejszej opinii przedstawiono, w jaki sposób wykorzystanie usług przetwarzania w chmurze na szeroką skalę może wywołać szereg zagrożeń, głównie takich jak brak kontroli nad danymi osobowymi oraz niewystarczające informacje na temat tego, w jaki sposób, gdzie i przez kogo dane są przetwarzane / przetwarzane przez podmiot, któremu powierzono przetwarzanie. Organy publiczne i przedsiębiorstwa prywatne muszą dokładnie ocenić te zagrożenia, gdy rozważają skorzystanie z usług oferowanych przez dostawcę usług w chmurze. W niniejszej opinii analizuje się kwestie związane z dzieleniem się zasobami z innymi stronami, brakiem przejrzystości łańcucha outsourcingu obejmującego licznych przetwarzających i podprzetwarzających, niedostępnością ogólnych globalnych ram w zakresie przenoszenia danych oraz niepewnością dotyczącą dopuszczalności przekazywania danych osobowych dostawcom usług w chmurze mającym siedzibę poza EOG. Podobnie, brak przejrzystości informacji, jakie administrator jest w stanie zapewnić osobie, której dane dotyczą na temat tego, jak przetwarzane są jej dane osobowe, jest wskazany w opinii jako kwestia budząca poważne obawy. Osoby, których dane dotyczą, muszą[1] być poinformowane o tym, kto przetwarza ich dane i w jakich celach oraz być w stanie realizować prawo przyznane im w tym zakresie.

Kluczowym wnioskiem płynącym z tej opinii jest fakt, że przedsiębiorstwa i organy administracji, które chcą skorzystać z usług przetwarzania danych w chmurze, powinny w pierwszej kolejności przeprowadzić szczegółową i dokładną analizę zagrożeń. Wszyscy dostawcy usług w chmurze oferujący usługi w EOG powinni zapewnić klientowi wszelkie

[1] Kluczowe słowa “MUSI’ (ang. "MUST"), “NIE MOŻE/NIE WOLNO” (ang. "MUST NOT"), “WYMAGANY’ (ang. "REQUIRED"), “POWINIEN/JEST ZOBOWIĄZANY’ (ang. "SHALL"), “NIE POWINIEN” ("SHALL NOT"), “POWINIEN” (ang. "SHOULD"), “ “NIE POWINIEN” (ang. "SHOULD NOT"), “ZALECANE” (ang. "RECOMMENDED"), “MOŻE” (ang. "MAY"), oraz “OPCJONALNE” (ang. "OPTIONAL") w tym dokumencie należy interpretować jak te opisane we Wniosku o uwagi 2119. Dokument jest dostępny na stronie: http://www.ietf.org/rfc/rfc2119.txt. Jednakże w celu ułatwienia czytelności słowa te nie są pisane dużymi literami w tej specyfikacji.

informacje niezbędne do odpowiedniego oszacowania zalet i wad korzystania z takiej usługi. Bezpieczeństwo, przejrzystość i pewność prawna dla klientów powinny być kluczowymi czynnikami związanymi z oferowaniem usług przetwarzania danych w chmurze.

Jeżeli chodzi o zalecenia zawarte w niniejszej opinii, podkreśla się odpowiedzialność klienta usługi w chmurze jako administratora i tym samym zaleca się, aby klient wybrał takiego dostawcę usługi w chmurze, który gwarantuje zgodność z ustawodawstwem UE w zakresie ochrony danych. W kwestii odpowiednich gwarancji umownych w opinii określono wymóg, że umowa między klientem usługi w chmurze i jej dostawcą powinna zapewniać odpowiednie gwarancje pod względem środków technicznych i organizacyjnych. Istotne jest również zalecenie, zgodnie z którym klient usługi w chmurze powinien sprawdzić, czy dostawca tej usługi może zagwarantować legalność wszelkich operacji transgranicznego międzynarodowego przekazywania danych.

Podobnie jak każdy proces ewolucji, rozwój cloud computingu jako globalnego technologicznego paradygmatu stanowi także wyzwanie. Niniejszą opinię, w jej obecnej formie, można traktować jako ważny krok w definiowaniu zadań, które mają być podjęte w tej kwestii przez środowisko zajmujące się ochroną danych ochrony danych w nadchodzących latach.

1. Wprowadzenie

Dla niektórych przetwarzanie danych w chmurze jest jedną z największych technologicznych rewolucji ostatnich czasów. Dla innych jest to jedynie naturalna ewolucja zestawu technologii mających na celu osiągnięcie długo oczekiwanego spełnienia snu o tzw. „utility computing". W każdym razie wielu interesariuszy definiując strategie technologicznego rozwoju na czele umieściło rozwój technologii przetwarzania w chmurze.

Cloud computing obejmuje zestaw technologii i modeli usług, które koncentrują się na wykorzystywaniu i dostarczaniu poprzez Internet aplikacji informatycznych, możliwości przetwarzania, zasobów pamięci („storage and memory space"). Przetwarzanie w chmurze obliczeniowej może przynieść znaczące korzyści ekonomiczne, ponieważ zasoby na żądanie można dosyć łatwo konfigurować, rozszerzać i mieć do nich dostęp w Internecie. Oprócz korzyści ekonomicznych cloud computing może przynieść także korzyści dotyczące bezpieczeństwa: przedsiębiorstwa, szczególnie małe i średnie, mogą nabyć, po koszcie marginalnym, najwyższej klasy technologie, które w innym przypadku przekraczałyby ich możliwości budżetowe.

Istnieje szeroka gama usług oferowanych przez dostawców usług w chmurze, począwszy od wirtualnych systemów przetwarzania (które zastępują i/lub działają obok tradycyjnych serwerów pod bezpośrednią kontrolą administratora) po usługi wspierające rozwijanie aplikacji i zaawansowany hosting, aż po bazujące na Internecie rozwiązania w zakresie oprogramowania, które mogą zastąpić aplikacje tradycyjnie instalowane na komputerach osobistych użytkowników końcowych. Chodzi tu o edytory tekstu, terminarze i kalendarze, systemy plików do przechowywania dokumentów online oraz zewnętrzne rozwiązania poczty e-mail. Załącznik do niniejszej opinii zawiera kilka z najpowszechniej stosowanych definicji dla tych różnych rodzajów usług.

W niniejszej opinii Grupa Robocza Artykułu 29 (dalej zwana GR Art. 29) analizuje właściwe prawo oraz obowiązki administratorów w Europejskim Obszarze Gospodarczym (dalej: EOG) oraz dostawców usług w chmurze z klientami w EOG. W opinii skupiono się na sytuacji, w której zakłada się relację administrator-przetwarzający, gdzie klient kwalifikuje się jako administrator a dostawca usługi w chmurze jako przetwarzający. W przypadkach, gdy dostawca usługi w chmurze działa również jako administrator, musi on spełnić dodatkowe wymogi. W konsekwencji warunkiem wstępnym polegania na rozwiązaniach cloud computingu jest przeprowadzenie przez administratora odpowiedniej oceny ryzyka,

obejmującej lokalizacje serwerów, gdzie przetwarzane są dane oraz rozważenie zagrożeń i korzyści z perspektywy ochrony danych, zgodnie z kryteriami określonymi poniżej.

W opinii określono zasady mające zastosowanie zarówno wobec administratorów, jak i przetwarzających, wynikające z ogólnej dyrektywy o ochronie danych (95/46/WE), takie jak określenie i ograniczenie celu, usuwanie danych oraz środki techniczne i organizacyjne. W opinii przedstawiono wytyczne dotyczące wymogów bezpieczeństwa, zarówno jako zabezpieczeń strukturalnych, jak i proceduralnych. Szczególny nacisk położono na ustalenie zobowiązań w umowie, które powinny regulować relację między administratorem a przetwarzającym w tym zakresie. Klasycznymi celami bezpieczeństwa danych są dostępność, integralność i poufność. Jednakże ochrona danych nie jest ograniczona do bezpieczeństwa danych i w związku z tym cele te są uzupełnione o określone cele z zakresu ochrony danych: przejrzystość, odizolowanie, możliwość interwencji i przenoszenia, w celu potwierdzenia prawa osoby fizycznej do ochrony danych, określonego w artykule 8 Karty Praw Podstawowych UE.

W odniesieniu do przekazywania danych osobowych poza EOG dokonano analizy instrumentów, takich jak standardowe klauzule umowne przyjęte przez Komisję Europejską, ustalenia adekwatności (odpowiedniego poziomu ochrony danych) oraz możliwe przyszłe wiążące reguły korporacyjne (BCR) dla przetwarzającego, jak również analizy zagrożeń z zakresu ochrony danych wynikających z międzynarodowych wniosków o egzekwowanie prawa.

Na końcu opinii przedstawiono zalecenia dla klientów usług w chmurze jako administratorów, dostawców usług w chmurze jako przetwarzających oraz Komisji Europejskiej w odniesieniu do przyszłych zmian europejskich ram prawnych ochrony danych.

Berlińska Międzynarodowa Grupa Robocza ds. Ochrony Danych w Telekomunikacji przyjęła *Memorandum z Sopotu*[2] w kwietniu 2012. W Memorandum zawarto analizę kwestii dotyczących ochrony danych i prywatności w przypadku przetwarzania danych w chmurze oraz pokreślono, że cloud computing nie musi prowadzić do obniżenia standardów ochrony danych w porównaniu z tradycyjnym przetwarzaniem danych.

2. Zagrożenia dla ochrony danych związane z przetwarzaniem danych w chmurze

[2] http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

Jako że niniejsza opinia koncentruje się na operacjach przetwarzania danych osobowych, rozważono w niej tylko określone zagrożenia związane z tym kontekstem.[3] Większość tych zagrożeń zalicza się do dwóch szerokich kategorii, mianowicie są to brak kontroli nad danymi oraz niewystarczające informacje dotyczące samej operacji przetwarzania (brak przejrzystości). Szczególne zagrożenia związane z cloud computingiem rozważane w niniejszej opinii obejmują:

Brak kontroli

Przekazując dane osobowe do systemów zarządzanych przez dostawcę usługi w chmurze, klienci tej usługi mogą nie mieć dalszej wyłącznej kontroli nad swoimi danymi. Oznacza to, że mogą nie mieć możliwości zastosowania środków technicznych i organizacyjnych na przykład w celu zapewnienia dostępności, integralności, poufności, przejrzystości, odizolowania[4], możliwości interwencji i możliwości przenoszenia danych. Ten brak kontroli może przejawiać się w następujący sposób:

- Brak dostępności ze względu na brak interoperacyjności (uzależnienie od dostawcy, tzw. „vendor lock-in"): Jeżeli dostawca usługi w chmurze bazuje na zastrzeżonej technologii, dla klienta usługi może się okazać trudne przenoszenie danych i dokumentów między różnymi systemami opartymi na cloud computingu (możliwość przenoszenia danych) lub wymiana informacji z podmiotami korzystającymi z usług w chmurze zarządzanych przez innych dostawców (interoperacyjność).
- Brak integralności spowodowany przez dzielenie się zasobami: Chmura składa się z współdzielonych systemów i infrastruktur. Dostawcy usług w chmurze przetwarzają dane osobowe wywodzące się z szeregu licznych źródeł - osób, których dane dotyczą, i organizacji – i istnieje możliwość, że mogą powstać sprzeczne interesy i/lub różne cele.
- Brak poufności w odniesieniu do wniosków z zakresu egzekwowania prawa składanych bezpośrednio do dostawcy usługi w chmurze: dane osobowe przetwarzane w chmurze mogą być przedmiotem wniosków z zakresu egzekwowania prawa pochodzących od organów egzekwowania prawa z państw członkowskich UE oraz krajów trzecich. Istnieje zagrożenie, że dane osobowe mogłyby być ujawnione

[3] Poza zagrożeniami związanymi z danymi osobowymi przetwarzanymi „w chmurze" wyraźnie wymienionymi w niniejszej opinii, pod uwagę trzeba wziąć także wszystkie zagrożenia związane z powierzaniem przetwarzania danych osobowych.

(zagranicznym) organom egzekwowania prawa bez ważnej podstawy prawnej UE i tym samym doszłoby do naruszenia prawa UE dotyczącego ochrony danych.

