Damian Karwala

Chmura obliczeniowa a nowa ustawa o działalności ubezpieczeniowej i reasekuracyjnej

Usługi informatyczne, świadczone w modelu tzw. chmury obliczeniowej (ang. *cloud computing*) zyskują coraz większą popularność, również w sektorze ubezpieczeniowym. W przepisach prawa, w tym w ustawie o działalności ubezpieczeniowej i reasekuracyjnej z 11 września 2015 r., brak jest zakazu korzystania z tego rodzaju rozwiązań. Analiza dopuszczalności oraz warunków korzystania z usług *cloud computing* wymaga uwzględnienia zatem, po pierwsze, aspektu związanego z przetwarzaniem w ramach chmury obliczeniowej danych osobowych oraz danych objętych tajemnicą ubezpieczeniową. Po drugie, istotna dla oceny jest problematyka związana z outsourcingiem w działalności ubezpieczeniowej, szczególnie po wprowadzeniu nowej europejskiej regulacji ubezpieczeniowej (Wypłacalność II), która budzi jednak pewne wątpliwości interpretacyjne i praktyczne (poza przedmiotem zainteresowania pozostawiono działalność reasekuracyjną). W niniejszym artykule podjęto próbę analizy tego szczególnego modelu korzystania z rozwiązań IT na gruncie ww. regulacji.

Słowa kluczowe: chmura obliczeniowa, tajemnica ubezpieczeniowa, outsourcing w działalności ubezpieczeniowej, ustawa o działalności ubezpieczeniowej i reasekuracyjnej.

1. Uwagi wprowadzające

Usługi i rozwiązania informatyczne, dostarczane (świadczone) w tzw. chmurze obliczeniowej (ang. *cloud computing*) zyskują coraz większą popularność w wielu sektorach gospodarki. Trend ten nie omija podmiotów z sektora ubezpieczeniowego, które korzystają z zasobów obliczeniowych (w tym z systemów i aplikacji) podmiotów zewnętrznych, oferowanych także przez podmioty mające swe siedziby w państwach nienależących do Unii Europejskiej, w szczególności w Stanach Zjednoczonych. Dotychczasowa ustawa z dnia 22 maja 2003 r. o działalności ubezpieczeniowej, jak również nowa ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (dalej: u.d.u.r.)[1] nie odnoszą się w żaden sposób wprost do kwestii korzystania przez zakłady ubezpieczeń z usług świadczonych w chmurze. Co jednak istotne, w przepisach prawa nie ma zakazu korzystania z tego rodzaju rozwiązań. Z opracowanych przez Komisję Nadzoru Finansowego „Wytycznych dotyczących zarządzania obszarami technologii informacyjnej bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji" wyprowadzić należy wniosek przemawiający za dopuszczalnością korzystania z usług chmurowych przez zakłady ubezpieczeń[2]. Tym samym analiza dopuszczalności oraz warunków korzystania z usług *cloud computing*, co stano-

[1] Dz. U. z 2015 r. poz. 1844 (ogłoszona 10.11.2015 r.).
[2] Wytyczne KNF z dnia 16 grudnia 2014 r. (dalej: Wytyczne KNF), por. pkt 10.6., s. 37.

wi cel i przedmiot niniejszego artykułu, wymaga uwzględnienia następujących zagadnień:

- aspektu związanego z przetwarzaniem w ramach chmury danych osobowych oraz danych objętych tajemnicą ubezpieczeniową z uwagi na to, że w modelu tym przetwarzane mogą być (i w praktyce często są przetwarzane) dane osobowe ubezpieczających, ubezpieczonych, uposażonych lub uprawnionych z umowy ubezpieczenia, w tym dane dotyczące umów ubezpieczenia;
- problematyki związanej z outsourcingiem w działalności ubezpieczeniowej, co po wprowadzeniu regulacji z 11 września 2015 r. budzi dodatkowe wątpliwości interpretacyjne i praktyczne – z reguły bowiem usługi „chmurowe" świadczone są przez zewnętrznych dostawców, zarówno w ramach modelu tzw. chmury prywatnej (tj. infrastruktury, serwerów, wykorzystywanych wyłącznie przez określonego klienta), jak i tzw. chmury publicznej, która zakłada współdzielenie określonej infrastruktury (serwerów) przez wiele podmiotów (klientów)[3].

2. Modele chmury obliczeniowej

Pojęcie chmura obliczeniowa (tzw. usługi chmurowe, *cloud computing*) nie występuje w języku prawnym, w tym w przepisach regulujących rynek ubezpieczeniowy. W doktrynie prawniczej powszechnie wykorzystuje się definicję przyjętą przez amerykański Narodowy Instytut Standaryzacji i Technologii (*National Institute of Standards and Technology*), zgodnie z którą *cloud computing* jest modelem korzystania z rozwiązań IT zapewniającym wszechobecny, wygodny i możliwy na żądanie dostęp za pośrednictwem sieci do dzielonych zasobów obliczeniowych (np. serwery, aplikacje). Model ten charakteryzuje się pięcioma podstawowymi cechami:

1) dostępnością na żądanie (klient ma możliwość uzyskania nowych zasobów obliczeniowych w razie potrzeby, bez konieczności kontaktu osobowego z dostawcą);
2) nieograniczonym dostępem do usług (dostęp możliwy jest bowiem poprzez każde urządzenie z dostępem do Internetu, np. laptop, tablet, smartfon);
3) wspólnym korzystaniem z zasobów (ang. *resource pooling*), pozwalającym na dzielenie tych samych zasobów (infrastruktury, aplikacji) pomiędzy wielu użytkowników równocześnie;
4) elastycznością (zasoby są elastycznie zapewniane i uwalniane w zależności od potrzeb);
5) mierzalnością usługi (zakres i intensywność korzystania z danej usługi są monitorowane na bieżąco)[4].

Usługi *cloud computing'u* mogą być świadczone w różnych modelach, jako tzw.:

1) IaaS (ang. *Infrastructure as a Service*), w którym dostawca (ang. *cloud provider*) zobowiązuje się do zapewnienia określonej infrastruktury informatycznej (mocy obliczeniowej, pojemności serwerów itd.);
2) PaaS (ang. *Platform as a Service*), w którym dostawca udostępnia środowisko pracy (platformę informatyczną z określonymi bibliotekami, językami programowania itd.), umożliwiającą klientowi tworzenie własnych aplikacji;

---

[3] Do popularnych rozwiązań chmury publicznej należą m.in.: Amazon Web Services, Google Apps, Microsoft Azure oraz rozwiązania firmy Salesforce.

