UNIWERSYTET SZCZECIŃSKI

ZESZYTY NAUKOWE NR 788

ACTA IURIS STETINENSIS 4

SZCZECIN 2013

Pełna wersja publikacji www.wpiaus.pl/actaiuris
Wersja papierowa jest wersją pierwotną
Streszczenia opublikowanych artykułów są dostępne online w międzynarodowej bazie danych
The Central European Journal of Social Sciences and Humanities http://cejsh.icm.edu.pl

ISSN 1640-6818
ISSN 2083-4373

WYDAWNICTWO NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

Wydanie I. Ark. wyd. 6,5. Ark. druk. 7,8. Format B5. Nakład 100 egz.

SPIS TREŚCI

Recenzje

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 788 ACTA IURIS STETINENSIS 4 2013

ALEKSANDRA MONARCHA-MATLAK[*]
Uniwersytet Szczeciński

CLOUD COMPUTING – PRZETWARZANIE W CHMURZE

Streszczenie

W artykule poruszono problematykę *cloud computing* w obszarze obowiązującej obecnie dyrektywy w sprawie ochrony danych osobowych, przyszłych przepisów unijnych oraz krajowych przepisów dotyczących ochrony danych osobowych. Perspektywa porównawcza umożliwiła sformułowanie istotnych wniosków wskazujących między innymi, że ani dyrektywa, ani nowe rozporządzenie unijne nie rozwiązują dotychczasowych problemów. Opisano podstawowe zagadnienia dotyczące przetwarzania w chmurze, wskazując jednocześnie jego wady i zalety. Nowe rozwiązania technologiczne sprawiły, że chmury stały się zjawiskiem ponad granicami i podziałami. Dla prawidłowego przetwarzania w chmurze konieczne jest stworzenie pewności prawnej, uproszczenie środowiska normatywnego oraz zapewnienie jasnych reguł dotyczących przesyłania danych za granicę.

Słowa kluczowe: chmura, przetwarzanie, ochrona danych, rozporządzenie o ochronie danych, prawo unijne

[*] E-mail: a.monarcha@mec.univ.szczecin.pl.

Zagadnienia ogólne

Cloud computing jest prostym pomysłem z olbrzymią siłą oddziaływania – zamiast indywidualnie eksploatować aplikacje na własnych komputerach, można uruchomić aplikacje na serwerach ośrodka obliczeniowego zarządzanego przez usługodawcę. Użytkownik tylko loguje się, dokonuje zmiany ustawień, w zależności od potrzeb, i zaczyna pracować.

Cloud computing to grupy komputerów, których nie widzimy, nie *odwiedzamy*, są w *chmurach*, zawsze blisko nas. Podstawowym celem usługi *cloud* jest przeniesienie danych tam, gdzie dostępne są zasoby *wolnej pamięci procesorów*, czyli do dostawców usług *cloud computing* (dalej: c.c.).

Dostawcy usług c.c. powinni zapewnić dostawy usług zgodnie z prawem ochrony danych osobowych. Obok wymogów: poufności, integralności, dostępności danych, powinni także zapewnić możliwość wpływania na przetwarzanie danych oraz ponosić odpowiedzialność za przetwarzanie danych w c.c.[1] Informacje usługodawców powinny być transparentne, otwarte co do wykazywanych ramowych warunków technicznych, organizacyjnych i prawnych oferowanych przez nich usług c.c. Dotyczy to także koncepcji bezpieczeństwa. Jednocześnie użytkownik usług c.c. powinien uzyskać informacje pozwalające na dokonanie wyboru między oferentami usług oraz sam powinien rozstrzygnąć, czy w ogóle będzie korzystał z tego typu usług. W świetle takich rozważań należałoby przyjąć za regułę, że usługi c.c. powinny być kształtowane zgodnie z prawem ochrony danych osobowych oraz dawać możliwość odwołania się do innych przepisów prawa.