- Brak możliwości interwencji ze względu na złożoność i dynamiczność łańcucha outsourcingu: Usługa w chmurze oferowana przez jednego dostawcę może być realizowana poprzez połączenie usług od szeregu innych dostawców, które mogą być dynamicznie dodawane lub usuwane w czasie trwania umowy klienta.
- Brak możliwości interwencji (prawa osób, których dane dotyczą): Dostawca usługi w chmurze może nie zapewnić niezbędnych środków i narzędzi mających pomóc administratorowi zarządzać danymi np. w zakresie dostępu, usunięcia lub poprawienia danych.
- Brak odizolowania: Dostawca usługi w chmurze może wykorzystywać swoją fizyczną kontrolę nad danymi od różnych klientów w celu łączenia danych. Jeżeli dostawcy usługi administrujący przetwarzaniem mieliby wystarczające prawa uprzywilejowanego dostępu (role wysokiego ryzyka), mogliby łączyć informacje od różnych klientów (administratorów danych).

Brak informacji na temat przetwarzania (przejrzystości)

Niewystarczające informacje na temat operacji przetwarzania w chmurze stanowi zagrożenie dla administratorów, jak i dla osób, których dane dotyczą, ponieważ mogą oni nie być świadomi potencjalnych zagrożeń i tym samym nie mogą podjąć środków, które uważają za odpowiednie.

Niektóre potencjalne zagrożenia mogą wyniknąć z faktu, że administrator nie wie, że:

- W przetwarzanie zaangażowani są liczni przetwarzający i podprzetwarzający (łańcuch przetwarzania).
- Dane osobowe są przetwarzane w różnych lokalizacjach geograficznych w ramach EOG. Ma to bezpośredni wpływ na prawo właściwe dla wszelkich sporów z zakresu ochrony danych, które mogą wyniknąć między użytkownikiem a dostawcą.
- Dane osobowe są przekazywane do krajów trzecich poza EOG. Kraje trzecie mogą nie zapewniać odpowiedniego poziomu ochrony danych, a operacje przekazywania mogą

[4] W Niemczech wprowadzono szerszą koncepcję „niemożliwości łączenia" („unlinkability"). Patrz przypis 24 poniżej.

nie być zabezpieczone odpowiednimi środkami (np. standardowe klauzule umowne lub wiążące reguły korporacyjne) i tym samym mogą być niezgodne z prawem.

Wymagane jest poinformowanie osób, których dane osobowe są przetwarzane w chmurze, o tożsamości administratora danych i celu przetwarzania (istniejący wymóg dla wszystkich administratorów na mocy dyrektywy o ochronie danych 95/46/WE). Zważywszy na potencjalną złożoność łańcuchów przetwarzania w środowisku przetwarzania w chmurze, w celu zagwarantowania rzetelnego przetwarzania w odniesieniu do osoby, której dane dotyczą (artykuł 10 dyrektywy 95/46/WE), administratorzy powinni również, w ramach stosowania dobrych praktyk, zapewnić dalsze informacje dotyczące (pod)przetwarzających świadczących usługi w chmurze.

2. Ramy prawne

3.1 Ramy prawne ochrony danych

Właściwe ramy prawne to dyrektywa o ochronie danych 95/46/WE. Ma ona zastosowanie w każdym przypadku, gdy dane osobowe są przetwarzane w wyniku korzystania z usług przetwarzania w chmurze. Dyrektywa 2002/58/WE o prywatności i łączności elektronicznej (zrewidowana dyrektywą 2009/136/WE) dotyczy przetwarzania danych osobowych w związku z świadczeniem powszechnie dostępnych usług łączności elektronicznej w publicznych sieciach łączności (operatorzy telekomunikacyjni) i tym samym ma zastosowanie, gdy takie usługi są świadczone przy wykorzystaniu technologii przetwarzania w chmurze[5].

3.2 Właściwe prawo

Kryteria stosowania właściwego ustawodawstwa zawarte są w artykule 4 dyrektywy 95/46/WE, który dotyczy prawa mającego zastosowanie do administratorów[6] mających jedną lub więcej siedzib w ramach EOG, a także prawa mającego zastosowanie do administratorów będących poza EOG, ale wykorzystujących do przetwarzania danych osobowych środki

[5] Dyrektywa 2002/58/WE o prywatności i łączności elektronicznej (zmieniona dyrektywą 2009/136/WE): dyrektywa 2002/58/WE o ochronie prywatności w sektorze łączności elektronicznej ma zastosowanie do dostawców usług łączności elektronicznej udostępnianych ogółowi i wymaga od nich, aby zapewniali przestrzeganie zobowiązań dotyczących poufności komunikacji i ochrony danych osobowych, jak również praw i obowiązków w odniesieniu do sieci i usług łączności elektronicznej. W przypadkach, gdy dostawcy cloud computingu działają jako dostawcy publicznie dostępnych usług łączności elektronicznej, będą podlegać tej regulacji.

[6] Koncepcja administratora zawarta jest w artykule 2.h) dyrektywy i została poddane analizie przez GR Art. 29 w Opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający".

zlokalizowane w ramach EOG. Grupa Robocza Artykułu 29 przeanalizowała tę kwestię w Opinii 8/2010 w sprawie prawa właściwego[7].

W pierwszym przypadku czynnikiem powodującym zastosowanie prawa UE wobec administratora jest lokalizacja jego siedziby oraz prowadzona przez niego działalność, zgodnie z artykułem 4 ust. 1 lit. a) dyrektywy, gdy rodzaj modelu usługi w chmurze jest nieistotny. Właściwe ustawodawstwo to prawo kraju, w którym siedzibę ma administrator powierzający usługi przetwarzania w chmurze, a nie miejsca, w którym dostawcy usług w chmurze mają lokalizację.

Jeżeli administrator ma siedziby w różnych państwach członkowskich, przetwarzając dane w ramach jego działalności w tych krajach, właściwym prawem powinno być prawo każdego z państw członkowskich, w którym prowadzone jest przetwarzanie.

Artykuł 4 ust. 1 punkt c)[8] dotyczy tego, w jaki sposób ustawodawstwo w zakresie ochrony danych ma zastosowanie do administratorów, którzy nie mają siedziby w EOG, ale wykorzystują środki zautomatyzowane lub niezautomatyzowane zlokalizowane na terytorium państwa członkowskiego, z wyjątkiem sytuacji, gdy środki są wykorzystywane tylko do celów tranzytu. Oznacza to, że jeżeli klient usługi w chmurze ma siedzibę poza EOG, ale powierza wykonawstwo dostawcy usługi w chmurze mającego lokalizację w EOG, wówczas ustawodawstwo o ochronie danych ma zastosowanie wobec klienta.

3.3 Zadania i obowiązki różnych podmiotów

Jak wskazano wcześniej, w proces przetwarzania w chmurze zaangażowanych jest szereg różnych podmiotów. Ważne jest, aby ocenić i wyjaśnić rolę każdego z tych podmiotów w celu ustalenia ich konkretnych obowiązków w odniesieniu do obecnie obowiązującego ustawodawstwa w zakresie ochrony danych.

Należy przypomnieć, że GR Art. 29 wskazała w swojej opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", że „*w przypadku pojęcia administratora danych podstawową i najważniejszą rolą jest określenie, kto odpowiada za zgodność z zasadami ochrony danych i w jaki sposób osoby, których dane dotyczą, mogą w praktyce wykonywać swoje prawa. Innymi słowy: powierzenie odpowiedzialności."* Zaangażowane strony powinny

[7] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_pl.pdf

[8] Artykuł 4 ust. 1 lit. c stanowi, że ustawodawstwo państwa członkowskiego ma zastosowanie wówczas, gdy „administrator danych nie prowadzi działalności gospodarczej na terytorium Wspólnoty a do celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane jak i inne, znajdujące się na

pamiętać o tych dwóch głównych kryteriach dotyczących odpowiedzialności za zgodność oraz powierzenia odpowiedzialności podczas całej analizy, o której mowa.

3.3.1 Klient i dostawca usługi w chmurze

Klient usługi w chmurze określa ostateczny cel przetwarzania i decyduje o powierzeniu tego przetwarzania oraz oddelegowaniu wszystkich lub części działań w zakresie przetwarzania zewnętrznej organizacji. Zatem klient usługi w chmurze działa jako administrator danych. Dyrektywa definiuje administratora jako „*osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych"*. Klient usługi w chmurze, jako administrator, musi przyjąć odpowiedzialność za przestrzeganie ustawodawstwa w zakresie ochrony danych i jest odpowiedzialny oraz podlega wszelkim obowiązkom prawnym, o których mowa w dyrektywie 95/46/WE. Klient usługi w chmurze może powierzyć dostawcy usługi w chmurze zadanie wyboru metod oraz środków technicznych lub organizacyjnych, które mają być wykorzystane w celu osiągnięcia celów administratora.

Dostawca usługi w chmurze to podmiot, który świadczy usługi cloud computingu w różnych formach omówionych powyżej. Gdy dostawca usługi w chmurze dostarcza środki oraz platformę, działając w imieniu klienta usługi chmurze, dostawca takiej usługi jest uważany za przetwarzającego dane, tj. zgodnie z dyrektywą 95/46/WE „*osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami przetwarza dane osobowe w imieniu administratora"*.[9] [10]

Jak określono w Opinii 1/2010, niektóre kryteria[11] można wykorzystać do oceny sprawowania kontroli nad przetwarzaniem. Rzeczywiście może mieć miejsce wiele sytuacji, w których dostawca usług w chmurze może być uznany albo za współ-administratora albo za administratora w zależności od konkretnych okoliczności. Może mieć to np. miejsce, gdy dostawca przetwarza dane do własnych celów.

---

terytorium wymienionego Państwa Członkowskiego, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium Wspólnoty

[9] Niniejsza opinia koncentruje się na zwykłej relacji administrator – przetwarzający.

[10] Środowisko cloud computingu może być także wykorzystywane przez osoby fizyczne (użytkowników) do wykonywania działalności o charakterze wyłącznie osobistym lub domowym. W takim przypadku należy dokładnie przeanalizować, czy ma zastosowanie tzw. wyłączenie ze względu na charakter domowy (działania), które zwalnia użytkowników z bycia uznanymi za administratorów. Jednak ta kwestia wykracza poza zakres niniejszej opinii.

[11] Np. poziom instrukcji, monitoringu prowadzonego przez klienta usługi w chmurze, wiedzy specjalistycznej stron

Należy podkreślić, że nawet w złożonych środowiskach przetwarzania danych, gdzie różni administratorzy odgrywają rolę w przetwarzaniu danych osobowych, należy wyraźnie przydzielić odpowiedzialność za przestrzeganie zasad ochrony danych oraz zobowiązania wynikające z ewentualnego naruszenia tych zasad, aby uniknąć sytuacji, gdy ochrona danych osobowych będzie ograniczona lub powstanie „negatywny konflikt w zakresie kompetencji" i luki, podczas gdy niektóre obowiązki i prawa wynikające z dyrektywy nie będą zapewnione przez żadną ze stron.

W obecnym scenariuszu przetwarzania danych w chmurze, klienci usług w chmurze mogą nie mieć marginesu swobody przy negocjowaniu umownych warunków wykorzystywania usług w chmurze, ponieważ standardowe oferty są cechą wielu usług cloud computingu. Niemniej ostatecznie to klient decyduje o przydzieleniu części lub wszystkich operacji przetwarzania usługom w chmurze w określonych celach; rolą dostawcy usług w chmurze będzie rola wykonawcy względem klienta, co jest kluczowym elementem w tym przypadku. Jak określono w Opinii 1/2010[12] Grupy Roboczej w sprawie pojęć „administrator danych" i „przetwarzający", „*nie należy uznawać nierównowagi w określonych w umowie uprawnieniach małego administratora danych w stosunku do dużego usługodawcy, jako uzasadnienia przyjmowania przez administratora danych klauzul i warunków umów niezgodnych z przepisami dotyczącymi ochrony danych*". Z tego powodu administrator musi wybrać dostawcę usługi w chmurze, który gwarantuje zgodność z przepisami dotyczącymi ochrony danych. Szczególny nacisk należy położyć na klauzule mających zastosowanie umów – muszą one obejmować zestaw standardowych zabezpieczeń w zakresie ochrony danych, w tym te wymienione przez GR w punkcie 3.4.3 (Środki techniczne i organizacyjne) i 3.5 (transgraniczne przekazywanie danych) – jak również na dodatkowe mechanizmy, które mogą okazać się przydatne w celu ułatwienia zapewnienia należytej staranności i rozliczalności (np. niezależne audyty przeprowadzane przez strony trzecie oraz certyfikacje usług dostawcy – patrz punkt 4.2).

