Agnieszka Grzegorek
Uniwersytet Warszawski

BEZPIECZEŃSTWO ORAZ ASPEKTY PRAWNE PRZETWARZANIA DANYCH W CHMURZE OBLICZENIOWEJ

WPROWADZENIE

Dynamicznie rozwijający się rynek technologii informacyjno-komunikacyjnych przynosi coraz to bardziej zaawansowane rozwiązania, których funkcjonalność pozwala na prowadzenie działalności gospodarczej w sposób bardziej efektywny. Przetwarzanie w chmurze obliczeniowej (ang. *cloud computing*) jest alternatywą do tradycyjnego modelu pozyskiwania zasobów informatycznych polegającego na samodzielnym nabywaniu przez przedsiębiorców sprzętu i oprogramowania. Istotą rozwiązań oferowanych w modelu chmury obliczeniowej jest przetwarzanie danych na serwerach należących do podmiotu trzeciego oraz korzystanie za pośrednictwem Internetu z aplikacji informatycznych dostarczanych przez dostawcę usług w chmurze. Przetwarzanie danych obejmuje jakiekolwiek operacje wykonywane na danych, w szczególności będzie to zbieranie, przechowywanie, utrwalanie, opracowywanie, zarządzanie, analizowanie, zmienianie, udostępnianie i usuwanie[1]. Dane przechowywane są w olbrzymich centrach przetwarzania danych, zazwyczaj zlokalizowanych w dyskretnych lokalizacjach, w warunkach zapewniających odpowiednie bezpieczeństwo.

Powszechnie funkcjonuje definicja przetwarzania w chmurze stworzona przez amerykański Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology, dalej: NIST), która przedstawia chmurę obliczeniową jako model świadczenia usług pozwalający na dostęp do dzielonej puli konfigurowalnych zasobów informatycznych (np. sieci, serwerów, pamięci masowych, aplikacji i usług), które są dynamicznie udostępniane i zwalniane stosownie do zapotrzebowania użytkownika przy minimalnym zaangażowaniu ze strony

[1] Por. definicję „przetwarzanie" w: R. Burnett, P. Klinger, *Drafting and Negotiating IT Contracts*, Bloomsbury Professional 2013, rozdz. 16, s. 428 i n.; Wytyczne Komisji Nadzoru Finansowego dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych z 16 grudnia 2014 r., https://www.knf.gov.pl/Images/wytyczne_IT_firmy_inwestycyjne_tcm75-40002.pdf (dostęp: 8.05.2016 r.).

dostawcy usług w chmurze. Dostęp do dzielonych zasobów chmury obliczeniowej jest realizowany za pośrednictwem sieci. Większość operacji przydzielania i zwalniania zasobów realizowana jest automatycznie, a system monitoruje i raportuje ich zużycie[2]. Podmiot zewnętrzny zobowiązuje się do realizacji usług w modelu chmury obliczeniowej w zamian za wynagrodzenie, które zazwyczaj zależy od rozmiaru skorzystania przez użytkownika z udostępnionego przez dostawcę zasobu.

W przetwarzaniu w chmurze mamy do czynienia ze zdigitalizowaną formą informacji. Wiedza przekazywana w informacji może dotyczyć zarówno informacji ogólnodostępnych, jak i prywatnych. W przypadku, gdyby te ostatnie trafiłyby do rąk osoby, która nie jest uprawniona do ich posiadania, mogłoby to spowodować poważne straty, których rozmiar jest trudny do przewidzenia. Zagadnienia poruszane na łamach niniejszego artykułu rozważane są w głównej mierze z perspektywy użytkownika chmury będącego podmiotem gospodarczym. Nie ulega wątpliwości, że zachowanie poufności danych stanowiących tajemnicę przedsiębiorstwa czy danych jego klientów ma fundamentalne znaczenie dla reputacji przedsiębiorstwa oraz utrzymania jego konkurencyjności[3].

W przetwarzaniu w chmurze stykamy się z globalnym przetwarzaniem informacji, jak również z procesem industrializacji usług informatycznych[4]. Z wielu powodów rozwiązanie to staje się obecnie atrakcyjną alternatywą wobec wdrażania systemów informatycznych. Pozwala ono znacząco zredukować koszty zakupu sprzętu i oprogramowania oraz koszty pośrednie związane z nakładem pracy niezbędnej do uruchomienia i administracji własnego systemu.

Złożoność rozwiązań w chmurze obliczeniowej przejawia się nie tylko w postaci zaawansowania technologicznego, lecz także konieczności uwzględnienia różnych reżimów prawnych, które znajdują tutaj zastosowanie (np. przepisy ochrony danych osobowych, prawo własności intelektualnej czy ochrona konsumentów)[5]. Warto także zwrócić uwagę, że w przypadku niektórych zawodów prawo do prywatności jest chronione odrębnymi przepisami (np. tajemnica bankowa, ubezpieczeniowa, lekarska, handlowa, skarbowa czy adwokacka)[6].

---

[2] P. Mell, T. Grance, *The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology*, *Computer Security Division*, *Information Technology Laboratory*, *National Institute of Standards and Technology*, National Institute of Standards and Technology, September 2011, s. 2; zob. szerzej na temat cech charakterystycznych chmury obliczeniowej: tamże.

[3] B. Hołyst, J. Pomykała, *Cyberprzestępczość*, *ochrona informacji i kryptologia*, „Prokura i Prawo" 2011, nr 1, s. 6–7.

[4] Przetwarzanie w chmurze jest przez niektórych autorów uznawane za rodzaj outsourcingu. Tak np. R. Burnett, P. Klinger, *Drafting*..., s. 429.

[5] K. McGillivray, *Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU*, „Tulane Journal of Technology and Intellectual Property" 2014, Vol. 17, s. 218.