Od dostawców usług c.c. należy wymagać:

- jednoznacznych, transparentnych, szczegółowych informacji o przetwarzaniu danych w chmurze, w szczególności o miejscu ich przetwarzania, o zmianie tego miejsca, o interoperacyjności;
- wdrożenia uzgodnionych środków bezpieczeństwa danych i to zarówno po stronie usługodawcy, jak i usługobiorcy;
- aktualnych dokumentów, na przykład certyfikatów bezpieczeństwa informacji, certyfikatów uznanych i niezależnych organizacji kontrolnych

[1] Usługi c.c. nie mogą prowadzić do tego, iż podmioty przetwarzające dane nie będą ponosiły odpowiedzialności za przetwarzanie niezgodnie z przepisami prawa. Stanowisko takie w pełni zasługuje na poparcie.

badających stan infrastruktury, która będzie używana przy świadczeniu usługi c.c.

Przedstawione uwagi skłaniają do wskazania celów szczegółowych, do których powinny dążyć podmioty świadczące usługi c.c., by prawidłowo *działała* chmura. Są to: 1) stworzenie pewności prawnej; 2) uproszczenie środowiska regulacyjnego (normatywnego); 3) zapewnienie jasnych reguł dotyczących przesyłania danych za granicę[2].

1. *Cloud computing* a ochrona danych w UE

Komisja Europejska zaproponowała nowy projekt rozporządzenia, który ma zastąpić unijną dyrektywę o ochronie danych[3]. Celem zmian wprowadzonych w rozporządzeniu jest zwiększenie możliwości rozwoju firm, które chcą prowadzić interesy na terenie Unii Europejskiej, zapewniając jednocześnie wysoki poziom ochrony danych osobowych. Pojawia się od razu pytanie, w jakim stopniu proponowane rozporządzenie wpłynie na użytkowanie *cloud computing* w Unii Europejskiej.

Nowe rozporządzenie stanowi część ogólnej strategii unijnej, tak zwanej ekonomii cyfrowej ujawnionej w dokumencie z 2010 roku *Digital agenda for Europe*. Celem do osiągnięcia jest stworzenie jednolitego rynku cyfrowego, bardziej jednolitego przede wszystkim dla konsumentów, ale także dla konkurencyjności. Ma to pozwolić na opracowanie w przyszłości światowego standardu ochrony danych.

---

[2] Coraz częściej daje się zauważać ostre stanowiska przeciwko amerykańskim dostawcom usług *cloud* (np. stanowisko rządu holenderskiego). Argumentacją jest to, że zgodnie z amerykańskim *Patriot Act* dostawcy usług są zobowiązani na żądanie władz amerykańskich dostarczać wszelkich danych usługobiorców, nie informując jednocześnie o tym zainteresowanych.

[3] W tej części pracy wykorzystano opracowanie: *Cloud computing under the European Commission`s proposed regulation to revise the EU data protection framework*; Bloomberg BNA, World Data Protection Report, February 2012, vol. 12, no. 2 oraz Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. L 281 z 23.11.1995 (dalej: dyrektywa), Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), Bruksela, 25.01.2012, COM (2012) 11 final, 2012/0011 (COD) (dalej: rozporządzenie).

Komisja zaproponowała zakładanie serwerów chmurowych w Unii Europejskiej i na obszarze Europejskiego Obszaru Gospodarczego. Obecnie wiele ważnych ośrodków obliczeniowych znajduje się poza tymi obszarami. Jednocześnie chodzi o wyważenie interesu tak zwanego programu cyfrowego dla Europy z potrzebą ustanowienia adekwatnych zabezpieczeń transferu danych poza Unię Europejską. Problemy prawne jednostek unijnych (zarówno sektora publicznego, jak i prywatnego), które chciałyby powierzyć swoje dane, są dobrze znane i skupiają się wokół dwóch zagadnień:

1. Czy właściwe jest, aby klient usług c.c. powierzał bezpieczeństwo danych osobowych dostawcy tych usług?
2. Czy powinien to uczynić, jeśli dane te będą przechowywane poza granicami Unii Europejskiej?

Przepisy rozporządzenia podnoszą jeszcze inne zagadnienia, które będą się odnosiły do *cloud computing*, a mianowicie podwyższony reżim egzekucji, na przykład kary pieniężne, i obowiązek notyfikacji awarii bezpieczeństwa.