[4] Por. dokument *The NIST Definition of Cloud Computing*, dostępny pod adresem: http://csrc.nist.gov/ publications/ nistpubs/ 800-145/ SP800-145.pdf (9.10.2015), s. 2; zob. również E. Molenda-Kropielnicka, *Cloud Computing – zagadnienia prawne*, Prace z Prawa Własności Intelektualnej 2013, z.119, s. 111.

3) SaaS (ang. *Software as a Service*), w którym dostawca udostępnia określone oprogramowanie (aplikacje) działające w infrastrukturze (zasobach) chmury[5].

Jak wskazuje się w doktrynie, atrakcyjność *cloud computing'u*, jako modelu dystrybucji rozwiązań IT, związana jest w głównej mierze z aspektem finansowym. W modelu tym klient płaci bowiem jedynie za tyle, ile rzeczywiście wykorzystuje np. pojemności lub mocy obliczeniowej serwerów/procesorów, aplikacji itd. (ang. *pay as you go*). Ponadto rozwiązania informatyczne oferowane w chmurze *„są elastyczne i dostosowane do zmieniających się potrzeb klientów. Klient nie musi inwestować w hardware i software, gdyż gwarantuje je provider, który odpowiada za utrzymanie i bezpieczne funkcjonowanie całej infrastruktury"*[6].

3. Ochrona danych osobowych w chmurze obliczeniowej

Jak już wskazano, w związku z korzystaniem z usług chmurowych przez zakłady ubezpieczeń dochodzić może do przetwarzania danych osobowych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[7], np. danych osobowych ubezpieczających, ubezpieczonych, uposażonych lub uprawnionych z umowy ubezpieczenia. Co jednak istotne, uwzględniając przyjętą w art. 6 ustawy definicję, należy przyjąć, iż danymi osobowymi nie będą informacje, które nie pozwalają na identyfikację osoby fizycznej (por. dalsze uwagi w tym zakresie). Dodatkowo, wyjątkowo pojemna definicja „przetwarzania" danych obejmuje jakiekolwiek operacje wykonywane na danych osobowych, w tym ich przechowywanie, udostępnianie i usuwanie, zwłaszcza zaś te operacje, które wykonuje się w systemach informatycznych (art. 7 pkt 2 u.o.d.o.).

Pomimo występujących w tym zakresie wątpliwości[8], obecnie dominuje stanowisko, zgodnie z którym w analizowanym tu modelu **administratorem danych osobowych jest usługobiorca** (tj. zakład ubezpieczeń), korzystający z usług świadczonych w chmurze. Wątpliwości, które w tym zakresie występują, związane są w szczególności z tym, iż to z reguły dostawca usług (*cloud provider*) określa nie tylko środki służące do przetwarzania danych osobowych, lecz również wpływa na określenie celów, w jakich dane osobowe są przez klientów tego rodzaju usług przetwarzane (w pewnym sensie predefiniuje on te cele). W doktrynie słusznie podkreśla się jednak, że *„administratorem będzie ten, kto decyduje o celach i środkach przetwarzania, ale nie abstrakcyjnie, tylko w odniesieniu do konkretnych danych. Nie jest więc administratorem ten, kto tworzy aplikację komputerową, program, projekt, promocję (zakładającą określony cel i sposób przetwarzania danych), ale ten, kto zadecydował o przeznaczeniu konkretnych danych do przetwarzania w taki sposób"*[9]. Również w ocenie Grupy Roboczej Art. 29 to od *„klienta usług w chmurze zależy ostateczny cel przetwarzania i to on podejmuje decyzje dotyczące outsourcingu przetwarzania i delegowania organizacji ze-*

[5] Dokument *The NIST Definition of Cloud Computing*, dostępny pod adresem: http://csrc.nist.gov/ publications/ nistpubs/ 800-145/ SP800-145.pdf (9.10.2015), s. 2–3.
[6] E. Molenda-Kropielnicka, *Cloud Computing*…, s. 112.
[7] Tekst jedn. Dz. U. z 2014 r. poz. 1182; dalej: u.o.d.o.
[8] Por. m.in. P. Balboni, *Data Protection and Data Security Issues Related to Cloud Computing in the EU*, Tilburg University Legal Studies Working Paper Series, no. 022/2010, s. 5–7.
[9] A. Mednis, *Administrator danych i podmiot przetwarzający dane na zlecenie – status prawny, zakres praw i obowiązków, problemy definicyjne*, (w:) *Ochrona danych osobowych. Skuteczność regulacji,* G. Szpor (red.), C.H. Beck, Warszawa 2009, s. 82.

wnętrznej całej lub części działalności związanej z przetwarzaniem. Klient usług w chmurze działa zatem w charakterze administratora danych"[10].

Przyjęcie, że to usługobiorca usług chmurowych występuje jako administrator danych osobowych pociąga za sobą istotne konsekwencje. Regulacja art. 26 oraz art. 31 ustawy o ochronie danych osobowych pozwala bowiem na zajęcie stanowiska, iż **administrator danych może ponosić odpowiedzialność** w związku z realizacją ustawowych obowiązków bez względu na to, czy samodzielnie przetwarza dane osobowe, czy też posługuje się w tym celu podmiotem zewnętrznym, tzw. procesorem danych (w tym *cloud providerem*). Wniosek taki wyprowadzić można w szczególności z brzmienia art. 31 ust. 4 u.o.d.o., zgodnie z którym, w przypadku powierzenia innemu podmiotowi przetwarzania danych, odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na administratorze danych. Jak podkreśla w tym zakresie Generalny Inspektor Ochrony Danych Osobowych: *„w przypadku powierzenia przetwarzania danych innemu podmiotowi, administrator danych musi mieć świadomość, że nie zwalnia go to z odpowiedzialności za bezpieczeństwo i jakość tego przetwarzania"*[11]. W praktyce oznaczać to będzie, że administrator danych (klient usług chmurowych) powinien zapewnić, aby podmiot przetwarzający (w tym także pochodzący z państwa trzeciego) spełniał odpowiednie wymogi w zakresie bezpieczeństwa danych, w tym również te pozwalające na realizację wymogów wynikających z obowiązującego administratora danych prawa krajowego[12].