[6] Zob. więcej np. w: M. Krzysztofek, *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, Warszawa 2015, rozdz. 1 i 2; B. Hołyst, J. Pomykała, *Cyberprzestępczość*..., s. 13.

Przetwarzanie w chmurze z natury swojej może przekraczać granice jednego kraju, a dane mogą być przechowywane na serwerach, których lokalizacja będzie użytkownikom nieznana. Nie dziwi więc fakt, że klienci chmury obliczeniowej przed podjęciem decyzji o powierzeniu podmiotowi trzeciemu kontroli nad własnymi danymi będą chcieli zweryfikować, w jaki sposób dostawca zamierza wypełnić zobowiązania kontraktowe.

Znaczenie gospodarcze przetwarzania w chmurze rośnie. W ślad za tym, rynek chmury obliczeniowej rozwija się bardzo dynamicznie. Na gruncie prawa polskiego brak jest odrębnych przepisów regulujących transakcje mające za swój przedmiot usługi przetwarzania w chmurze obliczeniowej. Należy jednak zauważyć, że biorąc pod uwagę złożoność oraz ciągły rozwój tych rozwiązań, stworzenie jednej regulacji i zapewnienie jej aktualności, byłoby zadaniem niezwykle trudnym[7]. Pewne inicjatywy na tym polu są podejmowane przez instytucje Unii Europejskiej. Ich celem jest zwiększenie pewności prawnej przetwarzania w chmurze obliczeniowej oraz stosowanie uczciwych warunków kontraktowych w tego typu transakcjach. Niektóre z tych działań zostaną omówione w dalszych fragmentach pracy, inne – z uwagi na ograniczenia związane z rozpiętością teksu – zostaną zasygnalizowane.

Celem artykułu jest omówienie wybranych aspektów prawnych przetwarzania danych w chmurze. Rozważania będą poświęcone w głównej mierze kwestii bezpieczeństwa, prywatności, zapewnienia zgodności z obowiązującymi przepisami prawa ochrony danych osobowych oraz najbardziej charakterystycznym postanowieniom umownym.

Początkowy fragment artykułu opisuje podstawowe rodzaje usług w chmurze funkcjonujące obecnie na rynku tych rozwiązań oraz pewne ich aspekty techniczne, których znajomość jest istotna w celu prawidłowej analizy problemów związanych z bezpieczeństwem, kontrolą danych oraz konstrukcją postanowień umownych.

USŁUGI PRZETWARZANIA W CHMURZE

Cechą charakterystyczną właściwej chmury obliczeniowej jest wbudowana możliwość skalowania mocy obliczeniowej[8]. Usługi w chmurze mogą być ofe-

[7] K. Biczysko-Pudełko, *Znaczenie soft law dla regulacji cloud computing*, (w:) K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne: współczesne problemy prawne*, Warszawa 2016, s. 220–221.

[8] Przykładem niemal nieograniczonej mocy obliczeniowej jest korzystanie z wyszukiwarki WWW, kiedy to na zadane zapytanie wyszukiwarka natychmiast zwraca stronę z wynikami, które najbardziej odpowiadają zadanemu zapytaniu. Zob. szerzej: C. Osterwalder, *Przetwarzanie na*

rowane przy założeniu współdzielenia zasobów przez nieograniczoną liczbę użytkowników – mamy wtedy do czynienia z tzw. chmurą publiczną, lub przy założeniu, że dostęp do jej zasobów jest ograniczony do określonego podmiotu lub członków tej samej organizacji – znana pod pojęciem chmury prywatnej[9]. Przetwarzanie w chmurze dostarczane jest w kilku powszechnie rozpoznawalnych modelach, które różnią się pod względem wydajności, bezpieczeństwa oraz stopniem kontroli sprawowanej przez dostawcę chmury i użytkownika. W najbardziej podstawowym modelu funkcjonującym pod nazwą *Infrastructe as a Service* (dalej: IaaS)[10] użytkownik otrzymuje infrastrukturę (najczęściej w formie wirtualnych maszyn), korzysta z przetwarzania danych, skalowanej wirtualizacji, może uruchomić własne oprogramowanie lub aplikacje na udostępnionym mu zasobie. Dostawca IaaS sprawuje kontrolę nad infrastrukturą chmury, natomiast począwszy od poziomu systemów operacyjnych kontrola jest po stronie użytkownika. Zaletami korzystania z IaaS są m.in.: zaawansowana technicznie ochrona przed fizycznymi awariami nośników informacji, zmniejszenie kosztów pozyskania infrastruktury sprzętowej oraz krótki czas uruchomienia usługi w porównaniu do budowy własnego centrum magazynowania danych. Z kolei usługa znana jako *Software as a Service* (dalej: SaaS)[11] polega – najogólniej rzecz ujmując – na eksploatacji aplikacji informatycznych poprzez przeglądarkę internetową. W tym modelu dostawca sprawuje kontrolę nad systemem począwszy od sprawowania pieczy nad prawidłowym funkcjonowaniem infrastruktury, poprzez przetwarzanie danych, po zapewnienie prawidłowego działania aplikacji. Rozwiązaniem pośrednim między IaaS a SaaS jest *Platforma as a Service* (dalej: PaaS)[12]. Model PaaS jest wykorzystywany przez użytkowników do budowania (i zwykle wdrażania) aplikacji, tworzonych w językach programowania i narzędziach wspieranych przez dostawcę infrastruktury[13]. Zdarza się, że dostawcy

---

dużą skalę i bezpieczeństwo danych, (w:) G. Szpor (red.), *Internet. Cloud computing. Przetwarzanie w chmurach*, Warszawa 2013, rozdz. 1, s. 15–16.