Dostawcy usług w chmurze (jako przetwarzający) mają obowiązek zapewnienia poufności. Dyrektywa 95/46/WE stanowi, że: „*Żadna osoba działająca z upoważnienia administratora danych lub przetwarzającego, włączając samego przetwarzającego, który ma dostęp do danych osobowych, nie może przetwarzać ich bez polecenia administratora danych, chyba że wymaga tego prawo"*. Dostęp dostawcy usług w chmurze do danych w czasie świadczenia

[12] Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_pl.pdf

usług również generalnie wiąże się z wymogiem przestrzegania postanowień artykułu 17 dyrektywy – patrz punkt 3.4.2.

Przetwarzający muszą wziąć pod uwagę rodzaj danej chmury (publiczna, prywatna, wspólnotowa lub hybrydowa / IaaS, SaaS lub PaaS [patrz Załącznik a) Modele wdrożenia – b) Modele świadczenia usługi]) oraz rodzaj usługi powierzonej przez klienta. Przetwarzający są odpowiedzialni za przyjęcie środków bezpieczeństwa zgodnych z tymi przewidzianymi w ustawodawstwie UE, stosowanych w jurysdykcjach administratora i przetwarzającego. Przetwarzający muszą również wspierać administratora i pomagać mu w przestrzeganiu (realizowanych) praw osób, których dane dotyczą.

3.3.2 Podmioty, którym podpowierzono świadczenie usług

Usługi przetwarzania w chmurze mogą cechować się zaangażowaniem szeregu stron, którym powierzono usługi i którzy działają jako przetwarzający. Powszechne jest również podpowierzanie usług przez przetwarzających dodatkowym podprzetwarzającym, którzy następnie uzyskują dostęp do danych osobowych. Jeżeli przetwarzający podpowierzają usługi podprzetwarzającym, są zobowiązani do udostępnienia tych informacji klientowi, podając rodzaj podpowierzonej usługi, określając obecne lub potencjalne podmioty, którym podpowierzono usługi, oraz wskazując gwarancje, jakie podmioty te oferują dostawcy usług cloud computingu celem zapewnienia zgodności z dyrektywą 95/46/WE.

W związku z tym wszystkie istotne obowiązki muszą mieć zastosowanie również wobec podprzetwarzających na mocy umów między dostawcą usługi w chmurze a podmiotem, któremu powierzono jej świadczenie, odzwierciedlając postanowienia umowy między klientem a dostawcą usługi w chmurze. W Opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" Grupa Robocza Artykułu 29 odniosła się do faktu istnienia wielu przetwarzających w przypadkach, w których przetwarzający mogą mieć bezpośredni kontakt z administratorem lub mogą działać jako podmioty, którym podpowierzono usługi, gdy przetwarzający zlecają na zewnętrz część działań z zakresu przetwarzania, będących ich zadaniem. „*Żaden z przepisów dyrektywy nie zabrania tego ze względu na wymogi organizacyjne, jako wykonawców lub podwykonawców przetwarzania danych można wyznaczyć szereg podmiotów, również poprzez podział odnośnych zadań. Przetwarzając dane*

wszystkie takie podmioty mają jednak obowiązek przestrzegać instrukcji wydanych przez administratora danych."[13]

W takich scenariuszach obowiązki i odpowiedzialność wynikająca z ustawodawstwa w zakresie ochrony danych powinny być wyraźnie określone i nie powinny być rozproszone w całym łańcuchu zlecania lub podpowierzania, w celu zapewnienia skutecznej kontroli nad działaniami w zakresie przetwarzania i jasnego przydzielenia odpowiedzialności za nie.

Potencjalny model gwarancji, który może być wykorzystany w celu wyjaśnienia obowiązków przetwarzających, gdy podpowierzają przetwarzanie danych, został po raz pierwszy wprowadzony Decyzją Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich.[14] W tym modelu podprzetwarzanie jest dozwolone tylko za uprzednią pisemną zgodą administratora oraz na podstawie pisemnych umów nakładających takie same obowiązki na podprzetwarzającego jak te nałożone na przetwarzającego. W sytuacji, gdy podprzetwarzający nie spełni zobowiązań z zakresu ochrony danych w ramach takiej pisemnej umowy, przetwarzający pozostaje w pełni odpowiedzialny wobec administratora za wykonanie zobowiązań podprzetwarzającego wynikających z takiej umowy. Takie postanowienie można by wykorzystać w każdych klauzulach umownych między administratorem a dostawcą usługi w chmurze, gdy ten ostatni zamierza świadczyć usługi w ramach ich podpowierzenia, w celu zapewnienia gwarancji wymaganych dla podprzetwarzania.

Podobne rozwiązanie dotyczące gwarancji w trakcie podpowierzonego przetwarzania zaproponowała niedawno Komisja we wniosku dotyczącym ogólnego rozporządzenia o ochronie danych[15]. Przetwarzanie przez podmiot przetwarzający jest regulowane umową lub innym aktem prawnym wiążącym podmiot przetwarzający z administratorem i stanowiącym w szczególności, że podmiot przetwarzający zatrudnia inny podmiot przetwarzający jedynie za uprzednią zgodą administratora (artykuł 26 ust. 2 wniosku).

Zdaniem GR Art. 29 przetwarzający może podpowierzyć swoje działania tylko na podstawie zgody administratora, która generalnie może być udzielona na początku świadczenia usługi[16],

[13] Patrz WP169, str. 29, Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_pl.pdf
[14] Patrz CZĘSTO ZADAWANE PYTANIE II.5 WP176.
[15] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, 25.1.1012 r.
[16] Patrz CZĘSTO ZADAWANE PYTANIE II, 1) WP176, przyjęty 12 lipca 2010 r.

z jasno określonym obowiązkiem, aby przetwarzający informował administratora o wszelkich planowanych zmianach dotyczących dodania lub zastąpienia podmiotów, którym podpowierzono przetwarzanie, przy czym administrator przez cały czas zachowuje możliwość wyrażenia sprzeciwu wobec takich zmian lub zakończenia umowy. Powinien istnieć wyraźny obowiązek nakazujący dostawcy usługi w chmurze wskazania wszystkich podmiotów, którym podpowierzono/zlecono usługi. Ponadto powinna być podpisana umowa między klientem a dostawcą usługi w chmurze, odzwierciedlająca postanowienia umowy między klientem a dostawcą usługi w chmurze. Administrator powinien mieć możliwość skorzystania z umownych środków odwoławczych w przypadku naruszeń umów spowodowanych przez podprzetwarzających. Można to ustanowić zapewniając, że przetwarzający będzie bezpośrednio odpowiedzialny wobec administratora za wszelkie naruszenia spowodowane przez wszelkich podprzetwarzających, których wskazał, lub tworząc prawo beneficjenta-strony trzeciej na rzecz administratora w umowach podpisanych między przetwarzającym a podprzetwarzającymi lub przez fakt, że umowy te będą podpisane w imieniu administratora danych, czyniąc tego ostatniego stroną umowy.

3.4 Wymogi w zakresie ochrony danych w relacji klient-dostawca

3.4.1 Przestrzeganie podstawowych zasad

Legalność przetwarzania danych osobowych w chmurze zależy od przestrzegania podstawowych zasad prawa UE w zakresie ochrony danych: Mianowicie musi być zagwarantowana przejrzystość wobec osoby, której dane dotyczą, musi być przestrzegana zasada określenia i ograniczenia celu, a dane osobowe muszą być usunięte jak tylko ich przechowywanie nie jest już niezbędne. Ponadto należy wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia odpowiedniego poziomu ochrony danych i bezpieczeństwa danych.

3.4.1.1 Przejrzystość

Przejrzystość ma kluczowe znaczenie dla rzetelnego i zgodnego z prawem przetwarzania danych osobowych. Dyrektywa 95/46/WE zobowiązuje klienta usługi w chmurze do zapewnienia osobie, której dane dotyczą i od której gromadzone są dane, informacje na temat jego tożsamości i celu przetwarzania. Klient usługi w chmurze powinien również przedstawić wszelkie dalsze informacje, np. dotyczące odbiorców lub kategorii odbiorców danych, mogących obejmować także przetwarzających i podprzetwarzających, o ile takie

dalsze informacje są potrzebne w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą (patrz artykuł 10 dyrektywy)[17].

Przejrzystość musi być zapewniona w relacji (relacjach) między klientem usługi w chmurze, dostawcą takiej usługi i podmiotami, którym podpowierzono usługi (o ile tacy istnieją). Klient usługi w chmurze jest jedynie w stanie ocenić legalność przetwarzania danych osobowych w chmurze, jeśli dostawca poinformuje klienta o wszelkich istotnych kwestiach. Administrator zastanawiający się nad zaangażowaniem dostawcy usługi w chmurze powinien dokładnie sprawdzić warunki tego dostawcy i ocenić je z punktu widzenia ochrony danych.

Przejrzystość w chmurze oznacza, że konieczne jest poinformowanie klienta usługi w chmurze o wszystkich podmiotach, którym powierzono określoną usługę i które przyczyniają się do świadczenia danej usługi w chmurze, jak również o lokalizacjach wszystkich ośrodków danych, w których mogą być przetwarzane dane osobowe.[18]

Jeżeli świadczenie usługi wymaga zainstalowania oprogramowania w systemach klienta (np. wtyczki przeglądarki), dostawca usługi w chmurze powinien w ramach dobrych praktyk poinformować klienta o tej okoliczności, a w szczególności o wynikających z tego implikacjach z punktu widzenia ochrony danych i bezpieczeństwa danych. Z drugiej strony, klient usługi w chmurze powinien podnieść tę kwestię *ex ante*, jeżeli dostawca usługi w chmurze nie zajął się nią w wystarczający sposób.

3.4.1.2 Określenie i ograniczenie celu

Zasada określenia i ograniczenia celu wymaga, aby dane osobowe były gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem (patrz artykuł 6 lit. (b) dyrektywy 95/46/WE). Klient usługi w chmurze musi określić cel/e przetwarzania przed zbieraniem danych osobowych od osoby, której dane dotyczą, oraz poinformować ją o tym. Klient usługi w chmurze nie może przetwarzać danych osobowych w innych celach niezgodnych z pierwotnymi celami.

Ponadto należy zapewnić, aby dane osobowe nie były (nielegalnie) przetwarzane w innych celach przez dostawcę usługi w chmurze lub jeden z podmiotów, którym podpowierzył

[17] Podobny obowiązek poinformowania osoby, której dane dotyczą, istnieje w przypadku uzyskiwania danych z innych źródeł niż osoba, której dane dotyczą, w przypadku ich gromadzenia lub ujawnienia stronie trzeciej (patrz artykuł 11).

[18] Tylko wtedy będzie mógł ocenić, czy dane osobowe mogą być przekazane do tzw. kraju trzeciego poza Europejskim Obszarem Gospodarczym (EOG), który nie zapewnia odpowiedniego poziomu ochrony w rozumieniu dyrektywy 95/46/WE. Patrz także punkt 3.4.6 poniżej.

realizację usługi w chmurze. W związku z tym, że typowy scenariusz usługi w chmurze może z łatwością obejmować dużą liczbę podmiotów, którym podpowierzono usługę, ryzyko przetwarzania danych osobowych w innych, niezgodnych z pierwotnymi celach musi być z tego względu ocenione jako dość wysokie. Na potrzeby zminimalizowania ryzyka umowa pomiędzy dostawcą a klientem usługi w chmurze musi zawierać środki techniczne i organizacyjne w celu zmniejszenia tego ryzyka i zapewnienia gwarancji rejestrowania (ang. logging) i kontroli istotnych operacji przetwarzania danych osobowych, które są dokonywane przez pracowników dostawcy usługi w chmurze lub przez podmioty, którym podpowierzono realizację usługi.[19] W umowie należy nałożyć sankcje na dostawcę lub podmiot, któremu podpowierzono realizację usługi, w przypadku naruszenia ustawodawstwa dotyczącego ochrony danych.

3.4.1.3 Usuwanie danych

Zgodnie z artykułem 6 lit. (e) dyrektywy 95/46/WE, dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane. Dane osobowe, które nie są już potrzebne, muszą być usunięte lub rzeczywiście zanonimizowane. Jeżeli danych tych nie można usunąć ze względu na prawne zasady przechowywania (np. regulacje podatkowe), dostęp do tych danych osobowych powinien być zablokowany. To klient usługi w chmurze jest zobowiązany do zapewnienia, aby dane osobowe zostały usunięte jak tylko nie będą już potrzebne do celów wskazanych powyżej[20].