Ponadto, z art. 31 ust. 4 u.o.d.o. wyprowadzić należy **obowiązek zapewnienia kontroli** przez administratora danych w zakresie powierzonych do przetwarzania danych, tj. przetwarzanych w chmurze. Na konieczność tę, zwłaszcza w kontekście umownego zapewnienia sobie przez administratora prawa do wykonywania audytu i kontroli powierzonych danych, zwraca uwagę Generalny Inspektor Ochrony Danych Osobowych podkreślając, że *„w czasie trwania umowy administrator danych powinien sprawować rzeczywistą kontrolę nad procesem ich przetwarzania poprzez okresowe wykonywanie audytów w zakresie realizacji celów przetwarzania zgodnie z umową oraz w zakresie zgodności z warunkami określonymi w przepisach o ochronie danych osobowych, w tym właściwego ich zabezpieczenia"*[13]. Nie wydaje się jednak, aby uprawnienia kontrolne administratora danych należało odnosić wyłącznie do modelu bezpośredniej (fizycznej) kontroli, realizowanej poprzez dostęp do infrastruktury lub np. wstęp do pomieszczeń dostawcy. Przyjąć należy, że realizację ww. wymogów zapewnić pozwalają takie uprawnienia oraz konstrukcje umowne, jak w szczególności:

---

[10] *Opinia 05/2012 na temat przetwarzania danych w chmurze obliczeniowej*, przyjęta w dniu 1 lipca 2012 r., WP 196, s. 9. Tak również Grupa Robocza Art. 29 w *Opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, przyjętej w dniu 16 lutego 2010 r., WP 169, s. 29. W doktrynie krajowej zob. m.in. X. Konarski, *Przetwarzanie danych osobowych w chmurze obliczeniowej*, dodatek do Monitora Prawniczego 2013, nr 8, s. 40.

[11] GIODO, *ABC zagrożeń bezpieczeństwa danych osobowych w systemach informatycznych*, Warszawa 2009, s. 63. Por. również wytyczne dotyczące *cloud computing'u* niemieckich federalnych organów ds. ochrony danych osobowych z dnia 29 września 2011 r., gdzie podkreślono, że *„korzystanie z rozwiązań cloud computing nie może zwalniać administratorów danych, w szczególności ich kierownictwa, z ich zobowiązań w zakresie operacji przetwarzania danych"* (za: http://www.huntonprivacyblog.com/2011/10/articles/german-dpas-issue-resolution-and-guidance-paper-on-cloud-computing-and-compliance-with-data-protection-law; dostęp 9.10.2015).

[12] Por. Wytyczne KNF, pkt 10.6., s. 38.

[13] GIODO, *ABC zagrożeń bezpieczeństwa danych osobowych w systemach informatycznych*, s. 63; por. tak również Wytyczne KNF, pkt 10.7., s. 38.

- wymóg posiadania przez dostawcę określonych certyfikatów – przy odpowiedniej weryfikacji ze strony administratora[14];
- prawo do prowadzenia weryfikacji stosowanych przez dostawcę mechanizmów kontrolnych, co – jak się wydaje – może być realizowane z wykorzystaniem audytu wewnętrznego usługodawcy lub niezależnych audytorów zewnętrznych[15];
- obowiązek informowania administratora o wszelkich incydentach w zakresie bezpieczeństwa przetwarzanych danych[16];
- prawo do żądania udzielenia przez dostawcę usług określonych informacji;
- wprowadzenie określonych sankcji, np. kar umownych, w sytuacji braku współdziałania ze strony dostawcy[17].

Należy jednak zauważyć, że w ramach współpracy z dostawcami rozwiązań *cloud computing'u*, w tym z wiodącymi na rynku, wprowadzenie do umowy określonych instrumentów zabezpieczających interesy usługobiorcy jest często praktycznie utrudnione lub wręcz niemożliwe. Wynika to z tego, że z reguły umowy o korzystanie z tego rodzaju usług są tzw. umowami adhezyjnymi, niepozwalającymi na ich negocjowanie i zmiany. Dlatego też w praktyce niezbędne jest – poza dążeniem do wprowadzenia określonych rozwiązań w treści umowy – podjęcie również innego rodzaju działań, takich jak m.in. dokonanie wyboru właściwego dostawcy, spełniającego określone wymagania w zakresie technicznym oraz prawnym, czy też przeprowadzenie analizy ryzyka, uwzględniającej specyfikę usług świadczonych „w chmurze" (por. dalsze uwagi w tym zakresie związane z u.d.u.r.)[18].

4. Ochrona danych osobowych w związku z transferem danych do państw trzecich

Dodatkowego omówienia wymaga korzystanie z usług chmurowych świadczonych przez dostawców spoza Europejskiego Obszaru Gospodarczego, którymi w praktyce są najwięksi dostawcy tego rodzaju usług. W sytuacji takiej dochodzi bowiem do przekazywania danych osobowych do tzw. państw trzecich (państw nienależących do EOG – art. 7 pkt 7 u.o.d.o.), co wymaga spełnienia przez administratora danych dodatkowych obowiązków, wynikających z rozdziału 7 ustawy. Podstawowym z nich jest legitymowanie się odpowiednią przesłanką (podstawą), pozwalającą na przełamanie generalnego zakazu przekazywania danych osobowych do państw trzecich niespełniających na swym terytorium adekwatnego poziomu ochrony danych. Wśród możliwych do zastosowania w kontekście usług chmurowych podstaw wskazać należy na:

1) możliwość skorzystania z jednego z **wyjątków określonych w art. 47 ust. 3 u.o.d.o.**, co jednak w praktyce napotyka na poważne trudności:

---

[14] Przy czym posiadanie określonego certyfikatu nie przesądza samo w sobie o zgodności z przepisami powszechnie obowiązującego prawa. Europejskie organy ochrony danych zgłaszają w tym zakresie zastrzeżenia, na co wskazuje m.in. stanowisko organu duńskiego dotyczące certyfikatu SAS70 Type II; por. opinię z dnia 3 lutego 2011 r., *Processing of sensitive personal data in a cloud solution*, dostępną pod adresem: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution (9.10.2015).

[15] Por. Wytyczne KNF, pkt 10.7., s. 38.

[16] Tak również Wytyczne KNF, rozszerzając to na wszelkie incydenty jedynie zagrażające bezpieczeństwu danych (pkt 10.6., s. 38).

[17] Tak również Wytyczne KNF, pkt 10.8., s. 39.