[9] Zob. szerzej: M. Kutyłowski, *Technologie bezpieczeństwa dla przetwarzania w chmurze*, (w:) G. Szpor (red.), *Internet. Cloud computing. Przetwarzanie w chmurach*, rozdz. 1, s. 6; G. Haibach, *Cloud computing and European Union private international law*, „Journal of Private International Law" 2015, Vol. 11, issue 2, s. 254; S. A. Zargari, A. Smith, *Policing as a Service in the Cloud*, „Information Security Journal: A Global Perspective" 2014, Vol. 23, issue 4–6, s. 149–150; J. F. S. R Cunha, C. A. Rohrmann, *Some Legal Aspects of Cloud Computing Contracts*, „Journal of International Commercial Law and Technology" 2015, Vol. 10, issue 1, s. 39.

[10] Ten model usługi jest dla przykładu oferowany przez Amazon Web Service, Amazon Elastic Compute Cloud, Amazon Simple Storage Service S3.

[11] Przykładami tej formy przetwarzania w chmurach jest Gmail, Yahoo Mail, Google Apps i Office Web Application Microsoftu, Salesforce CRM oraz SAP Business by Design.

[12] Przykładami platform chmurowych PaaS na dużą skalę są Google AppEngine, Force.com oraz Windows Azure.

[13] S. A. Zargari, A. Smith, *Policing*…, s. 149; K. McGillivray, *Conflicts in the Cloud*..., s. 223; C. Osterwalder, *Przetwarzanie na dużą skalę*..., s. 16–18; G. Haibach, *Cloud computing and European Union*..., s. 253; M. Kutyłowski, *Technologie bezpieczeństwa*..., s. 7. Zob. więcej na temat

usług w chmurze dostarczają usługi łączące cechy różnych modeli. Przykładem jest sytuacja, w której dostawca oferujący oprogramowanie w modelu SaaS nie posiada własnej infrastruktury serwerowej i nabywa ją od innego podmiotu w modelu IaaS. W takim przypadku jest on z jednej strony użytkownikiem usługi IaaS, a z drugiej świadczy usługi w modelu SaaS. Może być też tak, że dostawca udostępnia w formie usługi aplikację dostosowaną do potrzeb klienta i świadczy dla niej usługi wsparcia technicznego, zarządzania aplikacją oraz dostarcza aktualizacje[14].

ASPEKTY BEZPIECZEŃSTWA ORAZ ZAPEWNIENIA ZGODNOŚCI Z OBOWIĄZUJĄCYMI PRZEPISAMI PRAWA W ZAKRESIE PRZETWARZANIA DANYCH

Korzyści oferowane przez rozwiązania w chmurze obliczeniowej są nie do przecenienia. Z drugiej jednak strony, pojawiają się obawy o bezpieczeństwo tego środowiska, w szczególności o ochronę danych przechowywanych na dzielonym zasobie sieciowym przed ich nieuzasadnionym ujawnieniem (świadomym czy też przypadkowym), dostępem osób nieautoryzowanych, nieuprawnionym kopiowaniem, wykorzystaniem, modyfikacją, zniszczeniem lub kradzieżą.

Temat bezpieczeństwa sieci i informacji podjęty został przez instytucje Unii Europejskiej. Przykładem działań na tym polu jest chociażby powołanie do życia Agencji ds. Bezpieczeństwa Sieci i Informacji (dalej: ENISA). Wśród licznych zadań ENISA na uwagę zasługuje przyczynianie się do wzrostu wiedzy na temat bezpieczeństwa sieci m.in. poprzez promowanie wymiany najlepszych praktyk, śledzenie rozwoju norm bezpieczeństwa produktów i usług oraz promowanie podejmowania działań z zakresu oceny ryzyka i zarządzania nim. Agencja ds. Bezpieczeństwa Sieci i Informacji uczestniczy również w wysiłkach Unii Europejskiej zmierzających do współpracy z krajami trzecimi i organizacjami międzynarodowymi celem promowania globalnej propozycji dotyczącej bezpieczeństwa.

Biorąc pod uwagę zaawansowane narzędzia ochrony wdrażane w rozwiązaniach chmurowych oraz wysokiej klasy specjalistów angażowanych do zapewnienia prawidłowej pracy tych systemów, przeniesienie usług do chmury obliczeniowej powinno (teoretycznie) zapewnić wysoki poziom bezpieczeństwa[15]. Nie każdy przedsiębiorca może sobie pozwolić na samodzielny zakup tak

różnic między wyżej wymienionymi modelami przedstawione przez ENISA w: Exploring Cloud Incidents, June 2016, s. 3 i 4, https://www.enisa.europa.eu/publications/exploring-cloud-incidents (dostęp: 11.07.2016 r.).

[14] J. F. S. R. Cunha, C. A. Rohrmann, *Some Legal Aspects*..., s. 40.

[15] Zob. szerzej: C. Osterwalder, *Przetwarzanie na dużą skalę*..., rozdz. 1, s. 21–23.

zaawansowanych i kosztownych narzędzi czy pozyskanie wysoko wykwalifikowanych specjalistów.

Standardem staje się posiadanie przez dostawców usług w chmurze certyfikatu na zgodność z normą ISO/IEC 27000:2009, która jest międzynarodową normą opracowaną dla zarządzania bezpieczeństwem informacji[16]. Środki bezpieczeństwa mają gwarantować dostępność danych oraz związanych z nimi usług, identyfikację klienta, ochronę danych w trakcie transferu oraz bezpieczeństwo całej infrastruktury[17]. Zazwyczaj nieodłącznym elementem strategii bezpieczeństwa są plany przywracania dostępności usługi w przypadku wystąpienia awarii (ang. *disaster recovery plans*)[18].

Faza negocjacji przedkontraktowych to odpowiedni moment na skierowanie do dostawcy prośby o udostępnienie dokumentów, które zawierają informacje o środkach technicznych oraz procedurach zarządzania danymi w poszczególnych centrach przetwarzania danych. Dostawcy niechętnie ujawniają takie informacje z obawy, że wpłynie to na osłabienie ochrony. Z drugiej jednak strony, użytkownicy oczekują, że dostawca będzie w stanie wykazać, że zostały przez niego podjęte odpowiednie środki techniczne i organizacyjne, aby zapewnić odporność i szczelność systemu.

