t. LXXV • nr 4/2022 (886) • DOI 10.33226/0137-5490.2022.4.5

Mgr Weronika Wojturska

Uniwersytet Warszawski
ORCID: 0000-0002-9514-9611
e-mail: w.wojturska@uw.edu.pl

Outsourcing chmurowy a reżim działalności nadzorowanej zakładów ubezpieczeń

Outsourcing to the cloud and the regime of supervised activity of insurance companies

Streszczenie

Outsourcing chmury obliczeniowej jest wyzwaniem pod względem regulacyjnym i operacyjnym nie tylko dla zakładów ubezpieczeń, ale także dla polskiego prawodawcy i organu nadzoru, którzy mierzą się z dostosowaniem obowiązujących przepisów do bieżących potrzeb praktyki obrotu. Artykuł ma na celu zidentyfikowanie głównych trudności interpretacyjnych we wdrażaniu rozwiązań chmurowych, jakie mogą nastręczać przepisy ustawy o działalności ubezpieczeniowej i reasekuracyjnej, szczególnie istotnych po implementacji Dyrektywy Wypłacalność II oraz zidentyfikowanie zmian, które wprowadza Urząd Komisji Nadzoru Finansowego w Komunikacie dotyczącym przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z 2020 r. wobec stanowiska wydanego w 2017 r.. Zmiany te można oceniać w kategoriach ułatwień regulacyjnych w działalności krajowych zakładów ubezpieczeń.

Słowa kluczowe: zakłady ubezpieczeń, działalność ubezpieczeniowa, outsourcing, chmura obliczeniowa, Komisja Nadzoru Finansowego, KNF

JEL: K23, K24

Abstract

Cloud computing outsourcing is a regulatory and operational challenge not only for insurance companies, but also for the Polish legislator and supervisory authority, who are dealing with the adaptation of the applicable regulations to the current needs of the trading practice. The article is devoted to selected regulatory aspects of outsourcing to cloud computing in terms of the insurance activity regime based on the provisions of the Act on Insurance and Reinsurance Activity, particularly essential after the implementation of the Solvency II Directive, and the position of the Polish Financial Supervisory Authority in the Communication on information processing by supervised entities using public or hybrid cloud computing services from January 23, 2020.

Keywords: insurance companies, insurance activity, outsourcing, cloud computing, Polish Financial Supervisory Authority, PFSA

Wprowadzenie

Współcześnie także w sektorze ubezpieczeniowym dostrzega się korzyści płynące z zastosowania technologii *cloud computing*. Potrzeba progresywnego zwiększenia wolumenu sprzedaży przekłada się na inwestycje w zaawansowaną funkcjonalność aplikacji, odpowiadającą idei rozwiązań chmurowych. Outsourcing chmury obliczeniowej stał się wyzwaniem pod względem regulacyjnym i operacyjnym nie tylko dla zakładów ubezpieczeń, ale także dla polskiego prawodawcy i organu nadzoru, którzy mierzą się z dostosowaniem obowiązujących przepisów do bieżących potrzeb praktyki obrotu, uwarunkowanych dynamicznie zmieniającą się rzeczywistością technologiczną. W artykule podjęto się, po pierwsze, zidentyfikowania głównych trudności interpretacyjnych we wdrażaniu rozwiązań chmurowych, jakie mogą nastręczać przepisy ustawy o działalności ubezpieczeniowej i reasekuracyjnej (dalej jako u.d.u.r.)[1], szczególnie istotnych po implementacji Dyrektywy Wypłacalność II[2]. Po drugie, zidentyfikowano zmiany, które wprowadza Urząd Komisji Nadzoru Finansowego w Komunikacie UKNF z 2020 r. (UKNF, 2020)[3] wobec stanowiska wydanego w 2017 r. (UKNF,

2017)[4] w sprawie przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej. Zmiany te można oceniać w kategoriach ułatwień regulacyjnych w działalności krajowych zakładów ubezpieczeń.