[18] Tak wyraźnie tzw. Memorandum Sopockie z dnia 24 kwietnia 2012 r., *Working Paper on Cloud Computing – Privacy and Data Protection Issues*, s. 3; zob. również opinię Europejskiego Inspektora Ochrony Danych, dotyczącą komunikatu Komisji „Wykorzystanie potencjału chmury obliczeniowej w Europie", z dnia 16 listopada 2012 r., s. 15.

a) w kontekście korzystania z usług chmurowych i związanego z tym przekazywania danych należy bowiem zasadniczo wyłączyć możliwość powoływania się na wyjątki określone w art. 47 ust. 3 pkt 2 oraz pkt 3 u.o.d.o.[19]. Związane jest to z występującą w tym zakresie w przepisach przesłanką „niezbędności", której znaczenie i konieczność restrykcyjnej wykładni podkreślono na gruncie przepisów krajowej ustawy[20], jak i dyrektywy 95/46/WE[21]. Zakładając tym samym restrykcyjną interpretację przedmiotowej przesłanki, dla zalegalizowania operacji transferu danych nie będzie wystarczające, aby przekazanie danych było użyteczne, czy też np. bardziej opłacalne z gospodarczego punktu widzenia;
b) problematyczne będzie również skorzystanie z wyjątku określonego w art. 47 ust. 3 pkt 1 u.o.d.o. (**zgoda osób**, których dane dotyczą na przekazywanie ich danych do państw trzecich). Wynika to, po pierwsze, z wątpliwości natury prawnej. W sytuacji korzystania z usług chmurowych dochodzi bowiem do tzw. masowych czy też „strukturalnych" transferów danych. Grupa Robocza Art. 29 podkreśla natomiast w kontekście tego rodzaju operacji konieczność oparcia transferu danych na silniejszej niż zgoda podstawie prawnej. Po drugie, wątpliwości w tym zakresie wynikają również z kwestii faktycznych: ustawa wymaga bowiem, aby zgody były udzielone na piśmie. Dodatkowo, oparcie się na przesłance zgody rodzi ryzyko w postaci braku udzielenia zgody przez część podmiotów danych, co z kolei skutkować może np. koniecznością korzystania z dwóch niezależnych systemów czy centrów przetwarzania danych;

2) możliwość zawarcia stosownej **umowy transferowej**, zgodnej ze standardowymi klauzulami umownymi, zatwierdzonymi przez Komisję Europejską, na podstawie art. 26 ust. 4 dyrektywy 95/46/WE (art. 48 ust. 2 pkt 1 u.o.d.o.). W analizowanym tu przypadku, z uwagi na przyjętą kwalifikację stron umowy o korzystanie z usług chmurowych właściwym zestawem klauzul modelowych będzie zestaw stanowiący załącznik do decyzji Komisji nr 2010/87/UE (tzw. klauzule *controller-to-processor*)[22]; co przy tym istotne, na gruncie aktualnego brzmienia ustawy, w takiej sytuacji zgoda Generalnego Inspektora na przekazanie danych, o której mowa w art. 48 ust. 1 ustawy, nie będzie wymagana[23];
3) **wyrażenie przez Generalnego Inspektora zgody**, na podstawie art. 48 ust. 1 u.o.d.o., co następuje *„pod warunkiem, że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą"*.

---

[19] Przepisy te zezwalają na przekazanie danych osobowych do państwa trzeciego, w sytuacji gdy przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub gdy jest to podejmowane na jej życzenie, bądź też gdy przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem.

[20] GIODO, *ABC zasad przekazywania danych osobowych do państw trzecich*, Warszawa 2007, s. 12.

[21] Grupa Robocza Art. 29, *Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.*, przyjęty 25 listopada 2005 r., WP 114, s. 13 i n.

[22] Decyzja Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w państwach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady (Dz. Urz. UE L 39, s. 5 z 12.02.2010 r.).

[23] D. Karwala, X. Konarski, *Zasady transferu danych osobowych do państwa trzeciego po nowelizacji ustawy o ochronie danych osobowych z 7.11.2014 r.*, dodatek do Monitora Prawniczego 2015, nr 6, s. 27 i n.

W związku z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej, orzekającego w sprawie Maximillian Schrems vs. Data Protection Commissioner, i stwierdzeniu nieważności decyzji Komisji Europejskiej nr 2000/520 z dnia 26 lipca 2000 r., zatwierdzającej program tzw. Bezpiecznej Przystani (*Safe Harbor*)[24], aktualnie nie będzie już możliwe oparcie operacji przekazywania danych do amerykańskich dostawców na tej podstawie (co we wcześniejszej praktyce gospodarczej było częste).

5. *Cloud computing* a tajemnica ubezpieczeniowa

Ustawa o działalności ubezpieczeniowej i reasekuracyjnej z dnia 11 września 2015 r., podobnie jak ustawa o działalności ubezpieczeniowej z dnia 22 maja 2003 r., wprowadza obowiązek „*zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia*" przez zakład ubezpieczeń, osoby w nim zatrudnione oraz przez osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe (art. 35 ust. 1). Zgodnie z dominującym stanowiskiem, należy pojęciu tajemnicy ubezpieczeniowej nadawać szerokie znaczenie: obejmować ono będzie zarówno informacje dotyczące podmiotu zawierającego umowę ubezpieczenia, jak i informacje zawarte w takich umowach, które dotyczą czynności ubezpieczeniowych (np. wysokość składki, okres trwania umowy)[25].

W art. 35 ust. 2 ustawy o działalności ubezpieczeniowej i reasekuracyjnej określono zamknięty katalog sytuacji, w których **zakaz zachowania tajemnicy ubezpieczeniowej nie obowiązuje**. Zgodnie z brzmieniem art. 35 ust. 2 pkt 26 ustawy, „*obowiązek zachowania tajemnicy* [ubezpieczeniowej] *nie dotyczy informacji udzielanych na wniosek […] zleceniobiorców czynności ubezpieczeniowych i reasekuracyjnych oraz funkcji należących do systemu zarządzania powierzanych w drodze outsourcingu, w zakresie, w jakim dotyczą one zleconych czynności i funkcji*". Uznać należy, że podstawa ta pozwalać będzie na uchylenie tajemnicy w związku z korzystaniem z usług podmiotów świadczących na rzecz zakładów ubezpieczeń usługi chmurowe. Warunkiem jest, aby *cloud provider* uzyskiwał dostęp do informacji wyłącznie w zakresie, w jakim informacje te dotyczą zleconych czynności i funkcji, a więc w zakresie świadczonych usług. Pewne wątpliwości związane są w tym zakresie z brzmieniem art. 35 ust. 2 ustawy, który wymaga złożenia „wniosku" przez outsourcera. O ile bowiem wymóg ten znajduje uzasadnienie w kontekście podmiotów należących do sektora publicznego (sąd, prokuratura, Policja itd.), o tyle budzić może pewne zastrzeżenia w odniesieniu do podmiotów z sektora prywatnego. Przyjąć jednak należy – zachowując odpowiednie znaczenie przedmiotowego wymogu – iż stosowny wniosek może być ujęty umową zawartą z *cloud providerem*[26]. Podobnie, jak uczyniono to na gruncie ustawy o ochronie danych osobowych, uregulowana została kwestia odpowiedzialności zakładu ubezpieczeń w sytuacji powierzenia danych (informacji objętych tajemnicą). Zgodnie bowiem z art. 35 ust. 3 u.d.u.r., przetwarzanie danych oraz wykonywanie czynności i funkcji przez podmioty, o których mowa w ust. 2 pkt 25 i 26, „*nie ogranicza odpowiedzialności wynikającej z obowiązku zachowania tajemnicy, o którym mowa w ust. 1*".