Zasada usuwania danych dotyczy danych osobowych niezależnie od tego, czy są przechowywane na dyskach twardych czy na innych nośnikach danych (np. taśmy zapasowe). W związku z tym, że dane osobowe mogą być nadmiernie przechowywane na różnych serwerach w różnych lokalizacjach, należy zapewnić, aby w każdym przypadku były usunięte nieodwracalnie (tj. poprzednie wersje, pliki tymczasowe i nawet fragmenty pliku muszą być również usunięte).

Klienci usług w chmurze muszą być świadomi faktu, że dane zawarte w dzienniku (ang. „log data")[21], ułatwiające możliwość kontrolowania danych, tj. przechowywanie, modyfikowanie

[19] Patrz punkt 3.4.3 poniżej.
[20] Usunięcie danych jest istotną kwestią zarówno przez czas trwania umowy cloud computingu, jak i po jej zakończeniu. Jest również istotne w przypadku ustanowienia lub wycofania podmiotu, któremu podpowierzono usługę
[21] Uwagi nt. wymogów dotyczących rejestrowania ("logging") przedstawione są poniżej w punkcie 4.3.4.2.

lub usuwanie danych, mogą również być zaklasyfikowane jako dane osobowe dotyczące osoby, która zainicjowała określoną operację przetwarzania.[22]

Bezpieczne usuwanie danych osobowych wymaga, aby albo zostały zniszczone lub rozmagnetyzowane nośniki danych albo dane osobowe zostały skutecznie usunięte poprzez nadpisanie (ang. „overwriting"). Do nadpisywania danych osobowych należy wykorzystywać specjalne narzędzia programowe, które nadpisują dane kilkakrotnie zgodnie z uznaną specyfikacją.

Klient usługi w chmurze powinien zadbać o to, aby dostawca usługi w chmurze zapewnił bezpieczne usuwanie, jak wskazano powyżej, oraz aby umowa pomiędzy dostawcą a klientem zawierała wyraźne postanowienie dotyczące usuwania danych osobowych[23]. Dotyczy to również umów między dostawcami usług w chmurze a podmiotami, którym podpowierzono ich realizację.

3.4.2 Zabezpieczenia umowne relacji „administrator" – „przetwarzający"

W przypadku gdy administratorzy decydują się na powierzenie usług przetwarzania w chmurze, są zobowiązani do wybrania przetwarzającego zapewniającego wystarczające gwarancje pod względem technicznych środków bezpieczeństwa oraz środków organizacyjnych regulujących przetwarzanie, które ma być prowadzone, oraz musi zapewnić zgodność z tymi środkami (artykuł 17 ust. 2 dyrektywy 95/46/WE). Ponadto są prawnie zobowiązani do podpisania oficjalnej umowy z dostawcą usługi w chmurze, jak przewidziano w artykule 17 ust. 3 dyrektywy 95/46/WE. Artykuł ten ustanawia wymóg istnienia umowy lub innego wiążącego aktu prawnego regulującego relację między administratorem a przetwarzającym. W celach dowodowych części umowy lub aktu prawnego dotyczące ochrony danych i wymogów w zakresie środków technicznych i organizacyjnych powinny być sporządzone na piśmie lub w innej równoważnej formie.

Umowa musi co najmniej ustanowić fakt, w szczególności, że przetwarzający ma przestrzegać instrukcji administratora oraz że przetwarzający musi wdrożyć środki techniczne i organizacyjne, aby odpowiednio chronić dane osobowe.

W celu zapewnienia pewności prawnej umowa powinna przewidywać następujące kwestie:

[22] Oznacza to, że należy określić racjonalne okresy zatrzymywania dla plików dziennika (ang. „log files") oraz że muszą istnieć procedury zabezpieczające usuwanie lub anonimizację tych danych w określonym terminie.
[23] Patrz punkt 3.4.3 poniżej.

1. Szczegółowe informacje na temat (zakresu i rodzajów) instrukcji klienta powinny być zapewnione dostawcy, ze szczególnym odniesieniem do mających zastosowanie umów o gwarantowanym poziomie usług (ang. SLA) (które powinny być obiektywne i wymierne) oraz do właściwych sankcji (finansowych lub innych, obejmujących możliwość pozwania dostawcy w przypadku nie zapewnienia zgodności).
2. Określenie środków bezpieczeństwa, z którymi dostawca usługi w chmurze musi zapewnić zgodność, w zależności od zagrożeń związanych z przetwarzaniem i charakterem danych, które mają być chronione. Bardzo ważne jest, aby określić konkretne środki techniczne i organizacyjne, takie jak te wymienione w punkcie 3.4.3 poniżej. Jest to bez szkody dla zastosowania bardziej rygorystycznych środków, o ile takie istnieją, które mogą być przewidziane prawem krajowym klienta.
3. Przedmiot i ramy czasowe usługi w chmurze, która ma być świadczona przez dostawcę usługi w chmurze, zakres, sposób i cel przetwarzania danych osobowych przez dostawcę usługi w chmurze, jak również rodzaje przetwarzanych danych osobowych.
4. Określenie warunków zwrotu danych (osobowych) lub zniszczenia danych po zakończeniu realizacji usługi. Ponadto należy zapewnić, aby dane osobowe usunąć bezpiecznie na wniosek klienta usługi w chmurze.
5. Zawarcie klauzuli poufności, wiążącej zarówno dostawcę usługi w chmurze, jak i wszelkich jego pracowników, które mogą mieć możliwość dostępu do danych. Tylko upoważnione osoby mogą mieć dostęp danych.
6. Obowiązek po stronie dostawcy do wspierania klienta w ułatwianiu realizacji praw osoby, której dane dotyczą, do dostępu do swoich danych, ich poprawienia lub usunięcia.
7. Umowa powinna wyraźnie stanowić, że dostawca usługi w chmurze nie może przekazywać danych stronom trzecim, nawet w celach zatrzymania, chyba że umowa przewiduje zaangażowanie podmiotów, którym podpowierzona zostanie realizacja usługi. Umowa powinna określać, że podprzetwarzających można zaangażować tylko na podstawie zgody, której może generalnie udzielić administrator zgodnie z wyraźnym obowiązkiem nałożonym na przetwarzającego dotyczącym informowania administratora o wszelkich planowanych zmianach w tym zakresie, przy czym administrator zachowuje przez cały czas możliwość wyrażenia sprzeciwu wobec takich zmian lub do zakończenia umowy. Powinien istnieć wyraźny obowiązek, aby dostawca usługi w chmurze wskazał wszystkie podmioty, którym podpowierzono realizację usługi (np. w publicznym rejestrze

cyfrowym). Należy zapewnić, aby umowy między dostawcą usługi w chmurze a podmiotem, któremu podpowierzono jej realizację, odzwierciedlały postanowienia umowy między klientem chmury a dostawcą chmury (tj. podprzetwarzający podlegają takim samym obowiązkom umownym jak dostawca usługi w chmurze). W szczególności należy zagwarantować, że zarówno dostawca usługi w chmurze, jak i wszystkie podmioty, którym podpowierzono realizację, będą działać tylko na podstawie instrukcji pochodzących od klienta usługi w chmurze. Jak wyjaśniono w rozdziale dotyczącym powierzonego przetwarzania, łańcuch odpowiedzialności powinien być wyraźnie określony w umowie. Po stronie przetwarzającego należy ustanowić obowiązek regulowania transgranicznego przekazywania danych, na przykład poprzez podpisanie umów z podprzetwarzającymi, na podstawie standardowych klauzul umownych 2010/87/UE.

8. Wyjaśnienie zobowiązań dostawcy usługi w chmurze dotyczących zawiadamiania klienta usługi w chmurze w przypadku wszelkich naruszeń ochrony danych, które mają wpływ na dane klienta usługi w chmurze.
9. Obowiązek dostawcy usługi w chmurze dotyczący wskazania listy lokalizacji, w których dane mogą być przetwarzane.
10. Prawa administratora do monitorowania oraz odpowiadającemu temu zobowiązania dostawcy usługi w chmurze do współpracy.
11. Należy określić w umowie, że dostawca usługi w chmurze musi poinformować klienta o istotnych zmianach dotyczących określonej usługi w chmurze, takich jak wdrożenie dodatkowych funkcji.
12. Umowa powinna przewidywać rejestrowanie i kontrolowanie istotnych operacji przetwarzania danych osobowych, które są dokonywane przez dostawcę usługi w chmurze lub podmioty, którym podpowierzono ich realizację.
13. Zawiadamianie klienta usługi w chmurze o każdym prawnie wiążącym wniosku o udostępnienie danych osobowych przez organ egzekwowania prawa, o ile nie jest to zakazane w inny sposób, na przykład poprzez zakaz na mocy prawa karnego do zachowania poufności śledztwa dotyczącego egzekwowania prawa.
14. Podobny obowiązek po stronie dostawcy, aby zapewnił, że jego wewnętrzne ustalenia w zakresie organizacji i przetwarzania danych (oraz ustalenia jego podprzetwarzających, o

ile tacy są) będą zgodne z właściwymi krajowymi i międzynarodowymi wymogami prawnymi i standardami.

W przypadku naruszenia dokonanego przez administratora każda osoba doznająca szkody w wyniku nielegalnego przetwarzania ma prawo do otrzymania odszkodowania od administratora za wyrządzone szkody. Jeżeli przetwarzający będą wykorzystywali dane w innym celu bądź przekazywali lub wykorzystywali je w sposób naruszający umowę, będą również uznani za administratorów i będą pociągnięci do odpowiedzialności za naruszenia, w które byli osobiście zaangażowani.

Należy zauważyć, że w wielu przypadkach dostawcy usług w chmurze oferują standardowe usługi i umowy, które mają być podpisane przez administratorów, które przewidują standardową formę przetwarzania danych osobowych. Ten brak równowagi w uprawnieniach umownych małego administratora w odniesieniu do dużych dostawców usług nie może być uznany za usprawiedliwienie dla administratorów do przyjęcia klauzul i warunków umowy, które nie są zgodnie z prawem dotyczącym ochrony danych.

3.4.3 Środki techniczne i organizacyjne w zakresie ochrony danych i bezpieczeństwa danych

Artykuł 17 ust. 2 dyrektywy 95/46/WE nakłada na klientów usług w chmurze (działających jako administratorzy danych) pełną odpowiedzialność za wybranie dostawców usług w chmurze, którzy wdrożą odpowiednie techniczne i organizacyjne środki bezpieczeństwa w celu ochrony danych osobowych oraz w celu możliwości wykazania rozliczalności.

Poza kluczowymi celami w zakresie bezpieczeństwa, do których należą dostępność, poufność i integralność, należy również zwrócić uwagę na uzupełniające cele w zakresie ochrony danych, czyli przejrzystość (patrz punkt 3.4.1.1 powyżej), odizolowanie[24], możliwość interwencji, rozliczalność i możliwość przenoszenia. W tej części zwrócono uwagę na te główne cele w zakresie ochrony danych, bez szkody dla innej uzupełniającej analizy ryzyka ukierunkowanej na bezpieczeństwo[25].

3.4.3.1 Dostępność

[24] W Niemczech wprowadzono do ustawodawstwa szerszą koncepcję „niemożliwości łączenia" („unlinkability"), która jest propagowana przez Konferencję Rzeczników Ochrony Danych.

[25] Patrz np. ENISA na stronie http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloudcomputing-risk-assessment

Zapewnienie dostępności oznacza zapewnienie w odpowiednim czasie niezawodnego dostępu do danych osobowych.

Jednym z poważnym zagrożeń dla dostępności w chmurze jest przypadkowa utrata połączenia sieciowego między klientem a dostawcą lub przeciążeniem serwera spowodowanym szkodliwymi działaniami z sieci takimi jak (rozproszona) odmowa usługi (ataki DoS)[26]. Do innych zagrożeń dostępności należą przypadkowe uszkodzenia sprzętu, zarówno w sieci, jak i w systemach przetwarzania w chmurze i przechowywania danych, awaria zasilania oraz inne problemy z infrastrukturą.

Administratorzy danych powinni sprawdzić, czy dostawca usługi w chmurze przyjął racjonalne środki w celu zapewnienia ciągłości działania na wypadek zakłóceń, takie jak zapewnienie zapasowych łączy internetowych, nadmiarowe zasoby oraz skuteczne mechanizmy wykonywania kopii zapasowych danych.

3.4.3.2 Integralność

Integralność można określić jako fakt, że dane są prawdzie i nie zostały złośliwie lub przypadkowo zmienione podczas przetwarzania, przechowywania lub przekazywania. Pojęcie integralności można rozszerzyć na systemy informatyczne i wymagać, aby przetwarzanie danych osobowych w tych systemach pozostało niezmienione.