W sytuacji, gdy mamy do czynienia z danymi osób fizycznych, przetwarzanie danych w środowisku chmury obliczeniowej musi odbywać się w sposób zgodny z obowiązującymi przepisami prawa. Warto w tym miejscu wskazać, że 27 kwietnia 2016 r. zostało przyjęte rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: rozporządzenie 2016/679)[19]. Nowe przepisy są odpowiedzią na potrzebę dopasowania przepisów o ochronie danych osobowych do zmian, jakie zaszły w związku z rozwojem technologii informatycznych oraz zapewnienia wysokiego i jednolitego poziomu ochrony danych osób fizycznych na terenie całej Unii Europejskiej. Rozporządzenie 2016/679 ma zastosowanie od dnia 25 maja 2018 r., zastępując w polskim porządku prawnym ustawę o ochronie danych osobowych z 1997 r.[20]. Na uwagę zasługują również inne akty prawne, które są dopełnieniem przepisów o ochronie danych osobowych, a odnoszące się do zagrożeń towarzyszących przetwarzaniu danych w Internecie. Chodzi o dyrektywę Parlamentu Europejskiego i Rady 2000/31/WE

[16] Por. również SSAE 16 typ II.

[17] Zob. szerzej np.: S. A. Zargari, A. Smith, *Policing*..., s. 153–154; J. F. S. R. Cunha, C. A. Rohrmann, *Some Legal Aspects*..., s. 37–39.

[18] R. Burnett, P. Klinger, *Drafting and Negotiating*..., s. 429.

[19] Dz.Urz. UE L 119 z 4.5.2016, s. 1.

[20] Ustawa jest implementacją dyrektywy 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. UE L 281 z 23.11.1995, s. 31).

(dalej: dyrektywa o handlu elektronicznym)[21] oraz dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dalej: dyrektywa o prywatności i łączności elektronicznej)[22].

Przetwarzanie danych osobowych[23] w chmurze obliczeniowej z racji swego charakteru należy do operacji stwarzających szczególne ryzyko dla praw i wolności podmiotów danych. Cenne wytyczne dotyczące przetwarzania danych w tym środowisku zawierają dokumenty opracowane przez Grupę Roboczą Art. 29[24] (Opinia 5/2012 z 1.07.2012 r. (WP 196)[25], Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" z 16.02.2010 (WP 169)[26]) oraz Międzynarodową Grupę Roboczą ds. Ochrony Danych w Telekomunikacji (Memorandum Sopockie[27]). Opracowania te wskazują na zagrożenia związane z brakiem kontroli nad danymi osobowymi transferowanymi do systemów zarządzanych przez dostawcę usługi chmurowej, brak przejrzystości przetwarzania danych, konieczność zapewnienia środków technicznych i organizacyjnych w celu zagwarantowania dostępności, integralności, odizolowania danych, zapewnienia ich poufności oraz możliwości interwencji ze strony podmiotu, którego dane dotyczą. Dokumenty te przedstawiają zalecenia, wytyczne i rekomendacje odnośnie do dobrych praktyk.

Jednym z celów europejskiej reformy danych osobowych było wprowadzenie jednolitych obowiązków oraz zadań po stronie administratora i podmiotów przetwarzających. Należy jednak zwrócić uwagę, że nowe przepisy nie rozwiązują wszystkich problemów interpretacyjnych, jakie powstają w praktyce przetwarzania danych osobowych w środowisku chmury obliczeniowej. Wątpliwości dotyczą np. przypisania właściwego statusu dla dostawcy usług w chmurze, tj. czy

---

[21] Dz.Urz. UE L 178 z 17.7.2000, s. 1. Stosownie do art. 2 ust. 4 oraz motywu 21 rozporządzenia 2016/679, przepisy o ochronie danych osobowych pozostają bez uszczerbku dla stosowania dyrektywy o handlu elektronicznym.

[22] Dz.Urz. UE L 201 z 31.7.2002, s. 37. Zob. również art. 95 rozporządzenia 2016/679.

[23] Stosownie do definicji „przetwarzanie" podanej w rozporządzeniu 2016/679, „przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie".

[24] Jest to podmiot o charakterze doradczym ustanowiony na podstawie art. 29 dyrektywy 95/46/WE. Z kolei na mocy rozporządzenia 2016/679 Grupa Robocza Art. 29 zostaje zastąpiona Europejską Radą Ochrony Danych (EROD).

[25] Opinia 5/2012 Grupy Roboczej Art. 29, http://www.giodo.gov.pl/1520111/id_art/4760/j/pl (dostęp: 29.12.2017 r.).

[26] Opinia 1/2010 Grupy Roboczej Art. 29, http://www.giodo.gov.pl/1520057/id_art/3595/j/pl/ (dostęp: 29.12.2017 r.).

[27] Memorandum Sopockie, http://www.giodo.gov.pl/1520035/j/pl/ (dostęp: 29.12.2017 r.).

dostawca usługi w chmurze działa jako podmiot przetwarzający czy również jako administrator danych. W literaturze przedmiotu podawane są przykłady, w których rozstrzygnięcie tej kwestii nie zawsze jest jednoznaczne (np. czy udostępnienie infrastruktury informatycznej powinno być zaklasyfikowane jako przetwarzanie danych osobowych)[28]. Ponadto, w przywołanej wyżej Opinii 5/2012 (WP196) przytaczane są okoliczności, w których dostawca usług w chmurze może być uznany za administratora[29].