Dla praktyki gospodarczej szczególnie istotne znaczenie ma również odpowiedź na pytanie, czy informacje dotyczące zawartych umów ubezpieczenia, lecz **zanonimizo-**

---

[24] Wyrok z 6 października 2015 r.w sprawie C-362/14.

[25] Zob. m.in. wyrok Naczelnego Sądu Administracyjnego z 5 czerwca 2001 r., sygn. III SA 2661/00.

[26] Tak również *Raport o usługach cloud computing w działalności ubezpieczeniowej*, Warszawa, styczeń 2013 r., s. 17.

wane lub zagregowane (zbiorcze) stanowią tajemnicę ubezpieczeniową i podlegają pod analizowaną tu regulację ochronną. W literaturze przedmiotu wyrażono stanowisko, że informacje odpowiednio zanonimizowane lub zagregowane, które nie zawierają danych pozwalających na identyfikację określonej strony umowy ubezpieczenia, nie stanowią tajemnicy ubezpieczeniowej[27]. Z poglądem tym należy się zgodzić, pomimo że art. 35 ust. 1 u.d.u.r., który odwołuje się do *„tajemnicy dotyczącej poszczególnych umów ubezpieczenia"*, nie przewiduje wyjątku w stosunku do informacji mogących wchodzić w zakres informacji chronionych tajemnicą ubezpieczeniową. Przepis ten wymaga jednakże, aby określone informacje odnosiły się do *„poszczególnych umów ubezpieczenia"*. Tym samym w sytuacji, gdy informacje nie będą pozwalały na zidentyfikowanie konkretnej strony umowy przez dysponenta tychże informacji, wydaje się, iż nie będą one stanowić tajemnicy ubezpieczeniowej[28].

Analogiczne wnioski wynikają z ustawy o ochronie danych osobowych[29]. Regulacja tej ustawy nie będzie bowiem miała zastosowania do przetwarzania danych w chmurze, w tym do ich przekazywania na serwery zlokalizowane w państwach trzecich, o ile zakres danych nie będzie umożliwiał identyfikacji przez odbiorcę danych (dostawcę usług chmurowych) podmiotów danych, tj. gdy przekazywane będą wyłącznie dane zanonimizowane lub zagregowane (zbiorcze). Istotne jest jednak, aby w sytuacji zastosowania różnego rodzaju technik (np. szyfrowania, anonimizacji danych) usługodawca nie miał możliwości (technicznych, ale również prawnych) odszyfrowania czy też wykonania innych czynności w celu sprowadzenia danych do postaci pozwalającej na ponowną identyfikację osób fizycznych. W tym ostatnim bowiem przypadku nie sposób – jak się wydaje – twierdzić, że przekazywane są do niego dane niemające charakteru danych osobowych lub informacje niepodlegające tajemnicy ubezpieczeniowej. Tym samym ewentualne szyfrowanie lub np. poddanie danych anonimizacji przy zastosowaniu określonego oprogramowania powinno odbywać się nie po stronie dostawcy usługi, lecz po stronie zakładu ubezpieczeń, który powinien posiadać w szczególności stosowne klucze pozwalające na odszyfrowanie danych[30].

6. Usługi chmurowe jako przykład outsourcingu w świetle ustawy o działalności ubezpieczeniowej i reasekuracyjnej

Korzystanie z usług chmurowych stanowi przykład outsourcingu, definiowanego w ustawie o działalności ubezpieczeniowej i reasekuracyjnej, jako umowa między zakładem ubezpieczeń a dostawcą usług *„na podstawie której dostawca usług wykonuje proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez*

---

[27] Tak M. Krzemiński, *Tajemnica ubezpieczeniowa*, Gazeta Ubezpieczeniowa on-line z 8.11.2005 r., dostępna pod adresem www.gu.com.pl [31.01.2008]; na gruncie tajemnicy bankowej – J. Byrski, *Tajemnica prawnie chroniona w działalności bankowej*, C.H. Beck, Warszawa 2010, s. 52.

[28] Por. jednak wątpliwości, jakie podniesiono w tym kontekście w związku z wprowadzeniem art. 35 ust. 7 ustawy – D. Karwala, B. Mrozowska-Bartkiewicz, *Tajemnica ubezpieczeniowa na gruncie nowej ustawy ubezpieczeniowej*, Dziennik Ubezpieczeniowy z 27.10.2015 r.

[29] Jak również z dyrektywy 95/46/WE; por. W.K. Hon, Ch. Millard, I. Walden, *The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing*, International Data Privacy Law, 2011, vol. 1, no. 4, s. 211 i n.