2. Dyrektywa a rozporządzenie

W dyrektywie unijnej nr 95/46 poczyniono rozróżnienie między administratorem danych a przetwarzającym; rozciąga się ono na wszystkie postanowienia dyrektywy. Administrator, zgodnie z dyrektywą, ponosi przeważającą odpowiedzialność prawną, podczas gdy przetwarzający nie ponosi takiej odpowiedzialności, ma jedynie dochować zobowiązań kontraktowych zawartych z administratorem danych. W proponowanym nowym rozwiązaniu definicje administratora i przetwarzającego generalnie pozostają te same. Jako odejście od obecnego stanowiska w rozporządzeniu proponuje się, aby przetwarzający również ponosił odpowiedzialność za bezpieczeństwo (art. 30 rozporządzenia). Ponadto organy nadzorcze będą miały możliwość wyegzekwowania przestrzegania postanowień rozporządzenia i to nie tylko tych, które stwierdzają, że są obowiązkiem przetwarzającego (art. 52 ust. 1 lit. a oraz art. 53 rozporządzenia), w szczególności art. 27 rozporządzenia zezwalający na przetwarzanie danych tylko na polecenie administratora danych lub z mocy przepisów UE albo państwa członkowskiego. I tak, art. 28 wymaga od przetwarzającego i administratora adekwatnej dokumentacji przetwarzania danych, natomiast art. 29 zobowiązuje administratora i przetwarzającego do współpracy z organem nadzorczym.

Obecnie wielu dostawców usług c.c. twierdzi, że powinni być uważani tylko za przetwarzających i w ten sposób unikaliby obowiązków nałożonych na administratorów danych. W opinii Grupy Roboczej Art. 29 nie jest absolutnie pewne, czy tak też będzie w oczach regulatorów i ustawodawcy. Chociaż definicje pozostały te same, to ich interpretacja wcale nie prowadzi do jednoznacznych wniosków. Wątpliwości nadal pozostają, czy dostawca usług c.c. jest przetwarzającym czy administratorem.

3. Bezpieczeństwo przetwarzania

Artykuł 30 rozporządzenia wymaga zarówno od administratora, jak i przetwarzającego zapewnienia odpowiednich środków bezpieczeństwa oraz – zgodnie z art. 26 i art. 6 – uznaje się, że warunkiem koniecznym przetwarzania jest zawarcie umowy. Pojawiają się jednak nowe postanowienia, które mogą się utrwalić. Mianowicie, dostawca usług c.c. w porównaniu z treścią obecnej dyrektywy nie będzie mógł pozyskać innego przetwarzającego (art. 26 ust. 2 pkt d) bez zgody administratora. Uniemożliwi to dostawcy usługi typu SaaS użytkowanie usługi IaaS innego dostawcy bez zezwolenia klienta[4]. Oczywiste jest, że dostawcy usług będą stosowali generalne klauzule pozwalające na zawarcie umów z poddostawcami według uznania, trudno jednak stwierdzić, czy to w oczach regulatorów będzie oznaczało wypełnienie postanowień rozporządzenia.