Przepisy rozporządzenia 2016/679 nakładają na administratora i podmiot przetwarzający obowiązki wdrożenia odpowiednich środków technicznych oraz organizacyjnych celem zapewnienia poziomu bezpieczeństwa przetwarzania danych odpowiedniego do istniejącego ryzyka naruszenia praw lub wolności osób fizycznych[30]. Jednak biorąc pod uwagę fakt, że dostawcami usług w chmurze obliczeniowej są zazwyczaj międzynarodowe podmioty, które ustalają i wdrażają jednolite zasady bezpieczeństwa dla oferowanych przez nich rozwiązań, wpływ administratora danych na strategie bezpieczeństwa wdrażane przez dostawcę jest niewielki, tym samym możliwości wypełnienia niektórych wymagań nałożonych na administratora przepisami o ochronie danych osobowych są utrudnione[31]. Jako dobrą praktykę należy wskazać stosowanie przez dostawców usług w chmurze zatwierdzonych kodeksów postępowania[32] oraz mechanizmów certyfikacji, potwierdzających wypełnianie przez przedsiębiorcę przepisów o ochronie danych osobowych[33].

Właściwe ustalenie podmiotu będącego administratorem danych osobowych ma fundamentalne znaczenie dla wypełnienia obowiązków notyfikacyjnych wprowadzonych rozporządzeniem 2016/679 w związku z koniecznością zapewnienia transparentności i rzetelności przetwarzania danych osobowych oraz obowiązkami po stronie administratora dotyczącymi ułatwiania osobie, której dane dotyczą, korzystania z praw jej przysługujących[34]. W zakres ten wchodzą m.in.: prawo osoby do uzyskania dostępu do danych osobowych jej dotyczących, uzyskania informacji o zastosowaniu odpowiednich zabezpieczeń w przypadku, gdy dane przekazywane są do kraju trzeciego lub organizacji międzynarodowej,

[28] Zob. szerzej np.: P. Dynowski, I. Kowalczuk-Pakuła, G. Pacek, *Poradnik prawny dla e-biznesu*, Warszawa 2016, s. 123–124; R. Burnett, P. Klinger, *Drafting and Negotiating...*, s. 433; opracowanie DLA Piper UK LLP, *Comparative Study on Cloud Computing Contracts. Final Report*, 2015, s. 40, http://bookshop.europa.eu/en/comparative-study-on-cloud-computing-contracts-pbDS0115164/ (dostęp: 29.12.2017 r.).

[29] Por. również art. 28 ust. 10 rozporządzenia 2016/679.

[30] Art. 32 rozporządzenia 2016/679. Zob. szerzej: W. R. Wiewiórowski, *Prawne aspekty udostępniania usług administracji publicznej w modelu chmury*, (w:) G. Szpor (red.), *Internet. Cloud computing. Przetwarzanie w chmurach*, rozdz. 3, s. 107 i 108.

[31] K. Biczysko-Pudełko, *Znaczenie soft law...*, s. 227.

[32] Zob. art. 40 rozporządzenia 2016/679.

[33] Zob. art. 42–43 rozporządzenia 2016/679.

[34] Chodzi o korzystanie z praw wymienionych w art. 15–22 rozporządzenia 2016/679.

prawo do sprostowania i usuwania danych, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych. Nowe przepisy wprowadziły również obowiązek notyfikacji do organu nadzorczego incydentów, w których miało miejsce naruszenie ochrony danych osobowych[35], a w sytuacji, gdy naruszenie ochrony danych osób fizycznych może skutkować powstaniem wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, administrator zobowiązany jest również powiadomić podmiot danych. Ponadto, na mocy rozporządzenia 2016/679 wzmocnieniu ulega dotychczasowe „prawo do bycia zapomnianym". Pojawił się dodatkowy obowiązek po stronie administratora, który upublicznił dane osobowe. W świetle nowych przepisów jest on zobowiązany do podjęcia rozsądnych działań celem poinformowania innych administratorów przetwarzających o żądaniu osoby, której dane dotyczy, aby usunęli oni wszelkie łącza do jej danych, jak również kopie tych danych lub ich replikacje[36].

Stosowanie zastrzeżonej technologii uniemożliwiającej użytkownikom przenoszenie danych między różnymi systemami chmurowymi (tzw. syndrom *vendor lock-in*) jest często podnoszonym zastrzeżeniem kierowanym pod adresem dostawców rozwiązań w chmurze obliczeniowej. Kwestia ta została uregulowana przez prawodawcę unijnego w art. 20 rozporządzenia 2016/679, stosowanie do którego osoba, której dane dotyczą, ma prawo do otrzymania „w ustrukturyzowanym, powszechnie używanym formacie, nadającym się do odczytu maszynowego, dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi".

Dostawca usług w chmurze (przetwarzający) może mieć siedzibę w Polsce, ale jego centrum przetwarzania danych może być zlokalizowane poza Europejskim Obszarem Gospodarczym lub korzystać z podwykonawców, których serwery będą umieszczone w kraju trzecim. Należy jednak pamiętać, że jeśli powierzane dane podlegają reżimowi przepisów o ochronie danych osobowych, dostarczyciel usługi w chmurze, przed powierzeniem przetwarzania danych innemu podmiotowi (podprzetwarzającemu), musi uzyskać pisemną zgodę administratora danych[37]. Warto w tym miejscu zaznaczyć, że rozporządzenie 2016/679 rozszerzyło terytorialny zakres stosowania unijnych przepisów o ochronie danych osób fizycznych[38]. Rozporządzenie 2016/679 ma zastosowanie do przetwarzania

[35] Zob. art. 33 rozporządzenia 2016/679. Stosownie do definicji zawartej w rozporządzeniu 2016/679 „naruszenie ochrony danych osobowych" jest rozumiane jako: „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych".

[36] Zob. szerzej na temat prawa do bycia zapomnianym w: P Litwiński, *Nowe rozporządzenie ogólne w sprawie ochrony danych osobowych i jego wpływ na społeczeństwo informacyjne. Wybrane zagadnienia*, (w:) K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne: współczesne problemy prawne*, Warszawa 2016, s. 150–151.