[30] Co również istotne, wprowadzenie *„adekwatnych mechanizmów kontrolnych zapewniających poufność danych (np. poprzez ich szyfrowanie)"* stanowi jedno z podstawowych wymogów w zakresie korzystania przez zakłady ubezpieczeń z rozwiązań chmurowych, ujętych w Wytycznych KNF, por. pkt 10.6., s. 38.

zakład ubezpieczeń" (art. 3 ust. 1 pkt 27)[31]. Outsourcing w znaczeniu powszechnym (pozaustawowym) związany jest z wykorzystaniem zasobów zewnętrznych, w tym również w modelu tzw. outsourcingu łańcuchowego (ang. *chain outsourcing*), w którym główny dostawca korzysta – w celu świadczenia usług – z podwykonawców. W przypadku usług chmurowych można nawet zaryzykować stwierdzenie, że **outsourcing łańcuchowy** jest zasadą świadczenia tego rodzaju usług, nie zaś sytuacją wyjątkową. Wynika to zasadniczo ze specyfiki tego rodzaju usług, wykorzystujących rozproszoną infrastrukturę informatyczną, należącą do różnych podmiotów lub też wykorzystującą usługi (np. wsparcia, tzw. *help desk*) świadczone przez podwykonawców głównego dostawcy usług. Ustawa o działalności ubezpieczeniowej i reasekuracyjnej wydaje się uwzględniać tę specyfikę, obejmując definicją outsourcingu również umowę, na podstawie której dostawca usług powierza wykonanie procesu, usługi lub działania innym podmiotom, za pośrednictwem których wykonuje on dany proces, usługę lub działanie. Wątpliwość, jaka pojawia się w tym zakresie, związana jest jednakże z dopuszczalnością **dalszego pod-outsourcingu**, jako że ustawowa definicja odnosi się wyłącznie do dwóch rodzajów umów: umowy zawieranej przez zakład ubezpieczeń z dostawcą usługi (głównym outsourcerem) oraz umowy zawieranej przez dostawcę usługi z dalszym outsourcerem. Z drugiej jednak strony dopuszczono możliwość powierzenia przez dostawcę usługi wykonania procesu, usługi lub działania „innym podmiotom", nie precyzując jednak, czy pozwala to na zastosowanie konstrukcji tzw. outsourcingu gwiaździstego (głównego outsourcera wiążą bezpośrednie umowy z wieloma dalszymi outsourcerami), czy również konstrukcji outsourcingu łańcuchowego, w ramach którego również dalsi outsourserzy zawierają umowy z kolejnymi – w „łańcuchu" outsourcingu – podmiotami (podwykonawcami, dalszymi pod-outsourcerami)[32].

Ustawa o działalności ubezpieczeniowej i reasekuracyjnej, analogicznie jak inne ustawy regulujące działalność podmiotów z sektora finansowego (np. banki[33], instytucje płatnicze[34]), określa podstawowe zasady związane z outsourcingiem określonej sfery działalności. Do podstawowych wymogów w tym zakresie ustawa zalicza:

- **wymóg zawarcia umowy outsourcingowej na piśmie** (wniosek z art. 73 u.d.u.r.) Szczegółowe wymogi dotyczące **zawartości umowy outsourcingu** określa rozporządzenie delegowane Komisji (UE) 2015/35[35]. Zgodnie z art. 274 ust. 4 rozporządzenia umowa powinna uwzględniać m.in. następujące wymogi: 1) zobowiązanie usługodawcy do przestrzegania wszystkich mających zastosowanie przepisów prawa, wymogów regulacyjnych i wytycznych, jak również wszelkich za-

[31] Por. definicję wprowadzoną w art. 13 pkt 28 dyrektywy Parlamentu Europejskiego i Rady nr 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz. Urz. UE L 335, s. 1, z 17.12. 2009 r.).

[32] Wykładnia definicji ustawowej w świetle prawa unijnego (definicji przyjętej w dyrektywie 2009/138/WE) skłaniałaby jednak ku poglądowi o dopuszczalności stosowania konstrukcji tzw. outsourcingu łańcuchowego, obejmującej wiele „ogniw".

[33] Por. art. 6a i n. ustawy z dnia 29 sierpnia 1997 r.– Prawo bankowe (tekst jedn.. Dz. U. z 2015 r. poz. 128).

[34] Art. 86–88 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (tekst jedn. Dz. U. z 2014 r. poz. 873, z późn. zm.); zob. szerzej w tym zakresie J. Byrski, A. Wachowska, *Cloud computing w działalności instytucji płatniczej*, Monitor Prawa Bankowego, wrzesień 2012, s. 62.

[35] Rozporządzenie delegowane Komisji (UE) 2015/35 z dnia 10 października 2014 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2009/138/WE w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz. Urz. UE L 12, s. 1 z 17.01. 2015 r.).

sad zatwierdzonych przez zakład ubezpieczeń; 2) okres wypowiedzenia umowy przez usługodawcę, który powinien być wystarczająco długi, aby zakład ubezpieczeń mógł znaleźć rozwiązanie alternatywne; 3) obowiązek chronienia przez usługodawcę wszystkich informacji poufnych dotyczących zakładu ubezpieczeń oraz jego ubezpieczających, beneficjentów, pracowników, kontrahentów i wszelkich innych osób; 4) postanowienie, zgodnie z którym obowiązki i zadania usługodawcy wynikające z jego umowy z zakładem ubezpieczeń lub zakładem reasekuracji pozostaną nienaruszone pomimo ewentualnego sub-outsourcingu;

- konieczność opracowania (na piśmie) oraz wprowadzenia w życie przez zakład ubezpieczeń **zasad dotyczących outsourcingu**, w przypadku gdy zakład ubezpieczeń stosuje lub zamierza stosować outsourcing (art. 46 ust. 1 pkt 4 oraz ust. 5 u.d.u.r.)[36]. Zasady te powinny obejmować w szczególności: wykaz funkcji należących do systemu zarządzania oraz czynności ubezpieczeniowych, które zakład zamierza powierzać w drodze outsourcingu, ze wskazaniem, które z tych czynności zakład uznaje za podstawowe lub ważne; kryteria wyboru outsourcerów; sposób realizacji warunków, o których mowa w art. 74 i art. 75 ustawy; zasady zarządzania ryzykiem związanym z outsourcingiem. Zakład ubezpieczeń ma również obowiązek, co najmniej raz w roku, przeprowadzenia przeglądu ww. zasad i dostosowania ich *„do istotnych zmian w systemie zarządzania lub obszarze, którego dotyczą"* (art. 46 ust. 3 u.d.u.r.). Dodatkowo, ustawa nakłada obowiązek poinformowania organu nadzoru o zamiarze wprowadzenia zasad dotyczących outsourcingu oraz o istotnej zmianie tychże zasad oraz obowiązek przekazania organowi nadzoru treści tychże zasad (art. 46 ust. 4 u.d.u.r.);
- konieczność zapewnienia przez zakład ubezpieczeń, że dostawca usług *„będzie **współpracował z organem nadzoru w zakresie powierzonych czynności lub funkcji"*** **(art. 74 pkt 1 u.d.u.r.).** W związku z tym istotne jest w szczególności, aby umowa z dostawcą usług chmurowych uwzględniała aspekty nadzoru ubezpieczeniowego, co jednak biorąc pod uwagę stosowane w praktyce ogólne warunki umów w zakresie świadczenia tego rodzaju usług może stanowić pewną trudność;
- konieczność zapewnienia, aby zarówno zakład ubezpieczeń, jak i podmiot uprawniony do badania sprawozdań finansowych zakładu ubezpieczeń, podmiot uprawniony do badania sprawozdań o wypłacalności i kondycji finansowej zakładu ubezpieczeń oraz organ nadzoru posiadały ***„dostęp do danych związanych z powierzonymi czynnościami lub funkcjami"*** (art. 74 pkt 2 u.d.u.r.);
- wymóg zapewnienia, aby organ nadzoru miał możliwość ***„przeprowadzania kontroli działalności i stanu majątkowego dostawcy usług w zakresie powierzonych czynności lub funkcji"*** (art. 74 pkt 3 oraz art. 342 ust. 2 u.d.u.r.). Co w tym kontekście wydaje się szczególnie istotne, z ustawy oraz z dyrektywy 2009/138/WE należy wyprowadzić wniosek, iż organ powinien mieć zapewnioną możliwość prowadzenia kontroli „na miejscu" (ang. *on-site inspections*), tj. w lokalach usługodawcy (np. w jego serwerowniach), co w przypadku dostawców usług *cloud computing'u*, w szczególności tych z państw trzecich może być szczególnie utrudnione, o ile w ogóle możliwe (por. art. 38 ust. 1 lit. c) oraz motyw 37 preambuły do dyrektywy).