Zmiany danych osobowych można wykrywać przy wykorzystaniu mechanizmów uwierzytelniania kryptograficznego, takich jak kody czy podpisy służące do potwierdzenia niezmienności i źródła wiadomości.

Naruszeniu integralności systemów informatycznych w chmurze można zapobiec lub je wykryć przy pomocy systemów służących wykrywaniu / zapobieganiu włamaniom (IPS/IDS). Jest to szczególnie ważne w przypadku takich rodzajów otwartych środowisk sieciowych, w których zazwyczaj działają chmury.

3.4.3.3 Poufność

W środowisku cloud computingu szyfrowanie może znacznie przyczynić się do poufności danych osobowych, jeżeli będzie stosowane prawidłowo, choć nie anonimizuje danych nieodwracalnie[27]. Szyfrowanie danych osobowych powinno być stosowane we wszystkich

[26] Atak DoS to skoordynowana próba uniemożliwienia dostępności komputera lub zasobu sieciowego uprawnionym użytkownikom, czy to tymczasowo czy trwale (np. za pomocą dużej liczby atakujących systemów paraliżujących swój cel ogromną liczbą zewnętrznych żądań połączenia).

[27] Dyrektywa 95/46/WE – motyw 26: „(…)zasady ochrony danych nie mają zastosowania do danych, którym nadano anonimowy charakter w taki sposób, że podmiot danych nie będzie mógł być zidentyfikowany; (…)". W

przypadkach „w trakcie tranzytu” oraz w przypadku gdy jest dostępne dla danych nieaktywnych (ang. „data at rest”).[28] W niektórych przypadkach (np. usługa przechowywania IaaS) klient usługi w chmurze nie może polegać na rozwiązaniu szyfrowania oferowanym przez dostawcę usługi w chmurze, ale może zdecydować się na szyfrowanie danych osobowych przed wysłaniem ich do chmury. Szyfrowanie danych nieaktywnych („at rest”) wymaga zwrócenia szczególnej uwagi na zarządzanie kluczem kryptograficznym, ponieważ bezpieczeństwo danych zależy wówczas ostatecznie od poufności kluczy szyfrujących.

Komunikacja pomiędzy dostawcą usługi w chmurze i jej klientem oraz między ośrodkami danych powinna być zaszyfrowana. Zdalne zarządzanie platformą usługi w chmurze powinno odbywać się tylko za pośrednictwem bezpiecznego kanału komunikacyjnego. Jeżeli klient planuje nie tylko przechowywanie, ale również dalsze przetwarzanie danych osobowych w chmurze (np. wyszukiwanie wpisów w bazach danych), musi pamiętać, że szyfrowanie nie może być utrzymane podczas przetwarzania danych (z wyjątkiem konkretnych obliczeń).

Dalsze środki techniczne mające na celu zapewnienie poufności to mechanizmy autoryzacji oraz solidne uwierzytelnianie (np. uwierzytelnianie dwuelementowe). Klauzule umowne powinny również nakładać obowiązki w zakresie zapewnienia poufności na pracowników klientów usługi w chmurze, dostawców tej usługi oraz podmioty, którym podpowierzono jej realizację.

3.4.3.4 Przejrzystość

Środki techniczne i organizacyjne muszą wspierać przejrzystość, aby umożliwić przegląd, patrz 3.4.1.1.

3.4.3.5 Odizolowanie (ograniczenie celu)

W infrastrukturach cloud computingu zasoby, takie jak przestrzeń dyskowa, pamięć i sieci, są współdzielone przez wielu wynajmujących. Stwarza to nowe zagrożenia, że dane będą udostępniane i przetwarzanie do nielegalnych celów. „Odizolowanie”, jako cel mający zapewnić ochronę, ma być odpowiedzią na ten problem i ma przyczynić się do

tym samy sensie, techniczne procesy fragmentacji danych, które mogą być stosowane przy świadczeniu usług cloud computingu, nie doprowadzą do nieodwracalnej anonimizacji i w związku z tym nie pociągają za sobą faktu, że obowiązki w zakresie ochrony danych nie mają zastosowania.

[28] Jest to właściwe szczególnie dla administratorów danych, którzy planują przekazanie danych szczególnie chronionych w rozumieniu artykułu 8 dyrektywy 95/46/WE (np. danych dotyczących zdrowia) do chmury lub którzy podlegają szczególnych zobowiązaniom prawnym w zakresie tajemnicy zawodowej.

zagwarantowania, że dane nie będą wykorzystywane w celu innym niż cel pierwotny (artykuł 6 lit. (b) dyrektywy 95/46/WE), oraz do zachowania poufności i integralności.[29]

Osiągnięcie „odizolowania" wymaga po pierwsze odpowiedniego zarządzania prawami i rolami dotyczącymi dostępu do danych osobowych, co podlega systematycznemu przeglądowi. Należy unikać wprowadzania ról z nadmiernymi przywilejami (np. żaden użytkownik ani administrator nie powinien być upoważniony do dostępu do całej chmury). Bardziej ogólnie, administratorzy i użytkownicy mogą jedynie mieć możliwość dostępu do informacji, które są niezbędne do ich prawnie uzasadnionych celów (zasada jak najmniejszych przywilejów).

Po drugie, odizolowanie zależy również od środków technicznych, takich jak wzmocnienie hipernadzorców (ang. „hypervisors") oraz odpowiednie zarządzanie współdzielonymi zasobami, jeżeli maszyny wirtualne są wykorzystywane w celu współdzielenia zasobów fizycznych przez różnych klientów usługi w chmurze.

3.4.3.5 Możliwość interwencji

Dyrektywa 95/46/WE daje osobie, której dane dotyczą, prawa dostępu do danych, ich poprawienia, usunięcia, zablokowania lub wyrażenia sprzeciwu (patrz artykuł 12 i 14). Klient usługi w chmurze musi sprawdzić, czy dostawca usługi w chmurze nie stawia przeszkód technicznych i organizacyjnych w realizacji tych wymogów, w tym w przypadkach, gdy dane są dalej przetwarzane przez podmioty, którym podpowierzono realizację usługi.

Umowa między klientem i dostawcą powinna stanowić, że dostawca usługi w chmurze jest zobowiązany do wspierania klienta w ułatwianiu realizacji praw osoby, której dane dotyczą, oraz do zapewnienia, że to samo dotyczy jego relacji z każdym podmiotem, któremu podpowierzono realizację usługi.[30]

3.4.3.6 Możliwość przenoszenia danych

Obecnie większość dostawców usług w chmurze nie wykorzystuje standardowych formatów danych i interfejsów usługi ułatwiających interoperacyjność i możliwość przenoszenia danych między różnymi dostawcami usług w chmurze. Jeżeli klient usługi w chmurze zdecyduje się na przeniesienie się od jednego dostawcy usługi w chmurze do innego, ten brak interoperacyjności może doprowadzić do braku możliwości czy co najmniej trudności w

[29] Patrz 3.4.1.2.
[30] Patrz punkt 3.4.5 nr 7 powyżej. Dostawcę można nawet poinstruować, aby odpowiadał na wnioski w imieniu klienta.

przekazaniu danych (osobowych) klienta do nowego dostawcy usługi w chmurze (tzw. „vendor lock-in", czyli uzależnienie od dostawcy). To samo dotyczy usług, które klient rozwinął na platformie oferowanej przez pierwotnego dostawcę usługi w chmurze (PaaS). Klient usługi w chmurze powinien sprawdzić, czy i w jaki sposób dostawca gwarantuje możliwość przenoszenia danych i usług przed zamówieniem usługi w chmurze.[31]

3.4.3.7 Rozliczalność

W informatyce rozliczalność można zdefiniować jako możliwość ustalenia, co podmiot robił w określonym momencie w przeszłości i w jaki sposób. W dziedzinie ochrony danych termin ten często przyjmuje szersze znaczenie i opisuje możliwość pokazania przez strony, że podjęły odpowiednie kroki w celu zapewnienia, że zasady ochrony danych zostaną wdrożone.

Rozliczalność informatyczna jest szczególnie ważna w celu badania naruszeń ochrony danych osobowych, gdy każdy z podmiotów – tj. klienci usług w chmurze, ich dostawcy i podprzetwarzający - może ponosić jakiś procent odpowiedzialności operacyjnej. Możliwość zapewniania przez platformę cloud computingu wiarygodnego monitoringu i kompleksowych mechanizmów rejestrowania (ang. „logging") ma w tym względzie pierwszorzędne znaczenie.

Ponadto dostawcy usług w chmurze powinni przedstawić dokumentację dowodową potwierdzającą odpowiednie i skuteczne środki, które dostarczają wyniki stosowania zasad ochrony danych wskazane w poprzednich częściach. Przykładami takich środków są procedury mające na celu zapewnienie identyfikacji wszystkich operacji przetwarzania danych, odpowiedzenie na wnioski o dostęp, przydzielenie zasobów, w tym wyznaczenie pełnomocników ds. ochrony danych, którzy są odpowiedzialni za organizację zapewnienia zgodności z zasadami ochrony danych, lub niezależne procedury certyfikacji. Dodatkowo administratorzy danych powinni zapewnić, że są przygotowani do wykazania wprowadzenia niezbędnych środków na wniosek właściwego organu nadzorczego.[32]

3.5 Przekazywanie transgraniczne

Artykuł 25 i 26 Dyrektywy 95/46/WE przewidują swobodny przepływ danych poza EOG tylko, jeżeli kraj lub odbiorca zapewni odpowiedni poziom ochrony danych. W przeciwnym razie administrator i jego współ-administratorzy i/lub przetwarzający muszą wprowadzić

[31] Najlepiej by było, aby dostawca wykorzystywał standardowe lub otwarte formaty danych i interfejsy. W każdym przypadku należy uzgodnić klauzule umowne przewidujące zapewnione formaty, utrzymanie logicznych relacji oraz koszty wynikające z przeniesienia się do innego dostawcy usługi w chmurze.
[32] Grupa Robocza przedstawiła szczegółowe uwagi na temat rozliczalności w Opinii 3/2010 w sprawie zasady rozliczalności http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_pl.pdf.

szczególne zabezpieczenia. Jednak cloud computing najczęściej jest oparty na całkowitym braku stałej lokalizacji danych w ramach sieci dostawcy usługi w chmurze. Dane mogą się znajdować w jednym ośrodku o godzinie 14.00, a w innej części świata o godzinie 16.00. Zatem dostawca usługi w chmurze rzadko ma możliwość wiedzieć w czasie rzeczywistym, gdzie są zlokalizowane lub przechowywane lub przekazywane dane. W tym kontekście tradycyjne instrumenty prawne zapewniające ramy regulujące przekazywanie danych do krajów trzecich spoza UE niezapewniających odpowiedniej ochrony mają ograniczenia.

3.5.1 Safe Harbor (program tzw. bezpiecznej przystani) i kraje zapewniające odpowiedni poziom ochrony

Ustalenia odpowiedniego poziomu ochrony (adekwatności), w tym Safe Harbor, są ograniczone pod względem geograficznym, i w związku z tym nie obejmują wszystkich przypadków przekazywania w ramach chmury.

Przekazywanie do organizacji z USA przestrzegających zasad może mieć odbywać się legalnie na mocy prawa UE, ponieważ organizacje będące odbiorcami są uznawane za zapewniające odpowiedni poziom ochrony dla przekazanych danych.

Jednakże zdaniem Grupy Roboczej jedynie samo-certyfikacja w ramach Safe Harbor nie może być uznana za wystarczającą przy braku solidnego wdrożenia zasad ochrony danych w środowisku cloud computingu. Ponadto artykuł 17 Dyrektywy UE wymaga, aby umowę podpisał administrator, aż po przetwarzającego, do celów przetwarzania, co potwierdzono w pytaniu FAQ 10 dokumentów ramowych w sprawie Safe Harbor UE-USA. Umowa ta nie podlega wcześniejszej autoryzacji przez europejskie organy ochrony danych. Umowa taka określa przetwarzanie, które ma być prowadzone, oraz wszelkie środki niezbędne do zapewnienia, że dane będą przechowywane bezpiecznie. Różne ustawodawstwa krajowe oraz organy ochrony danych mogą mieć dodatkowe wymogi.

Grupa Robocza uważa, że przedsiębiorstwa przekazujące dane nie powinny jedynie polegać na oświadczeniu przedsiębiorstwa, któremu przekazywane są dane, w którym twierdzi ono, że posiada certyfikat Safe Harbor. Przeciwnie przedsiębiorstwo przekazujące dane powinno uzyskać dowody, że samo-certyfikacja Safe Harbor istnieje, i zwrócić się o dowody pokazujące, że jego zasady są przestrzegane. Jest to szczególnie ważne w odniesieniu do informacji zapewnianych osobom, których dane dotyczą, do których odnosi się przetwarzanie danych[33] [34].