---

[4] Usługi SaaS, PaaS, IaaS, czyli oprogramowanie jako usługa SaaS, w której ramach klient otrzymuje najbardziej rozbudowany model chmury. Dostawca dostarcza klientowi wszystko, czyli infrastrukturę i aplikacje. Użytkownik użytkuje bezpośrednio aplikacje, nie musi nic rozmieszczać w chmurze. Aplikacje są dostępne z różnych urządzeń klienckich, np. wyszukiwarka sieciowa albo interfejs programowy.
Platforma jako usługa – PaaS, oznacza zdolności obliczeniowe udostępnione użytkownikowi. Mają one umożliwić rozmieszczenie przez użytkownika aplikacji zakupionych lub stworzonych przez niego samego. Stworzonych przy użyciu języka oprogramowania, narzędzi dostarczanych przez dostawcę. Nie oznacza to zakazu *a priori* używania języków oprogramowania z innych źródeł. Użytkownik nie zarządza i nie kontroluje infrastruktury chmury obejmującej serwery, nośniki danych. Ma kontrolę nad rozmieszczonymi aplikacjami i ustawieniami aplikacyjnymi środowiska, w którym działa aplikacja.
Infrastruktura jako usługa IaaS – to jest zestaw sprzętu i oprogramowania, które umożliwia funkcjonowanie c.c. Infrastrukturę można rozpatrywać w podziale na warstwę fizyczną (zasoby sprzętowe niezbędne do wsparcia usług chmury, serwer, nośniki danych, składniki sieci) i warstwę *abstrakcji*, na którą składa się oprogramowanie zawieszone na warstwie fizycznej. To oprogramowanie wykonuje podstawowe cechy chmury (samoobsługa, swobodny dostęp przez sieć, agregacje zasobów niezależnie od lokalizacji, elastyczność, płatność tylko za wykorzystane zasoby). Koncepcyjnie warstwa *abstrakcji* znajduje się ponad warstwą fizyczną.

Umowa musi być zawarta na piśmie i zobowiązywać dostawcę przetwarzającego do działania zgodnie z zasadami przetwarzania danych osobowych. Rozporządzenie proponuje te same zadania, jakie były przewidziane w dyrektywie, dla upewnienia się, czy administrator danych podejmuje odpowiednie działania, delegując zadania do przetwarzającego.

Rozporządzenie nie usuwa trudności, na jakie napotyka obecnie klient, który musi zaakceptować *standardowe* bezpieczeństwo oferowane przez dostawców.

Dostawca powinien podejmować racjonalne wysiłki dla zapewnienia bezpieczeństwa danych. Bardziej dociekliwi klienci będą starali się uszczegółowić, co faktycznie powinno być zapewnione. W ostateczności jednak będą musieli zaufać dostawcom chmur.

Ekonomika chmury zależy od rentowności, zależy także od tego, czy jest to oferta standardowa, czy też adresowana do wielu indywidualnych użytkowników. Z tego względu dostawca nie będzie w stanie dostosować swoich mechanizmów bezpieczeństwa do specyficznych klientów.

Zamiar wprowadzenia zmian w reżimie egzekucyjnym spowoduje, że klienci będą ostrożniejsi, a dostawcy – zwłaszcza amerykańscy (pomimo dużej liczby protestów z ich strony) – będą tymi, od których będzie można żądać odszkodowania oraz na których mogą być nałożone wysokie kary (chociaż projekt rozporządzenia nie odnosi się do tego problemu).

4. Prawo do kontroli

Zgodnie z unijną dyrektywą (art. 17 ust. 2) administrator musi zapewnić środki bezpieczeństwa, zgodnie z przepisami, u przetwarzającego. Często jest to interpretowane jako żądanie fizycznej możliwości zbadania urządzeń dostawcy (usługodawcy). W praktyce jest to jednak trudne do spełnienia, zwłaszcza w kontekście usług c.c. Nadal nic się nie zmieniło i chmura nie została *wyzwolona.*

Takie postawienie sprawy odnośnie do fizycznego zbadania urządzeń wydaje się dyskusyjne z kilku powodów. Jest ono między innymi utrudnione przy kompleksowym pozyskiwaniu usług c.c., obejmującym lokalizację danych na wielu serwerach, z wieloma użytkownikami, do tego w nieokreślonych bliżej lokalizacjach. Usługi mogą być świadczone jednocześnie lub podyktowane

nieustannie zmieniającą się sytuacją, albo świadczone jednocześnie w wielu miejscach. Chcąc wyegzekwować stosowanie takiego przepisu, prawie niemożliwe stanie się korzystanie z usług c.c. w przypadku, gdy będziemy mieli do czynienia z danymi osobowymi. Ten aspekt bezpieczeństwa może być zrealizowany za pomocą innych środków kontroli, na przykład pełnego monitoringu i raportowania przez dostawcę usługi c.c. lub poddanie się pełnej certyfikacji bezpieczeństwa przez akredytowaną organizację.