[37] Zob. więcej: W. R. Wiewiórowski, *Prawne aspekty…*, rozdz. 3, s. 111–112.

[38] Zob. art. 3 rozporządzenia 2016/679.

danych osobowych w przypadku, gdy jednostka organizacyjna administratora lub podmiotu przetwarzającego prowadzą działalność w Unii, bez względu na to czy przetwarzanie odbywa się na terenie Unii Europejskiej oraz do przetwarzania danych osób fizycznych przebywających w Unii Europejskiej przez administratora lub podmiot przetwarzający, nawet jeśli nie mają oni jednostek organizacyjnych na terenie Unii Europejskiej, w przypadku, gdy podmioty te przetwarzają dane osób przebywających na obszarze Unii Europejskiej, w związku z oferowaniem tym osobom towarów lub usług, bez względu na to czy są to towary i usługi wymagające zapłaty czy też nie[39].

Podstawową przesłanką przekazania danych osobowych na serwer znajdujący się w kraju trzecim lub organizacji międzynarodowej jest zapewnienie ochrony danych osobowych przynajmniej na poziomie odpowiadającym ochronie przysługującej w Unii Europejskiej[40]. Rozporządzenie 2016/679 określa podstawy dopuszczalnego transferu danych osobowych do państw trzecich lub organizacji międzynarodowych[41]. Możliwości jest kilka. Natomiast do najbardziej powszechnych w użyciu należą standardowe klauzule umowne, których wzorce zostały zatwierdzone przez Komisję Europejską w formie decyzji[42], oraz wiążące reguły korporacyjne (ang. *Binding Corporate Rules*). Komisja Europejska jest uprawniona do wydania decyzji, na mocy której państwo czy organizacja spoza Europejskiego Obszaru Gospodarczego zostaną uznane za zapewniające odpowiedni poziom ochrony danych osobowych, wskazując jednocześnie, które kategorie danych osobowych mogą być transferowane na podstawie takiej decyzji[43].

Odrębnego omówienia wymaga przekazywanie danych do podmiotów działających na terenie Stanów Zjednoczonych. Do niedawna, na mocy decyzji Komisji Europejskiej 2000/520/WE z dnia 26 lipca 2000 r., podmioty amerykańskie uczestniczące w programie *Safe Harbor* były traktowane jako zapewniające poziom ochrony danych osobowych zgodny z prawem unijnym. Przystąpienie do programu automatycznie klasyfikowało przedsiębiorców amerykańskich jako zapewniających odpowiedni poziom ochrony. Ostatecznie jednak, wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 6 października 2015 r., C-362/14, *Maximillian Schrems v Data Protection Commissioner*[44], unieważnił decyzję Komisji Europejskiej 2000/520/WE z dnia 26 lipca 2000 r.[45] Obecnie przedsiębiorcy, przesyłając dane do Stanów Zjednoczonych, są zobowiązani do uregu-

[39] Zob. również art. 3 ust. 3 rozporządzenia 2016/679.

[40] Por. B. Fischer, *Ochrona prywatności*..., rozdz. 5, s. 221–222.

[41] Zob. rozdział V rozporządzenia 2016/679.

[42] Decyzja Komisji z dnia 5 lutego 2010 r. (2010/87/UE). Standardowe klauzule umowne są dostępne na stronie GIODO: http://www.giodo.gov.pl/163/id_art/1519/j/pl/.

[43] Zob. szerzej: http://www.giodo.gov.pl/163/id_art/1519/j/pl/.

[44] Zob. http://curia.europa.eu/juris/document/document.jsf?docid=172254&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=PL&cid=97913 (dostęp: 29.12.2017 r.).

[45] Zob. szerzej: P. Dynowski, I. Kowalczuk-Pakuła, G. Pacek, *Poradnik*..., s. 187.

lowania współpracy z odbiorcami danych w Stanach Zjednoczonych w sposób przewidziany przez przepisy unijne.

Kolejne zagadnienie, które zasługuje chociażby na zasygnalizowanie, dotyczy zobowiązań dostawców chmury obliczeniowej w stosunku do policji, służb specjalnych czy organów ścigania w zakresie przekazywania im dostępu do danych zamieszczonych w chmurze obliczeniowej. Użytkownik chmury powinien posiadać informacje, w jakim kraju dane będą przetwarzane, aby móc zaznajomić się z krajowymi regulacjami w tym zakresie. Wymaganie to dotyczy również wszystkich podwykonawców dostawcy. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. ustanawia minimalne standardy dotyczące przetwarzania danych na potrzeby policji we wszystkich państwach członkowskich.

KLAUZULE KONTRAKTOWE CHARAKTERYSTYCZNE DLA USŁUG W MODELU CHMURY OBLICZENIOWEJ

Chociaż rynek usług oferowanych w chmurze obliczeniowej nie jest nowy, nie ma jeszcze jednolitego podejścia odnośnie do konstrukcji prawnych stosowanych do rozwiązań oferowanych w modelu chmury obliczeniowej[46]. Z uwagi na złożoność i rozległość tematu analiza tych zagadnień w sposób wyczerpujący nie jest możliwa w ramach niniejszej pracy. Celem artykułu jest natomiast wskazanie najbardziej charakterystycznych postanowień umownych dla relacji kontraktowej między użytkownikiem (klientem) a dostawcą usług w chmurze (ang. *Cloud Services Provider*).

W literaturze przedmiotu poruszana jest konieczność podjęcia działań celem opracowania wzorca umownego dla usług dostępnych w modelu chmury obliczeniowej. Obecna praktyka kontraktowa wskazuje bowiem, że dostawcy narzucają standardowe warunki umowne skonstruowane na zasadzie *provider-favorable*, nie pozostawiając zbyt wiele miejsca na negocjacje (*take-it-or-leave-it*).