[33] Patrz niemiecki organ ochrony danych: : http://www.datenschutzberlin.

Grupa Robocza uważa również, że klient usługi w chmurze musi sprawdzić, czy standardowe umowy sporządzane przez dostawców usług w chmurze są zgodne z krajowymi wymogami dotyczącymi przetwarzania danych w ramach umowy. Krajowe ustawodawstwo może wymagać, aby w umowie zdefiniować podpowierzone przetwarzanie, które obejmuje lokalizacje i inne dane podprzetwarzających, oraz możliwość śledzenia lokalizacji danych (ang. „traceability"). Normalnie dostawcy usług w chmurze nie oferują klientowi takich informacji – ich zobowiązanie się do przestrzegania zasad Safe Harbor nie może zastąpić braku powyższych gwarancji, gdy wymaga tego ustawodawstwo krajowe. W takich przypadkach podmiot przekazujący jest zachęcany do stosowania innych dostępnych instrumentów, takich jak standardowe klauzule umowne lub wiążące reguły korporacyjne.

I wreszcie, Grupa Robocza uważa, że same zasady Safe Harbor także nie mogą zagwarantować podmiotowi przekazującemu dane niezbędnych środków do zapewnienia, że odpowiednie środki bezpieczeństwa będą zastosowane przez dostawcę usługi w chmurze w USA, czego mogą wymagać przepisy krajowe w oparciu o dyrektywę 95/46/WE[35]. Pod względem bezpieczeństwa danych cloud computing niesie ze sobą kilka zagrożeń bezpieczeństwa typowych dla przetwarzania danych w chmurze, takich jak utrata zarządzania, niezabezpieczone lub niekompletne usuwanie danych, niewystarczające dzienniki kontroli lub brak odizolowania[36], których nie regulują w wystarczającym stopniu istniejące zasady Safe Harbor dotyczące bezpieczeństwa danych[37]. Zatem należy zastosować dodatkowe zabezpieczenia służące bezpieczeństwu danych; np. uwzględniając wiedzę specjalistyczną i zasoby stron trzecich, które są w stanie ocenić adekwatność (odpowiedni poziom ochrony) dostawców usługi w chmurze przy wykorzystaniu różnych programów kontroli, standaryzacji i certyfikacji[38]. Z tych względów może wskazane byłoby uzupełnienie zobowiązania podmiotu, do którego przekazywane są dane, do przestrzegania zasad Safe Harbor o dodatkowe zabezpieczenia przy uwzględnieniu szczególnego charakteru chmury.

3.5.2 Wyłączenia

---

de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

[34] Wymogi dotyczące powierzania podmiotom podprzetwarzającym – patrz punkt 3.3.2.

[35] Patrz opinia duńskiego organu ochrony danych: http://www.datatilsynet.dk/english/processing-of-sensitive-personaldata-in-a-cloud-solution.

[36] Opisane w dokumencie ENISA „Cloud Computing; Korzyści, zagrożenia i zalecenia dla społeczeństwa informacyjnego, dostępnego na stronie: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloudcomputing-risk-assessment.

[37] „Organizacje muszą podjąć racjonalne środki ostrożności w celu ochrony danych osobowych przed utratą, niewłaściwym wykorzystaniem i nieuprawnionym dostępem, udostępnieniem, zmianą i zniszczeniem."

[38] Patrz punkt 4.2 poniżej.

Wyłączenia przewidziane w artykule 26 Dyrektywy UE 95/46 pozwalają podmiotom przekazującym dane na przekazywanie danych z UE bez zapewnienia dodatkowych gwarancji. Jednak GR Art. 29 przyjęła opinię, w której uznała, że wyłączenia powinny mieć zastosowanie tylko wówczas, gdy operacje przekazywania nie są powtarzalne, masowe ani strukturalne.[39]

W oparciu o takie interpretacje niemal niemożliwe jest poleganie na wyłączeniach w kontekście cloud computingu.

3.5.3 Standardowe klauzule umowne

Standardowe klauzule umowne, przyjęte przez Komisję Europejską w celu uregulowania transgranicznego przekazywania danych między dwoma administratorami lub jednym administratorem i przetwarzającym, oparte są na podejściu bilateralnym. Gdy dostawca usługi w chmurze jest uznawany za przetwarzającego, wzorcowe klauzule 2010/87/WE stanowią instrument, który może być wykorzystany pomiędzy przetwarzającym i administratorem jako podstawa do tego, aby środowisko cloud computingu oferowało odpowiednie zabezpieczenia w kontekście transgranicznego przekazywania.

Grupa Robocza uważa, że poza standardowymi klauzulami umownymi dostawcy usług w chmurze mogliby dodatkowo oferować klientom postanowienia, które oparte są na ich pragmatycznym doświadczeniu, o ile nie pozostają one w sprzeczności, pośrednio lub bezpośrednio, ze standardowymi klauzulami umownymi zatwierdzonymi przez Komisję, ani nie szkodzą podstawowym prawom lub wolnościom osób, których dane dotyczą[40]. Niemniej przedsiębiorstwa nie mogą nowelizować ani zmieniać standardowych klauzul umownych bez wskazania, że klauzule nie będą już „standardowymi" klauzulami[41].

Gdy dostawca usługi w chmurze działający jako przetwarzający ma siedzibę w UE, sytuacja może być bardziej złożona, ponieważ klauzule wzorcowe, generalnie, mają zastosowanie tylko do przekazywania danych od administratora w UE do przetwarzającego poza UE (patrz motyw 23 decyzji Komisji w sprawie wzorcowych klauzul 2010/87/UE oraz dokument WP 176).

---

[39] Dokument roboczy 12/1998: Przekazywanie danych osobowych do krajów trzecich: Zastosowanie artykułów 25 i 26 dyrektywy UE o ochronie danych, przyjęty przez Grupę Roboczą 24 lipca 1998 r. (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf).

[40] Patrz pyt. FAQ B1.9 9, Czy przedsiębiorstwa mogą zawrzeć standardowe klauzule umowne w obszerniejszej umowie i dodać określone klauzule? Opublikowane na stronie http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[41] Patrz pyt. FAQ B1.10, Czy przedsiębiorstwa mogą nowelizować lub zmieniać standardowe klauzule umowne zatwierdzone przez Komisję Europejską?

Jeżeli chodzi o stosunek umowny między przetwarzającym w UE oraz podprzetwarzającymi, powinna zostać zawarta pisemna umowa, która nakłada takie same obowiązki na podprzetwarzającego jak te nałożone na przetwarzającego w klauzulach wzorcowych.

3.5.4 Wiążące reguły korporacyjne (BCR): w kierunku globalnego podejścia

Wiążące reguły korporacyjne stanowią kodeks postępowania dla przedsiębiorstw, które przekazują dane w ramach swojej grupy. Takie rozwiązanie będzie zapewnione także w kontekście przetwarzania danych w chmurze, gdy dostawca jest przetwarzającym. W rzeczywistości GR Art. 29 pracuje obecnie nad wiążącymi regułami korporacyjnymi dla przetwarzających, które pozwolą na przekazywanie w ramach grupy na korzyść administratorów bez wymogu podpisywania umów między przetwarzającym i podprzetwarzającymi dla danego klienta.[42]

Takie BCR dla przetwarzających pozwolą klientowi dostawcy na powierzenie swoich danych osobowych przetwarzającemu przy zapewnieniu, że dane przekazywane w ramach działalności dostawcy otrzymają odpowiedni poziom ochrony.

4. Wnioski i zalecenia

Przedsiębiorstwa i organy administracji, które chcą skorzystać z usług przetwarzania danych w chmurze, powinny w pierwszej kolejności przeprowadzić szczegółową i dokładną analizę zagrożeń. Analiza musi dotyczyć zagrożeń związanych z przetwarzaniem danych w chmurze (brak kontroli lub niewystarczające informacje – patrz punkt 2 powyżej), zważając na rodzaj danych przetwarzanych w chmurze.[43] Szczególną uwagę należy również zwrócić na oszacowanie zagrożeń prawnych związanych z ochroną danych, które dotyczą głównie obowiązków w zakresie bezpieczeństwa oraz dodatkowych zabezpieczeń.[44] Przedstawione poniżej wnioski mają na celu dostarczenie listy kontrolnej służącej weryfikacji zapewniania zgodności z zasadami ochrony danych przez klientów usług w chmurze i ich dostawców w oparciu o istniejące ramy prawne; niektóre zalecenia są przedstawione również z myślą o przyszłych wydarzeniach dotyczących ram prawnych na poziomie UE i poza nią.

[42] Patrz dokument roboczy 02/2012 ustanawiający tabelę zawierającą elementy i zasady, które muszą znaleźć się w wiążących regułach korporacyjnych dla przetwarzających, przyjęty 6 czerwca 2012 r.: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

[43] ENISA przedstawia listę zagrożeń, które muszą być wzięte pod uwagę http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

4.1 Wytyczne dla klientów i dostawców usług przetwarzania danych w chmurze

- Relacja administrator-przetwarzający: Niniejsza opinia koncentruje się na relacji klient-dostawca jako relacji administrator-przetwarzający; (patrz punkt 3.3.1); Niemniej konkretne okoliczności wskazują, że mogą istnieć sytuacje, gdy dostawca usługi w chmurze również działa jako administrator, np. gdy dostawca ponownie przetwarza dane osobowe do własnych celów. W takim przypadku dostawca usługi w chmurze ponosi pełną (wspólną) odpowiedzialność za przetwarzanie i musi spełnić zobowiązania prawne określone w dyrektywach 95/46/WE oraz 2002/58WE (gdy to właściwe);
- Odpowiedzialność klienta usługi w chmurze jako administratora: Klient jako administrator musi przyjąć odpowiedzialność za przestrzeganie przepisów w zakresie ochrony danych i podlega wszystkim zobowiązaniom prawnym wskazanym w dyrektywie 95/46/WE i 2002/58/WE, gdy to właściwe, w szczególności względem osób, których dane dotyczą (patrz 3.3.1). Klient powinien wybrać dostawcę usługi w chmurze, który gwarantuje zgodność z przepisami w zakresie ochrony danych, co odzwierciedlają odpowiednie zabezpieczenia umowne podsumowane poniżej;
- Zabezpieczenia w przypadku powierzenia: Przepisy dla podmiotów, którym podpowierzono realizację usług, powinny być przewidziane w każdej umowie miedzy dostawcą usługi w chmurze i jej klientami. Umowa powinna określać, że podprzetwarzającym można powierzyć realizację usług tylko na podstawie zgody, która generalnie może być udzielona przez administratora zgodnie z wyraźnym obowiązkiem przetwarzającego do informowania administratora o wszelkich planowanych zmianach w tym względzie, przy czym administrator przez cały czas zachowuje możliwość wyrażenia sprzeciwu wobec takich zmian lub rozwiązania umowy. Powinien istnieć wyraźny obowiązek w przypadku dostawcy usługi w chmurze do wskazania wszystkich podmiotów, którym podpowierzono usługi. Dostawca usługi w chmurze powinien podpisać umowę z każdym takim podmiotem, odzwierciedlającą postanowienia swojej umowy z klientem usługi w chmurze; klient powinien zadbać o to, że będzie miał umowne możliwości dochodzenia roszczeń w przypadku naruszeń umowy przez podmioty, którym dostawca podpowierzył usługi (patrz 3.3.2);

[44] Patrz Memorandum z Sopotu, patrz przypis 2 powyżej.