5. Transgraniczny przesył danych

Wiele negatywnych komentarzy dotyczących możliwości korzystania z usług c.c. oferowanych przez Stany Zjednoczone Ameryki (gdzie ma siedzibę większość dostawców usług c.c.) dotyczy nienależytego poziomu ochrony danych osobowych w myśl przepisów unijnej dyrektywy.

Niektórzy z większych dostawców usług IaaS twierdzą, że przynajmniej w niektórych oferowanych przez nich usługach dane pozostaną w *serwerowniach* zlokalizowanych na obszarze Unii Europejskiej. Inni natomiast otwarcie przyznają, że dane nie pozostaną na jej terenie. W takim przypadku należałoby wdrożyć jeden z mechanizmów, który upoważniałby do przesyłu danych zgodnie z zasadą, że przekazanie może nastąpić tylko wtedy, gdy zapewniony będzie odpowiedni poziom ochrony, to jest zachowana będzie praworządność w tym zakresie oraz będzie istniał i skutecznie działał niezależny organ nadzorczy.

6. Stanowisko pod rządami dyrektywy

W literaturze prawniczej pojawiły się następujące opcje (koncepcje) dotyczące bezpieczeństwa danych w *chmurze*. Ma być ono zapewnione przez przyjęcie następujących zasad:

1. Dane będą przechowywane w krajach europejskich lub w państwie zapewniającym odpowiednią ochronę danych osobowych (co, oczywiście, wyklucza Stany Zjednoczone Ameryki jako dostawcę usług c.c.).
2. Amerykański dostawca usług c.c. powinien znajdować się na liście Safe Harbor.

3. W umowach powinny mieć zastosowanie klauzule standardowe, które działają dobrze z punktu widzenia klienta, nie są jednak dobrze widziane przez dostawców, gdyż zmuszają ich do zaakceptowania dodatkowych warunków odpowiedzialności.
4. Klient powinien mieć możliwość kontroli i oceny bezpieczeństwa swoich danych. Użytkownik sam ocenia, czy wszystko jest w porządku (takie rozwiązanie jest przyjęte w Wielkiej Brytanii i w niektórych krajach UE), to znaczy może dojść do wniosku, że przekazane dane osobowe są należycie chronione. Dotyczy to sytuacji, gdy dane nie są szczególnie wrażliwe; zachowano należytą staranność ochrony danych wrażliwych; zadbano, aby w umowie znalazły się odpowiednie klauzule dotyczące bezpieczeństwa; gdy dostawca chmury jest renomowaną firmą.

7. Inne metody

Dla kompletności rozważań warto zauważyć, że istnieją także inne metody transferu danych, które nie są jednak pomocne w większości rozwiązań świadczonych w ramach usług c.c. Ułatwiają one jedynie transfery w ramach grup (lub w grupie) i jako takie mogą być użyteczne w odniesieniu do chmur prywatnych. Konieczne jest wówczas uzyskanie zgody osób, których dane dotyczą, na transfer danych oraz wskazanie, gdzie mają być przekazane. Koniecznym warunkiem dokonania transferu jest również zawarcie umowy z osobą, której dane dotyczą.

8. Sytuacja pod rządami rozporządzenia

Rozporządzenie obiecuje harmonizację zarządzania usługami c.c. również dzięki temu, że ma być stosowane bezpośrednio we wszystkich państwach. Zakłada ono, że narodowi regulatorzy będę postępowali spójnie w zakresie stosowania podstawowych reguł. W rozporządzeniu przewidziano następujące opcje:

1. Przechowywanie danych będzie mogło mieć miejsce na terenie Unii Europejskiej lub w innym państwie aktywnie odpowiadającym za

ochronę danych. W rozporządzeniu proponuje się większą precyzję co do tego, czym jest *odpowiedzialność*.