Spośród postanowień kontraktowych charakterystycznych dla usług w chmurze obliczeniowej na szczególną uwagę i konieczność uregulowania umownego zasługują takie kwestie, jak: minimalne paramenty świadczenia usług, wsparcie techniczne, zapewnienie integralności danych, zobowiązania do zachowania poufności, podwykonawstwo, zakres odpowiedzialności dostawcy z tytułu nie-

[46] Zob. szerzej: DLA Piper UK LLP, *Comparative Study on Cloud Computing Contracts*..., rozdz. 2.3.2, s. 26–29; K. Żok, *Kwalifikacja umowy o korzystanie z programu komputerowego jako usługi (Software as a Service*, *SaaS) – uwagi na tle prawa polskiego i wybranych zagranicznych systemów prawnych*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2012, z. 3, s. 19 i n.

wykonania lub nienależytego wykonania zobowiązań kontraktowych, możliwość jednostronnej zmiany umowy przez dostawcę, warunki rozwiązania kontraktu, zabezpieczenie danych po zakończeniu umowy, obowiązki związane z ochroną danych osobowych, prawo właściwe[47]. Podobny katalog kluczowych postanowień umownych został zdefiniowany przez ENISA[48].

Standardem, co prawda, stają się procedury wykonywania przez dostawcę kopii zapasowych (ang. *backup*), nie zmienia to jednak faktu, że uregulowanie tych obowiązków *expressis verbis* w kontrakcie wraz z określeniem, która strona ponosi odpowiedzialność za utratę danych, jest niezwykle istotne.

Użytkownicy oczekują, że usługi przetwarzania w chmurze obliczeniowej będą świadczone na odpowiednim poziomie. Minimalne parametry oraz warunki świadczenia są zazwyczaj określane w tzw. *Service Level Agreement* (dalej: SLA)[49]. W przypadku usług przetwarzania w modelu chmury obliczeniowej parametrem podstawowym jest poziom gwarantowanej dostępności czasowej usługi ustalany przeważnie na poziomie między 97% a 99%[50], mierzonej najczęściej dla okresów miesięcznych lub dłuższych, nierzadko powiązanych z okresem rozliczeniowym lub okresem trwania umowy. Dobrą praktyką jest, aby w SLA został określony zakres odpowiedzialności dostawcy z tytułu niewykonania lub nienależytego wykonania umowy[51]. Praktyka kontraktowa wskazuje, że odszkodowanie jest zazwyczaj ustanawiane w formie tzw. *service credits*, którego wysokość jest z góry określana i powiązana ze stopniem naruszenia minimalnych parametrów SLA[52]. Brak jest jednak jednolitego podejścia odnośnie do ograniczeń odpowiedzialności odszkodowawczej dostawcy usług chmurowych, w szczególności, czy użytkownik zachowuje prawo dochodzenia odszkodowania przekraczającego wartość *service credits*[53]. Odnośnie do samego *service credits* dostawcy zazwyczaj ograniczają okoliczności uprawniające do przyznania tejże rekompensaty, zastrzegając np. że nie ponoszą odpowiedzialności za zdarzenia,

---

[47] W. Kuan Hon, Ch. Millard, I. Walden, *Negotiating Cloud Contracts: Looking at Clouds from both sides now*, „Stanford Technology Law Review" 2012, Vol. 16, issue 1, s. 92 i n.; S. A. Zargari, A. Smith, *Policing*..., pkt 3 i 4, s. 150 i n.; Eversheds in conjunction with The Lawyer Research Service, *Spotlight on the cloud: Highlighting industry trends*, The Lawyer 2016, s. 31.

[48] Zob. szerzej: *Cloud Computing: Benefits*, *risks and recommendations for information security*, 2009, s. 97 i n., https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport (dostęp: 29.12.2017 r.).

[49] Zob. szerzej na temat SLA w: opracowaniu DLA Piper UK LLP, *Comparative Study on Cloud Computing Contracts*..., s. 29–36; J. Wilczewski, *Gwarancja Jakości Świadczonych Usług (Service Level Agreement) jako szczególny rodzaj odpowiedzialności*, Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, Wrocław 2004, www.bibliotekacyfrowa.pl/Content/24715/Gwarancja_Jakosci_Swiadczon.pdf (dostęp: 18.07.2016 r.).

[50] J. F. S. R. Cunha, C. A. Rohrmann, *Some Legal Aspects*..., s. 42.

[51] Zob. szerzej w rozdz. 2.3.7 „Warranties and liability" DLA Piper UK LLP, *Comparative Study on Cloud Computing Contracts*..., s. 44–51.

[52] DLA Piper UK LLP, *Comparative Study on Cloud Computing Contracts*..., s. 22–23.

[53] *Ibidem*, s. 10.

które są poza ich kontrolą (np. przyczyna niedostępności systemu leży po stronie systemów klienta, niedostępności sieci, nieprzewidzianych przeciążeń ruchu w sieci). Częstą praktyką jest również zastrzeganie oznaczonego czasu, w którym użytkownik jest uprawniony do ubiegania się o *service credits*[54].

Dostawcy zazwyczaj posługują się różnego rodzaju instrumentami prawnymi, takimi jak polityki prywatności, kodeksy postępowania[55] czy warunki korzystania z usługi (ang. *Acceptable Use Policy*, AUP)[56].

Kontrakt najczęściej jest zawierany na minimalny czas oznaczony, który trwa od roku do lat trzech, oraz zawiera postanowienia co do możliwości i sposobu przedłużenia relacji kontraktowej[57].