[36] Por. również art. 274 ust. 1 rozporządzenia delegowanego Komisji (UE) nr 2015/35 z dnia 10 października 2014 r. uzupełniającego dyrektywę Parlamentu i Rady 2009/138/WE..., Dz. Urz. UE L 12 z 17 stycznia 2015 r.

Ustawa o działalności ubezpieczeniowej i reasekuracyjnej wprowadza dodatkowe ograniczenia w odniesieniu do outsourcingu funkcji należących do systemu zarządzania oraz **„podstawowych lub ważnych czynności"** (art. 75 ust. 1 u.d.u.r.), nie definiując jednak tych pojęć, w zamian nakładając na zainteresowane podmioty obowiązek stosownego ich zdefiniowania, co następować będzie w ramach zasad dotyczących outsourcingu, o których mowa w art. 46 ust. 1 pkt 4 u.d.u.r.[37] Zgodnie z ustawą o działalności ubezpieczeniowej i reasekuracyjnej, powierzenie tego rodzaju funkcji i czynności nie może odbywać się w sposób prowadzący do:

a) przekazania zarządzania zakładem ubezpieczeń, w znaczeniu przyjętym w art. 368 § 1 Kodeksu spółek handlowych;
b) przekazania wykonywania działalności ubezpieczeniowej w sposób powodujący brak faktycznego wykonywania działalności przez zakład ubezpieczeń;
c) pogorszenia jakości systemu zarządzania zakładu ubezpieczeń;
d) zwiększenia ryzyka operacyjnego zakładu ubezpieczeń;
e) pogorszenia możliwości monitorowania przez organ nadzoru przestrzegania przez zakład ubezpieczeń jego obowiązków;
f) pogorszenia jakości świadczenia usług ubezpieczającym, ubezpieczonym lub uprawnionym z umów ubezpieczenia oraz cedentom[38].

Dodatkowo, w przypadku planowanego outsourcingu tego rodzaju funkcji i czynności, zakład ubezpieczeń ma **obowiązek zawiadomienia organu nadzoru** na co najmniej 30 dni przed wdrożeniem takiego outsourcingu; obowiązek notyfikacyjny dotyczy również wszelkich istotnych zmian w outsourcingu tych funkcji lub czynności (art. 75 ust. 2 u.d.u.r.). Z obowiązkiem tym powiązane jest uprawnienie organu nadzoru do nałożenia na zakład ubezpieczeń – w drodze decyzji administracyjnej – zakazu realizacji planowanego outsourcingu funkcji lub czynności (art. 363 ust. 1 u.d.u.r.). Organ może nakazać także wprowadzenie istotnej zmiany do umowy outsourcingu lub też może nakazać zakładowi ubezpieczeń rozwiązanie w wyznaczonym terminie umowy outsourcingu w przypadku stwierdzenia, że wykonywanie zleconych na zewnątrz funkcji lub czynności mogłoby odbywać się lub też odbywa się z naruszeniem warunków, o których mowa w art. 73–77 ustawy (art. 363 ust. 1 *in fine* oraz ust. 2 u.d.u.r.). Ustawa nakłada ponadto na zakład ubezpieczeń wymóg prowadzenia **ewidencji umów outsourcingu** (art. 77 u.d.u.r.). Ewidencja taka powinna zawierać co najmniej: dane identyfikujące outsourcerów; zakres powierzonych czynności i funkcji oraz miejsce ich wykonywania (co ma

[37] Do „podstawowych lub ważnych czynności" zaliczyć należy m.in. tworzenie oferty produktów ubezpieczeniowych, w tym ich wycenę, likwidację szkód, utrzymywanie i serwis systemów IT. Zob. również raport EIOPA, *Final Report on Public Consultation No. 13/008 on the Proposal for Guidelines on the System of Governance*, dostępny pod adresem https://eiopa.europa.eu/Publications/Reports/EIOPA-13-413_Final_Report_on_CP8.pdf (9.10.2015), s. 89, w którym do „podstawowych lub ważnych czynności" zaliczono także usługi związane z przechowywaniem (magazynowaniem) danych, a więc usługi, które świadczone są również w modelu chmury obliczeniowej.

[38] Dodatkowe wymogi w tym zakresie określa rozporządzenie delegowane Komisji (UE) 2015/35. Zgodnie z art. 274 ust. 3 tego rozporządzenia, wybierając usługodawcę, organ administrujący, zarządzający lub nadzorczy zapewnia m.in.: przeprowadzenie szczegółowej analizy w celu zapewnienia, aby potencjalny usługodawca posiadał umiejętności i możliwości oraz ewentualne zezwolenia wymagane na podstawie przepisów prawa, pozwalające mu wykonywać w odpowiedni sposób zlecane funkcje lub czynności, uwzględniając przy tym cele i potrzeby zakładu; brak naruszeń prawa, a w szczególności przepisów dotyczących ochrony danych, w związku z outsourcingiem; podleganie przez usługodawcę takim samym przepisom dotyczącym bezpieczeństwa i poufności informacji, jak przepisy mające zastosowanie do danego zakładu ubezpieczeń.

szczególne znaczenie w przypadku usług chmurowych, część bowiem z dostawców nie zapewnia w tym zakresie niezbędnych informacji); okres obowiązywania umów.