2. Przyjęcie postanowień Safe Harbor w związku z art. 41 rozporządzenia.
3. Zastosowanie klauzul standardowych pozostanie rozwiązaniem opcjonalnym. W rozporządzeniu nie zostało wyraźnie powiedziane, że klauzule modelowe, zatwierdzone pod rządami starych przepisów, będą nadal wymagane. Należy się jednak spodziewać takiego rezultatu.
4. Pozostawienie tak zwanych wiążących przepisów korporacyjnych (BCR – *Bending Corporation Rouls*) wymagających zgody na transfer i wskazujących konieczność zachowania formy pisemnej umowy (art. 43 i 44).
5. W projekcie jest mowa o *ocenie klienckiej* ujętej w taki sposób, że nie będzie ona miała zastosowania w usługach c.c. (art. 44 ust. 1 lit. h) – przekazanie danych jest konieczne z uwagi na potrzeby wynikające ze słusznych interesów administratora lub podmiotu przetwarzającego, których nie można uznać za częste lub masowe. W odniesieniu do *oceny klienckiej* nacisk położono na transfer *ad hoc* (nie częsty lub masowy), w przeciwieństwie do ciągłego (stałego) *outsorsingu* przetwarzania danych przez dostawcę chmury. Proponuje się, aby wymogiem stało się udokumentowanie takiej oceny i informowanie regulatora o fakcie transferu (nie jest to jednak użyteczne z punktu widzenia potencjalnego klienta usług c.c.).

Równie niewiele zaproponowano w postanowieniach dotyczących przekazywania danych ułatwiających pozyskiwanie lub korzystanie z usług c.c. w Unii Europejskiej. Tak naprawdę główną intencją i znaczącą zmianą jest pozbawienie klienta chmury oceny poziomu ochrony danych. Artykuł 31 rozporządzenia stanowi: „W przypadku naruszenia ochrony danych osobowych, administrator zgłasza organowi nadzorczemu takie naruszenie..." Jeżeli natomiast zlecono przetwarzanie danych podmiotowi trzeciemu w chmurze, to niezwłoczne powiadomienie może mieć miejsce tylko wtedy, gdy podmiot przetwarzający poinformuje administratora. Właściwe byłoby natychmiastowe powiadomienie administratora po naruszeniu przez podmiot przetwarzający. Administratorowi daje się 24 godziny na dokonanie zgłoszenia, podczas gdy przetwarzającemu nie wyznacza się żadnego terminu ani nie grożą mu żadne sankcje. Należałoby przyjąć, że jeżeli dostawcą usług c.c. byłby faktycznie administrator danych, to zobowiązanie do poinformowania organu nadzorczego po-

winno spoczywać łącznie na obu stronach. Biorąc pod uwagę względnie skomplikowane wymagania dotyczące takiej informacji, istnieje teoretycznie możliwość niezależnego poinformowania organu nadzorczego. Dlatego istotne wydaje się, aby w umowie o świadczenie usług c.c. określono, kto ma informować właściwych regulatorów. Powiadomienie organu nadzorczego musi zawierać określone informacje – rodzaj naruszenia uprawnienia, konsekwencje naruszenia, środki, które administrator proponuje, aby usunąć skutki naruszenia ochrony danych osobowych. Administrator musi udokumentować fakty, skutki naruszenia oraz podjęte działania zaradcze, aby organ nadzorczy mógł zweryfikować, czy administrator przestrzega przepisów (art. 31 ust. 4 rozporządzenia).

Końcowym zagadnieniem w tej części jest zakres terytorialny rozporządzenia, o którym mowa w art. 3 ust. 3. Rozporządzenie ma także zastosowanie do przetwarzania danych osobowych przez administratora, który nie ma siedziby na terytorium Unii Europejskiej, lecz w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo krajowe państwa członkowskiego. W ten sposób na przykład amerykański dostawca usług c.c. byłby zobowiązany do poinformowania klienta o naruszeniach ochrony danych osobowych. Ten eksterytorialny zasięg rozporządzenia spotkał się z powszechną krytyką, gdyż właściwie jest niemożliwy do wyegzekwowania w stosunku do podmiotów spoza UE.