PODSUMOWANIE

Zaawansowanie technologiczne chmury obliczeniowej oraz złożoność tego rozwiązania nie są „widoczne" dla użytkownika usługi w chmurze, jeżeli rozwiązanie działa poprawnie. Natomiast wystąpienie jakiejkolwiek awarii czy problemu jest odczuwalne w znacznym stopniu, sprawiając, że usługa, która w swoim założeniu ma być źródłem wymiernych korzyści biznesowych, może być przyczyną strat i sporów. Dlatego tak ważne jest, aby wybór dostawcy usług w modelu chmury obliczeniowej został poprzedzony rozważeniem wielu aspektów technicznych i prawnych oraz możliwie najpełniejszym uregulowaniem w umowie praw i obowiązków stron. Podejmując starania, aby przetwarzanie w chmurze było bardziej bezpieczne, przewidywalne i oferowane na uczciwych zasadach kontraktowych, możemy przyczynić się do poprawy zaufania do usług przetwarzania w chmurze, a tym samym do ich stosowania na większą skalę.

BIBLIOGRAFIA

Biczysko-Pudełko K., *Znaczenie soft law dla regulacji cloud computing*, (w:) K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne: współczesne problemy prawne*, Warszawa 2016

Burnett R., Klinger P., *Drafting and Negotiating IT Contracts*, Bloomsbury Professional 2013

[54] W. Kuan Hon, Ch. Millard, I. Walden, *Negotiating Cloud Contracts*..., s. 97.

[55] K. McGillivray, *Conflicts in the Cloud*..., s. 218.

[56] Por. DLA Piper UK LLP, *Comparative Study on Cloud Computing Contracts*..., s. 9.

[57] Zob. szerzej: W. Kuan Hon, Ch. Millard, I. Walden, *Negotiating Cloud Contracts*..., s. 119–121.

Cunha J. F. S. R., Rohrmann C. A., *Some Legal Aspects of Cloud Computing Contracts*, „Journal of International Commercial Law and Technology" 2015, Vol. 10, issue 1

DLA Piper UK LLP, *Comparative Study on Cloud Computing Contracts. Final Report*, 2015, http://bookshop.europa.eu/en/comparative-study-on-cloud-computing-contracts-pbDS0115164/ (dostęp: 9.07.2016 r.)

Dynowski P., Kowalczuk-Pakuła I., Pacek G., *Poradnik prawny dla e-biznesu*, Warszawa 2016

Eversheds in conjunction with The Lawyer Research Service, *Spotlight on the cloud: Highlighting industry trends*, The Lawyer 2016

Fischer B., *Ochrona prywatności i wykorzystanie instrumentów samoregulacji w modelu cloud computingu*, (w:) G. Szpor (red.), *Internet. Cloud computing. Przetwarzanie w chmurach*, Warszawa 2013

Grance T., Mell P., *The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology*, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Special Publication 800–145, 2011

Haibach G., *Cloud computing and European Union private international law*, „Journal of Private International Law" 2015, Vol. 11, issue 2

Hołyst B., Pomykała J., *Cyberprzestępczość*, *ochrona informacji i kryptologia*, „Prokura i Prawo" 2011, nr 1

Krzysztofek M., *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, Warszawa 2015

Kuan Hon W., Millard Ch., Walden I., *Negotiating Cloud Contracts: Looking at Clouds from both sides now*, „Stanford Technology Law Review" 2012, Vol. 16, issue 1

Kutyłowski M., *Technologie bezpieczeństwa dla przetwarzania w chmurze*, (w:) G. Szpor (red.), *Internet. Cloud computing. Przetwarzanie w chmurach*, Warszawa 2013

Litwiński P., *Nowe rozporządzenie ogólne w sprawie ochrony danych osobowych i jego wpływ na społeczeństwo informacyjne. Wybrane zagadnienia*, (w:) K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne: współczesne problemy prawne*, Warszawa 2016

McGillivray K., *Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU*, „Tulane Journal of Technology and Intellectual Property" 2014, Vol. 17

Mell P., Grance T., *The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology*, *Computer Security Division*, *Information Technology Laboratory*, *National Institute of Standards and Technology*, National Institute of Standards and Technology, September 2011

Osterwalder C., *Przetwarzanie na dużą skalę i bezpieczeństwo danych*, (w:) G. Szpor (red.), *Internet. Cloud computing. Przetwarzanie w chmurach*, Warszawa 2013

Wiewiórowski W. R., *Prawne aspekty udostępniania usług administracji publicznej w modelu chmury*, (w:) G. Szpor (red.), *Internet. Cloud computing. Przetwarzanie w chmurach*, Warszawa 2013

Wilczewski J., *Gwarancja jakości świadczonych usług (Service Level Agreement) jako szczególny rodzaj odpowiedzialności*, Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, Wrocław 2004

Zargari S. A., Smith A., *Policing as a Service in the Cloud*, „Information Security Journal: A Global Perspective" 2014, Vol. 23, issue 4–6

Żok K., *Kwalifikacja umowy o korzystanie z programu komputerowego jako usługi (Software as a Service, SaaS) – uwagi na tle prawa polskiego i wybranych zagranicznych systemów prawnych*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2015, nr 3

SECURITY AND LEGAL ASPECTS OF DATA PROCESSING IN THE CLOUD COMPUTING

Summary

Many issues need to be considered and tackled before moving data into the cloud. Adoption of cloud computing raises concerns and questions in particular with respect to security, control and privacy in cloud computing environment. Users should be aware where their data will be stored and what law governs. In a case where personal data are to be processed it is important for the contracting parties to ensure that requirements and obligations placed on them pursuant to the EU data protection laws will be fulfilled.

This article also includes an overview of typical terms and conditions of cloud computing contracts, stressing that most of contractual arrangements in current practice fall short of achieving a fair balance of rights and obligations arising under the contract between cloud providers and users. The aim of this study is to indicate regulations and guidelines which are applicable to cloud computing contracts as well as initiatives undertaken at the EU level and their role in building legal certainty and trust to cloud computing technology.

KEYWORDS

cloud computing, EU law, data protection, data security, privacy, *Service Level Agreements*

SŁOWA KLUCZOWE

przetwarzanie w chmurze, prawo UE, ochrona danych, bezpieczeństwo danych, prywatność, *Service Level Agreements*