- Przestrzeganie podstawowych zasad ochrony danych:

  - Przejrzystość (patrz 3.4.1.1): dostawcy usług w chmurze powinni informować klientów tych usług o wszystkich istotnych aspektach (dotyczących ochrony danych) odnoszących się do ich usług podczas negocjacji umowy; w szczególności klientów należy poinformować o wszystkich podmiotach, którym podpowierzono realizację usługi i którzy przyczyniają się do świadczenia określonej usługi w chmurze, oraz o wszystkich lokalizacjach, w których dane mogą być przechowywane lub przetwarzane przez dostawcę usługi w chmurze i/lub podmioty, którym podpowierzył usługi (szczególnie gdy niektóre lub wszystkie lokalizacje znajdują się poza Europejskim Obszarem Gospodarczym (EOG)); klientowi należy zapewnić zrozumiałe informacje na temat środków technicznych i organizacyjnych wdrożonych przez dostawcę; klient w ramach dobrych praktyk powinien przekazać osobom, których dane dotyczą, informacje na temat dostawcy usługi w chmurze i wszystkich podmiotów, którym podpowierzył jej realizację (o ile takie podmioty istnieją), jak również na temat lokalizacji, w których dane mogą być przechowywane lub przetwarzane przez dostawcę usługi i/lub podmiotów, którym podpowierzył realizację usług;

  - Określenie i ograniczenie celu (3.4.1.2): klient powinien zapewnić zgodność z zasadami określenia i ograniczenia celu oraz zadbać o to, aby żadne dane nie były przetwarzane do innych celów przez dostawcę ani którykolwiek z podmiotów, którym podpowierzył realizację usługi. Zobowiązania w tym zakresie powinny zostać ujęte w odpowiednich środkach umownych (w tym zabezpieczenia techniczne i organizacyjne);

  - Zatrzymywanie danych (3.4.1.3): klient jest odpowiedzialny za zapewnienie, aby dane osobowe zostały usunięte (przez dostawcę i wszystkie podmioty, którym podpowierzył usługi) ze wszystkich miejsc, w których są przechowywane, jak tylko nie będą już niezbędne do określonych celów; w umowie powinny być przewidziane bezpieczne mechanizmy usuwania (zniszczenie, rozmagnetyzowanie, nadpisanie);

- Zabezpieczenia umowne (patrz 3.4.2, 3.4.3 i 3.5);

  - Ogólnie: umowa z dostawcą (oraz umowy, które mają być ustanowione między dostawcą i podmiotami, którym podpowierzono realizację usług) powinna

zapewniać wystarczające gwarancje pod względem technicznych środków bezpieczeństwa i środków organizacyjnych (na mocy art. 17 ust. 2 dyrektywy) oraz powinna być sporządzona na piśmie lub w innej równoważnej formie. Umowa powinna przedstawiać instrukcje/wskazówki klienta dla dostawcy, w tym przedmiot i ramy czasowe usługi, cel i wymierne poziomy usługi oraz właściwe sankcje (finansowe lub inne); powinna określać środki bezpieczeństwa, które należy zapewnić stosownie do zagrożeń przetwarzania, oraz charakteru danych, zgodnie z wymogami wskazanymi poniżej oraz z bardziej rygorystycznymi środkami przewidzianymi w prawie krajowym klienta; gdy dostawcy usług w chmurze dążą do wykorzystania standardowych warunków umownych, powinni zapewnić, że warunki te będą zgodne z wymogami w zakresie ochrony danych (patrz 3.4.2); w szczególności w konkretnych warunkach należy określić środki techniczne i organizacyjne wprowadzone przez dostawcę;

- Dostęp do danych: tylko upoważnione osoby powinny mieć dostęp do danych; w umowie powinna być zawarta klauzula poufności w odniesieniu do dostawcy i jego pracowników;
- Udostępnianie danych stronom trzecim: powinno być ono uregulowane umową, która powinna zawierać obowiązek po stronie dostawcy do wskazania wszystkich podmiotów, którym podpowierzył realizację usługi – np. w publicznym rejestrze cyfrowym – oraz do zapewnienia klientowi dostępu do informacji o wszelkich zmianach w celu umożliwienia mu wyrażenia sprzeciwu wobec tych zmian lub do rozwiązania umowy; umowa powinna również wymagać od dostawcy zgłaszania wszelkich prawnie wiążących wniosków o udostępnienie danych osobowych przez organ egzekwowania prawa, o ile takie udostępnienie nie jest zakazane w inny sposób; klient powinien zagwarantować, że dostawca odrzuci wszelkie wnioski o udostępnienie niewiążące prawnie;
- Zobowiązania do współpracy: klient powinien zapewnić, aby dostawca był zobowiązany do współpracy w związku z prawem klienta do monitorowania operacji przetwarzania, do ułatwiania realizacji praw osób, których dane dotyczą, do dostępu do/poprawiania/usuwania ich danych, oraz (gdy to właściwe) do powiadamiania klienta usługi w chmurze o wszelkich naruszeń ochrony danych mających wpływ na dane klienta;

- Transgraniczne przekazywanie danych: Klient usługi w chmurze powinien sprawdzić, czy dostawca usługi w chmurze może zagwarantować legalność transgranicznego przekazywania danych oraz ograniczyć przypadki przekazywania do krajów wybranych przez klienta, gdy to możliwe. Przekazywanie danych do krajów trzecich niezapewniających odpowiedniego poziomu ochrony wymaga szczególnych zabezpieczeń przy wykorzystaniu odpowiednio zobowiązań umownych Safe Harbor, standardowych klauzul umownych (SCC) lub wiążących reguł korporacyjnych (BCR); wykorzystanie SCC dla przetwarzających (na mocy decyzji Komisji 2010/87/WE) wymaga pewnych dostosowań do środowiska cloud computingu (aby zapobiec temu, że będą istniały odrębne umowy dla danego klienta między dostawcą i podmiotami, którym podpowierzył usługi), co może oznaczać potrzebę wcześniejszej autoryzacji przez właściwy organ ochrony danych; lista lokalizacji, w których może być świadczona usługa powinna być zawarta w umowie;
- Rejestrowanie (ang. „logging") i kontrolowanie przetwarzania: klient powinien wymagać rejestrowania operacji przetwarzania dokonywanych przez dostawcę lub podmioty, którym podpowierzył realizację usług; klient powinien być uprawniony do kontroli (audytu) takich operacji przetwarzania, jednak kontrole dokonywane przez strony trzecie wybrane przez administratora oraz certyfikacja również mogą być dopuszczalne, pod warunkiem że zagwarantowana jest pełna przejrzystość (np. poprzez zapewnienie możliwości uzyskania kopii certyfikatu potwierdzającego kontrolę dokonaną przez stronę trzecią lub kopii sprawozdania z kontroli weryfikującej certyfikację);
- Środki techniczne i organizacyjne: powinny mieć na celu eliminację lub złagodzenie zagrożeń wynikających z braku kontroli i braku informacji, które najczęściej charakteryzują środowisko cloud computingu. Chodzi tu o środki mające na celu zapewnienie dostępności, integralności, poufności, odizolowania, możliwości interwencji i przenoszenia danych, jak określono w dokumencie, podczas gdy środki skupiają się na przejrzystości (patrz 3.4.3 – szczegółowe informacje).

4.2 Certyfikacja w zakresie ochrony danych zapewniana przez strony trzecie

- Niezależna weryfikacja i certyfikacja przez renomowaną stronę trzecią może być dla dostawców usług w chmurze wiarygodnym sposobem wykazania, że przestrzegają zobowiązań określonych w niniejszej Opinii. Taka certyfikacja wskazywałaby co najmniej, że kontrole w zakresie ochrony danych zostały poddane audytowi lub przeglądowi zgodnie z uznanym standardem spełniającym wymogi określone w tej Opinii dokonanemu przez renomowaną organizację będącą stroną trzecią.[45] W kontekście cloud computingu potencjalni klienci powinni sprawdzić, czy dostawcy usług w chmurze mogą zapewnić kopie takiego certyfikatu potwierdzającego kontrolę dokonaną przez stronę trzecią lub faktycznie kopię sprawozdania z kontroli weryfikującej certyfikację, w tym w odniesieniu do wymogów określonych w tej Opinii.

- Niezależne kontrole danych utrzymywanych (hosting) na wirtualnych serwerach przeznaczonych dla wielu stron mogą być niepraktyczne pod względem technicznym i mogą w niektórych przypadkach prowadzić do zwiększenia zagrożeń dla istniejących kontroli bezpieczeństwa fizycznego i logicznego sieci. W takich przypadkach określona kontrola wykonywana przez stronę trzecią wybrana przez administratora może być uznana za wystarczającą realizację prawa danego administratora do kontroli.

- Przyjęcie standardów i certyfikacji typowych dla ochrony prywatności jest szczególnie istotne dla ustanowienia wiarygodnej relacji między dostawcami usług w chmurze, administratorami i osobami, których dane dotyczą.

- Te standardy i certyfikacje powinny dotyczyć środków technicznych (takich jak lokalizacja danych lub szyfrowanie) oraz procesów w środowisku dostawców usług w chmurze, które gwarantują ochronę danych (takich jak polityki kontroli dostępu, kontrola dostępu lub kopie zapasowe).

4.3 Zalecenia: Przyszłe wydarzenia

GR jest w pełni świadoma faktu, że cloud computing jest zagadnieniem złożonym i nie można odnieść się do niego całkowicie przedstawiając zabezpieczenia i rozwiązania przedstawione w zarysie w niniejszej Opinii, która zapewnia jednak solidną podstawę do

[45] Takie standardy obejmowałyby standardy wydane przez Międzynarodową Organizację Normalizacyjną (ISO), Międzynarodową Radę Standardów Rewizji Finansowej i Usług Atestacyjnych oraz Radę ds. Standardów Audytu Amerykańskiego Instytutu Biegłych Rewidentów, pod warunkiem że te organizacje zapewniają standardy, które spełniają wymogi określone w tej opinii.

zabezpieczenia przetwarzania danych osobowych, które klienci w EOG przekazują dostawcom usług w chmurze. Celem tej części jest zwrócenie uwagi na niektóre kwestie, którymi należy się zająć krótkoterminowo lub średnioterminowo w zmaganiach nad zwiększeniem poziomu stosowanych zabezpieczeń, pomagając branży cloud computingu w zakresie wskazanych kwestii, przy zapewnieniu poszanowania podstawowych praw do ochrony danych i prywatności.

- Lepsze wyważenie odpowiedzialności pomiędzy administratorem i przetwarzającym: GR z zadowoleniem przyjmuje przepisy zawarte w artykule 26 wniosku Komisji (projekt Ogólnego Rozporządzenia o Ochronie Danych UE), których celem jest zwiększenie odpowiedzialności przetwarzających względem administratorów poprzez zapewnienie im pomocy w przestrzeganiu szczególnie zobowiązań w zakresie bezpieczeństwa i powiązanych z nimi zobowiązań. Artykuł 30 wniosku wprowadza prawny obowiązek dla przetwarzającego w zakresie wprowadzenia odpowiednich środków technicznych i organizacyjnych. Projekty wniosków wyjaśniają, że przetwarzający nieprzestrzegający instrukcji administratora uznawany jest za administratora i podlega szczególnym przepisom dotyczącym sprawowania wspólnej kontroli. Grupa Robocza Artykułu 29 uważa, że wniosek ten zmierza w dobrym kierunku na rzecz zaradzenia brakowi równowagi, który często cechuje środowisko cloud computingu, gdzie klient (szczególnie jeśli jest to małe lub średnie przedsiębiorstwo) może mieć trudności ze sprawowaniem pełnej kontroli wymaganej przez ustawodawstwo w zakresie ochrony danych nad sposobem świadczenia żądanych usług przez dostawcę. Ponadto z uwagi na asymetryczną sytuację prawną osób, których dane dotyczą, oraz użytkowników będących małymi przedsiębiorstwami względem dużych dostawców cloud computingu, zalecana jest bardziej proaktywna rola dla organizacji służących ochronie interesów konsumentów i przedsiębiorstw w celu wynegocjowania bardziej zrównoważonych warunków ogólnych takich przedsiębiorstw.
- Dostęp do danych osobowych ze względu na bezpieczeństwo państwa i w celach egzekwowania prawa: Jest sprawą najwyższej wagi dodanie do przyszłego Rozporządzenia zakazu dla administratorów działających w UE udostępniania danych osobowych krajowi trzeciemu, jeżeli wymaga tego organ sądowy lub administracyjny kraju trzeciego, chyba że wyraźnie zezwala na to umowa międzynarodowa lub przewidziane jest to w traktatach o wzajemnej pomocy prawnej bądź zatwierdzone przez organ nadzorczy. Rozporządzenie

Rady (WE) Nr 2271/96 jest odpowiednim przykładem podstawy prawnej do tego.[46] Grupę Roboczą martwi ta luka we wniosku Komisji, ponieważ niesie ze sobą znaczną utratę pewności prawnej dla osób, których dane są przechowywane w ośrodkach danych na całym świecie. Z tego względu Grupa Robocza chciałaby podkreślić[47] potrzebę zawarcia w Rozporządzeniu obligatoryjnego stosowania Traktatów o Wzajemnej Pomocy Prawnej (tzw. MLAT) w przypadku udostępnień nieautoryzowanych przez prawo Unii ani Państw Członkowskich.