9. Sankcje administracyjne

Zgodnie z art. 79 rozporządzenia, organ nadzorczy jest uprawniony do nakładania sankcji administracyjnych w przypadku naruszeń przepisów rozporządzenia. Istotne jest to, że w tym artykule nie zostały wyraźnie określone sankcje. Mają być one skuteczne, proporcjonalne i przekonywające oraz nakładane indywidualnie. Organ nadzorczy powinien ocenić naturę naruszenia (czas trwania, stopień odpowiedzialności) i ewentualnie nałożyć karę grzywny.

Kolejne wątpliwości pojawiają się w związku z niezastosowaniem się do art. 30 rozporządzenia w kontekście usług c.c. Administrator oraz podmiot przetwarzający mają obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić odpowiedni poziom bezpieczeństwa stosowny do ryzyka związanego z przetwarzaniem oraz charakterem danych osobowych, uwzględniając najnowsze osiągnięcia techniczne oraz koszty ich wdrożenia.

Klienci chmury zazwyczaj polegają na zapewnieniach dostawcy co do bezpieczeństwa danych oraz na jego informacjach o naruszeniach. Jeżeli dostawca źle zadziałał, *większe* firmy będą w stanie wystąpić o odpowiednie odszkodowanie od dostawcy chmury, w związku z zaistniałymi zaniedbaniami. Jednocześnie większość klientów usług c.c. zawiera umowy na standardowym formularzu, udostępnionym przez dostawcę, wobec czego aspektem pozwalającym na odróżnienie tej umowy od umów dotyczących innych technologii jest przyjęte rozwiązanie techniczne. Klient, zawierając umowę standardową na usługi c.c., jedynie akceptuje warunki dostawy chmury, nie mając żadnej przestrzeni do negocjacji. Tymczasem tam, gdzie kontrakty nie są negocjowane, dostawcy zazwyczaj nie ponoszą odpowiedzialności za zaistniałe problemy i naruszenia, albo ma ona bardzo niewielki wymiar.

Konkluzje

W kontekście dotychczasowych rozważań trudno jest obecnie stwierdzić, czy proponowane rozporządzenie przyczyni się do zwiększenia zainteresowania usługami c.c. Trudności prawne, które powstały pod rządami dyrektywy, pozostaną nadal (jak na przykład kwestie transgranicznego przesyłu danych, restrykcje odnoszące się do poddostawców), tak jak i trudności koncepcyjne dotyczące na przykład rozstrzygnięcia, czy dostawca usług jest podmiotem przetwarzającym, czy administratorem. Rozporządzenie również pod niektórymi względami tworzy nowe przeszkody, na przykład z uwagi na zwiększone obciążenie przepisami prawnymi dostawców usług, którzy zostali obarczeni większą odpowiedzialnością za bezpieczeństwo, a regulatorzy otrzymali narzędzia, za pomocą których łatwiej będą mogli egzekwować przestrzeganie przepisów rozporządzenia. Jednym słowem zwiększony będzie potencjał sankcji.

Należy stwierdzić, że w zasadzie rozporządzenie nie rozwiązuje problemów, z którymi obecnie borykają się klienci z Unii Europejskiej i dostawcy usług chcący sprzedać swoje usługi. Na dłuższą metę może ono zachęcić klientów z UE do korzystania z usług dostawców działających na jej terenie, jednak, biorąc pod uwagę przewagę Stanów Zjednoczonych Ameryki w tym sektorze, niewiele to pomoże, aby zliberalizować chmurę. Pod tym względem rozporządzenie można uznać za straconą szansę, gdyż biznes już rozpoczął intensywny proces lobbystyczny.

CLOUD COMPUTING

Summary

The paper discusses the issues of Cloud computing in the current Directive on the protection of personal data, future EU regulations and the national legislation on protection of personal data. A comparative perspective has enabled to draw the conclusions which suggested, inter alia, that neither the Directive nor the new EU regulations does not solve the existing problems. the basic problems relating to cloud computing indicating, at the same time, its pros and cons, have been described. New technological solutions made the clouds become a phenomenon across borders and boundaries. For the proper processing in the cloud it is necessary to create legal certainty and simplification of the regulatory rules in the environment to provide clear data transmission abroad.

Translated by mgr Krystyna Sobczak

Keywords: cloud, computing, data protection, general data protection regulation, union law