Ustawa o działalności ubezpieczeniowej i reasekuracyjnej, wzorem dyrektywy 2009/138/WE, wprowadza również szczególną regulację dotyczącą **odpowiedzialności zakładu ubezpieczeń** korzystającego z zewnętrznych dostawców, w tym dostawców rozwiązań chmurowych. Zgodnie bowiem z art. 76 ust. 1 ustawy, odpowiedzialności zakładu ubezpieczeń za szkody wyrządzone ubezpieczającym, ubezpieczonym lub uprawnionym z umów ubezpieczenia wskutek niewykonania lub nienależytego wykonania outsourcingu nie można wyłączyć ani ograniczyć (ust. 2 zasadę tę odnosi dodatkowo do cedentów)[39]. W ustawie nie wprowadzono natomiast – odmiennie niż uczyniono np. w ustawie Prawo bankowe (art. 6b ust. 1) – zasady, zgodnie z którą nie można wyłączyć ani ograniczyć odpowiedzialności outsourcera wobec banku za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy outsourcingowej. Rozwiązanie to należy ocenić jako korzystne, odmienne rozwiązania są bowiem niejednokrotnie trudne do pogodzenia z praktyką rynkową (w tym umowną) występującą w tym zakresie[40].

7. Podsumowanie

Korzystanie z usług *cloud computing'u* przez zakłady ubezpieczeń wymaga przede wszystkim uwzględnienia kwestii związanych z przetwarzaniem danych osobowych oraz tajemnicą ubezpieczeniową, z uwagi na to, że w modelu tym przetwarzane są z reguły dane osobowe ubezpieczających, ubezpieczonych, uposażonych lub uprawnionych z umowy ubezpieczenia, w tym dane dotyczące umów ubezpieczenia. W zakresie ochrony danych osobowych szczególną uwagę zwrócić należy na obowiązek zapewnienia kontroli przez administratora danych (tj. zakład ubezpieczeń) w zakresie powierzonych do przetwarzania i przetwarzanych w chmurze danych. Biorąc jednak pod uwagę, że w ramach współpracy z dostawcami wprowadzenie do umowy określonych instrumentów zabezpieczających interesy zakładu ubezpieczeń może być utrudnione, konieczne jest również podjęcie innego rodzaju działań, takich jak np. dokonanie wyboru właściwego dostawcy czy też przeprowadzenie analizy ryzyka. W kontekście tajemnicy ubezpieczeniowej zwrócić należy uwagę na art. 35 ust. 2 pkt 26 u.d.u.r., który to przepis pozwala na uchylenie tajemnicy w związku z korzystaniem z usług podmiotów świadczących na rzecz zakładów ubezpieczeń usługi chmurowe. Z uwagi na to, że korzystanie z usług chmurowych stanowi przykład outsourcingu, uwzględnienia wymaga również szczegółowa regulacja przyjęta w tym zakresie w ustawie o działalności ubezpieczeniowej i reasekuracyjnej. Niestety regulacja ta budzi pewne wątpliwości interpretacyjne i praktyczne (m.in. problem dopuszczalności outsourcingu łańcuchowego, uwzględnienie w umowie aspektów nadzoru ubezpieczeniowego, zapewnienie możliwości prowadzenia przez organ kontroli w lokalach usługodawcy, określenie zakresu „podstawowych lub ważnych czynności" itd.), co wymagać będzie dalszych analiz zarówno w doktrynie, jak i w praktyce obrotu, nie wykluczając również konieczności zajęcia stanowiska w tym zakresie ze strony Komisji Nadzoru Finansowego.

Damian Karwala
współpracujący z Kancelarią Prawną DLA Piper Wiater sp.k.,
członek zespołu Intellectual Property and Technology

[39] Por. art. 49 ust. 1 dyrektywy 2009/138/WE.
[40] J. Byrski, A. Wachowska, *Cloud computing*…, s. 70.

Bibliografia

Balboni P. 2010. „Data Protection and Data Security Issues Related to Cloud Computing in the EU", Tilburg University Legal Studies Working Paper Series (no. 22).
Byrski J. 2010. „Tajemnica prawnie chroniona w działalności bankowej", Warszawa: C.H. Beck.
Byrski J., A. Wachowska. 2012. „Cloud computing w działalności instytucji płatniczej", Monitor Prawa Bankowego (wrzesień).
Hon W.K., Ch. Miliard, I. Walden. 2011. „The problem of „personal data" in cloud computing: what information is regulated? – the cloud of unknowing", International Data Privacy Law, vol. 1 (no. 4).
Karwala D., X. Konarski. 2015. „Zasady transferu danych osobowych do państwa trzeciego po nowelizacji ustawy o ochronie danych osobowych z 7 listopada 2014 r., dodatek do Monitora Prawniczego (nr 6).
Konarski X. 2013. „Przetwarzanie danych osobowych w chmurze obliczeniowej", dodatek do Monitora Prawniczego (nr 8).
Krzemiński M. 2005. „Tajemnica ubezpieczeniowa", Gazeta Ubezpieczeniowa on-line z 8 listopada 2005, dostępna pod adresem: www.gu.com.pl.
Mednis A. 2009. „Administrator danych i podmiot przetwarzający dane na zlecenie – status prawny, zakres praw i obowiązków, problemy definicyjne", w: „Ochrona danych osobowych. Skuteczność regulacji", G. Szpor (red.), Warszawa: C.H. Beck.
Molenda-Kropielnicka E. 2013. „Cloud computing – zagadnienia prawne", Prace z Prawa Własności Intelektualnej (z. 119).

Cloud Computing and the New Insurance and Reinsurance Activity Act

Services provided in the model of so-called cloud computing are becoming more and more popular also in the insurance sector. According to legal regulations, including the Insurance and Reinsurance Activity Act of 11 September 2015, there is no prohibition on the use of this type of solutions. Firstly, the analysis of the admissibility and the conditions for the application of cloud computing services requires taking into consideration aspects related to the personal data processing within cloud computing as well as confidential insurance information. Secondly, the issues connected with outsourcing in insurance activity are essential for the evaluation, especially after the introduction of a new insurance regulation (Solvency II), which raises certain doubts in interpretation and practice, as reinsurance has not been included. The present article is an attempt to analyse this particular IT model pursuant to the above-mentioned regulation.

Keywords: cloud computing, insurance secrecy, outsourcing in insurance activity, Insurance and Reinsurance Activity Act.