- Szczególne środki ostrożności podejmowane przez sektor publiczny: Należy dodać specjalne zastrzeżenie co do potrzeby, aby organ publiczny najpierw oszacował, czy przekazywanie, przetwarzanie i przechowywanie danych poza terytorium kraju może narazić bezpieczeństwo i prywatność obywateli oraz bezpieczeństwo i gospodarkę narodową na niedopuszczalne ryzyko – szczególnie, gdy chodzi o bazy zawierające dane szczególnie chronione (np. dane w spisie ludności) lub usługi pociągające za sobą wykorzystanie danych szczególnie chronionych (np. opieka zdrowotna).[48] Takie szczególne podejście powinno w każdym razie być stosowane zawsze, gdy dane szczególnie chronione są przetwarzane w kontekście cloud computingu. Z tego punktu widzenia takie szczególne podejście mogłoby być wprowadzone przez rządy krajowe oraz instytucje Unii Europejskiej w celu dalszego zbadania koncepcji ‘europejskiej chmury rządowej’ jako ponadnarodowej przestrzeni wirtualnej, w której mógłby być zastosowany spójny i ujednolicony zestaw zasad.
- - Europejskie Partnerstwo Cloud Computingu (ang. European Cloud Partnership - ECP): Grupa Robocza wspiera strategię ECP przedstawioną prze Panią Kroes, Wiceprzewodniczącą Komisji Europejskiej w styczniu 2012 r. w Davos.[49] Strategia ta dotyczy zamówień publicznych rozwiązań IT w celu pobudzenia europejskiego rynku

[46] Rozporządzenie Rady (WE) Nr 2271/96 z dnia 22 listopada 1996 r. zabezpieczające przed skutkami eksterytorialnego stosowania ustawodawstwa przyjętego przez państwo trzecie oraz działaniami opartymi na nim lub z niego wynikającymi, Dz. Urzędowy L 309, 29/11/1996 str. 0001 – 0006, adres URL: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:EN:HTML

[47] Patrz WP 191 – Opinia 1/2012 w sprawie propozycji reformy ochrony danych, str. 23.

[48] W tej kwestii ENISA przedstawia następujące zalecenie w swoim dokumencie dotyczącym bezpieczeństwa i odporności w przypadku rządowych usług w chmurze (http://www.enisa.europa.eu/activities/risk-management/emerging-and-futurerisk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): „Pod względem architektury, chmury prywatne i społecznościowe wydają się być rozwiązaniem dla wrażliwych aplikacji, które obecnie najlepiej dostosowane jest do potrzeb administracji publicznej, ponieważ chmury te zapewniają najwyższy poziom zarządzania, kontroli i widoczności, choć przy planowaniu chmury prywatnej lub społecznościowej szczególną uwagę należy zwrócić na skalę infrastruktury.”

usług w chmurze. Przekazywanie danych osobowych do europejskiego dostawcy usług w chmurze, regulowane europejskim prawem dotyczącym ochrony danych, może przynieść klientom ogromne korzyści w zakresie ochrony danych, wspierając w szczególności przyjęcie wspólnych standardów (szczególnie w zakresie interoperacyjności oraz możliwości przenoszenia danych) jak również legalność prawną.

[49] Neelie Kroes, Wiceprzewodnicząca Komisji Europejskiej odpowiedzialna za Agendę Cyfrową, utworzenie European Cloud Partnership podczas Światowego Forum Ekonomicznego w Davos, w Szwajcarii, 26 stycznia 2012 r., adres URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ZAŁĄCZNIK

a) Modele wdrożenia

Chmura prywatna[50] oznacza infrastrukturę informatyczną, która jest przeznaczona dla określonej organizacji; zlokalizowana jest w siedzibie organizacji lub zarządzanie nią jest powierzane stronie trzeciej (zazwyczaj poprzez hosting serwera), która ściśle podlega administratorowi. Chmurę prywatną można porównać do typowego ośrodka danych, a różnica polega na tym, że procedury technologiczne są wdrażane w celu zoptymalizowania wykorzystania dostępnych zasobów i zwiększenia tych zasobów poprzez małe inwestycje dokonywane racjonalnie i stopniowo i rozłożone w czasie.

Chmura publiczna to, przeciwnie, infrastruktura, którą posiada dostawca specjalizujący się w dostarczaniu usług, który udostępnia swoje systemy użytkownikom, przedsiębiorstwom i/lub organom administracji publicznej - i w związku z tym dzieli się nimi. Dostęp do tych usług możliwy jest przez Internet, co pociąga za sobą przekazywanie operacji przetwarzania danych i/lub danych do systemów usługowych dostawcy. W związku z tym dostawca usług podejmuje się kluczowej roli w zakresie skutecznej ochrony danych powierzonych tym systemom. Wraz z danymi użytkownik jest zobowiązany przekazać dużą część swojej kontroli nad tymi danymi.

Obok chmur „publicznych" i prywatnych" istnieją tzw. chmury „pośrednie" lub „hybrydowe", w przypadku których usługi dostarczane przez infrastruktury prywatne współistnieją z usługami nabywanymi z chmur publicznych. Należy również odnieść się do „chmur wspólnotowych", w przypadku których infrastruktura informatyczna jest współdzielona przez kilka organizacji na rzecz społeczności określonego użytkownika.

Elastyczność i łatwość konfigurowania systemów cloud computingu pozwala na ich „elastyczny" wymiar, tj. systemy te mogą być dostosowane do określonych wymogów zgodnie z podejściem opartym na wykorzystaniu. Użytkownicy nie muszą zarządzać żadnymi

---

[50] NIST (Narodowy Instytut Standaryzacji i Technologii) w USA, który od kilku lat pracuje nad standaryzacją technologii opartych na cloud computingu i którego definicje są również przeniesione do dokumentu ENISA:
Chmura prywatna.
Infrastruktura chmury jest prowadzona jedynie dla organizacji. Może nią zarządzać organizacja lub strona trzecia i może ona istnieć w siedzibie lub poza nią. Należy wskazać, że „chmura prywatna" bazuje co najmniej na określonych technologiach, które są również typowe dla „chmur publicznych" – w tym w szczególności technologiach wirtualizacji wspierających reorganizację (lub przegląd) architektury przetwarzania danych, jak wyjaśniono powyżej.
Chmura publiczna.
Infrastruktura chmury jest udostępniana opinii publicznej lub dużej grupie branżowej, a jej właścicielem jest organizacja sprzedająca usługi przetwarzania w chmurze.

systemami informatycznymi, które polegają na umowach outsourcingu i w związku z tym są w pełni zarządzane przez stronę trzecią, w której chmurze przechowywane są dane. Często zdarza się, że w grę wchodzą duzi dostawcy posiadający złożone infrastruktury; z tego powodu chmura mogłaby się rozprzestrzenić na kilka lokalizacji i użytkownicy mogliby ignorować fakt, gdzie dokładnie ich dane są przechowywane.

b) Modele świadczenia usługi

W zależności od wymogów użytkownika istnieje kilka rozwiązań cloud computingu dostępnych na rynku; można je podzielić na trzy główne kategorie lub „modele usług". Modele te zazwyczaj mają zastosowanie zarówno do rozwiązań chmury prywatnej, jak i publicznej.

- **IaaS (infrastruktura chmury jako usługa):** dostawca dzierżawi infrastrukturę technologiczną, tj. wirtualne zdalne serwery, na których użytkownik końcowy może polegać zgodnie z mechanizmami i ustaleniami mającymi przyczynić się do prostego, skutecznego i pożytecznego zastąpienia korporacyjnych systemów informatycznych w siedzibie firmy i/lub wykorzystania dzierżawionej infrastruktury obok systemów korporacyjnych. Tacy dostawcy to zazwyczaj wyspecjalizowani gracze rynkowi i mogą oni faktycznie bazować na fizycznej złożonej infrastrukturze, która często rozciąga się na kilka obszarów geograficznych.

- **SaaS (oprogramowanie chmury jako usługa):** dostawca dostarcza, za pośrednictwem sieci, różne usługi w zakresie aplikacji i udostępnia je użytkownikom końcowym. Usługi te często mają na celu zastąpienie tradycyjnych aplikacji, które mają być instalowane przez użytkowników w ich lokalnych systemach; w związku z tym użytkownicy mają powierzać swoje dane danemu dostawcy. Ma to miejsce np. w przypadku typowych internetowych aplikacji biurowych, takich jak arkusze kalkulacyjne, edytory tekstów, skomputeryzowane rejestry i terminarze, współdzielone kalendarze, etc.; jednak przedmiotowe usługi obejmują także programy e-mailowe w chmurze.

- **PaaS (platforma chmury jako usługa):** dostawca oferuje rozwiązania do zaawansowanego rozwijania i hostingu aplikacji. Usługi te są zazwyczaj kierowane do graczy rynkowych, którzy je wykorzystują w celu rozwijania i hostingu prawnie chronionych rozwiązań opartych o aplikacje w celu spełnienia wewnętrznych wymogów i/lub świadczenia usług stronom trzecim. Ponownie usługi dostarczane przez dostawcę PaaS powoduje, że nie jest konieczne, aby użytkownik polegał na dodatkowym i/lub specjalnym sprzęcie lub oprogramowaniu na poziomie wewnętrznym.

Pełnoprawne przejście na całkowicie publiczny system chmury okazałby się niewykonalny w krótkim czasie z szeregu powodów, w szczególności jeżeli chodzi o duże podmioty, takie jak duże przedsiębiorstwa lub organizacje, które muszą spełnić określone zobowiązania – np. duże banki, organy rządowe, duże miasta, etc. Wyjaśnieniem tego faktu mogą być głównie dwa względy: po pierwsze, istnieje chwilowy czynnik związany z inwestycjami wymaganymi do osiągnięcia takiej zmiany (przejścia); po drugie, należy uwzględnić szczególnie cenne i/lub szczególnie chronione informacje, które mają być przetwarzane w określonych przypadkach.

Inny czynnik przemawiający za bazowaniem na chmurach prywatnych (co najmniej w przypadkach wymienionych powyżej) dotyczy okoliczności, że często żaden dostawca chmury publicznej nie może zaoferować jakości usług (w oparciu o SLA – umowy o gwarantowanym poziomie usług), tak aby dotrzymać kroku istotnemu charakterowi usługi, którą dostawca ma zapewnić – być może dlatego, że przepustowość i niezawodność sieci nie są wystarczające lub odpowiednie w danym obszarze, lub w odniesieniu do szczególnych powiązań między użytkownikiem a dostawcą. Z drugiej strony, należy racjonalnie założyć, że chmury prywatne mogą być dzierżawione lub wynajmowane w niektórych z powyższych przypadków (ponieważ może to się okazać bardziej opłacalne), lub mogą być zastosowane modele chmury hybrydowej (w tym zarówno elementy publiczne, jak i prywatne). We wszystkich przypadkach należy dokładnie rozważyć istotne implikacje.

Przy braku standardów uzgodnionych na forum międzynarodowym, istnieje ryzyko stosowania rozwiązań cloud computingu typu „zrób to sam", lub zintegrowanych rozwiązań przetwarzania w chmurze, z którymi wiązałyby się większe zagrożenia tzw. zamknięciem (ang. „lock-in") (jak również tzw. „monokulturami prywatności")[51] i które uniemożliwiłyby pełną kontrolę nad danymi bez zapewnienia interoperacyjności. Zarówno interoperacyjność, jak i możliwość przenoszenia danych są rzeczywiście kluczowymi czynnikami służącymi rozwojowi technologii bazującej na cloud computingu oraz umożliwiającymi pełną realizację praw do ochrony danych przyznanych osobom, których dane dotyczą (takich jak dostęp do danych lub ich poprawienie).

Z tego punktu widzenia obecna debata nad technologiami cloud computingu stanowi znaczący przykład istnienia napięcia między podejściem zorientowanym na koszty, a tym zorientowanym na prawa, co zostało pokrótce wskazane w części 2 powyżej. Podczas gdy bazowanie na chmurach prywatnych może być wykonalne i rzeczywiście zalecane z

[51] Patrz studium Parlamentu Europejskiego „Czy to pomaga czy jest przeszkodą? Propagowanie innowacji Internetu oraz prawo obywateli do prywatności" opublikowane w grudniu 2011 r.

perspektywy ochrony danych, przy uwzględnieniu określonych okoliczności przetwarzania, może nie być to wykonalne dla organizacji na dłuższą metę, głównie przy podejściu zorientowanym na koszty. Niezbędna jest dokładna ocena wchodzących w rachubę interesów, ponieważ w tym obszarze nie można wskazać jednego uniwersalnego rozwiązania.