Chmura obliczeniowa

Fenomen chmury obliczeniowej jawi się jako *sui generis* wypadkowa postępujących przemian w zakresie implementacji nowych technologii we współczesnej gospodarce. Koncepcja *cloud computing* ewoluowała od lat 60. XX w., a wraz z nią używane nazewnictwo. Jej początków należy szukać w rozwoju idei *utility computing*[5], która ustąpiła 30 lat później koncepcji *grid computing*[6], co w konsekwencji dalszych przemian mających miejsce od 2006 r. dało początek współczesnemu rozumieniu chmury obliczeniowej[7]. Zjawisko to wpisało się w uniwersalny proces zmian zachodzących w sektorze łączności elektronicznej w opozycji do tradycyjnych usług telefonii głosowej. W rezultacie przyczyniło się do przechodzenia na płaszczyznę świadczenia usług opartych w całości na protokole IP[8] z dostępem do sieci Internet czy OTT (*Over the Top*)[9]. Podstawowa trudność związana jest z przyjęciem jednego uniwersalnego znaczenia „chmury obliczeniowej" w związku z deficytem definicji legalnych w prawie polskim i aktach prawa unijnego.

Najczęściej przywoływaną definicją, także przez polski organ regulacyjny, jest ta sformułowana w 2009 r. przez Narodowy Instytut Standaryzacji i Technologii (NIST) — instytucję uznawaną za prekursora rozwoju usług teleinformatycznych. Proponowane ujęcie zjawiska *cloud computing* wskazuje, że jest to model udostępniania w sposób zapewniający swobodny dostęp na żądanie z każdego miejsca współdzielonych i konfigurowalnych zasobów teleinformatycznych, w tym sieci komputerowych, serwerów, magazynów danych, oprogramowania systemowego, aplikacji, usług, które mogą być dynamicznie dostarczone i udostępnione przy minimalnym zaangażowaniu ze strony zarządzającego usługą lub jej dostawcy (Mell & Grance, 2011, s. 4). Klasyfikacja usług przetwarzanych w chmurze obliczeniowej jest zależna od rodzaju pozyskiwanych zasobów udostępnianych użytkownikowi przez dostawcę. W literaturze przedmiotu wyróżnia się trzy podstawowe modele świadczenia usług — są to: infrastruktura jako usługa (IaaS, *Infrastructures as a Service*), platforma jako usługa (PaaS, *Platform as a Service*) oraz aplikacja jako usługa (SaaS, *Software as a Service*). Wyodrębnienie poszczególnych modeli jest istotne nie tylko ze względów badawczych i ułatwiających proces prac normalizujących, ale także komercyjnych. Z perspektywy klientów umożliwia trafniejszy wybór podyktowany realizacją zasady skalowalności, a dostawcom pozwala pozyskać lepszą orientację w zakresie przedmiotu świadczenia. Modele chmury obliczeniowej można klasyfikować nie tylko ze względu na formę świadczenia usługi, lecz również ze względu na tryb jej eksploatacji (odniesienie się do skali oferty usług). Co do zasady ze względu na to kryterium wyróżnia się trzy główne rodzaje chmury: chmurę publiczną, prywatną i hybrydową (tak: Mell & Grance, 2011, s. 4; Dillon i in., 2010, s. 28), które mogą znaleźć zastosowanie w sektorze ubezpieczeniowym.

Outsourcing chmury obliczeniowej w reżimie u.d.u.r.

Zakład ubezpieczeń, korzystając już z outsourcingu lub zamierzając outsourcować usługi chmury obliczeniowej, powinien każdorazowo zapewnić zgodność całego procesu w pierwszej kolejności z przepisami prawa powszechnie obowiązującego, a następnie ze stanowiskiem krajowego organu nadzoru. Sektor ubezpieczeniowy doczekał się uregulowania obszaru outsourcingu w obowiązującej od stycznia 2016 r. u.d.u.r. (art. 3 ust. 1 pkt 27, art. 46, art. 73–77, art. 342, 351, 352, 362, 363) w rezultacie implementacji do polskiego porządku prawnego założeń drugiego filaru nowego systemu wypłacalności, Dyrektywy Wypłacalność II[10]. Zarówno znowelizowana w 2015 r. u.d.u.r., jak i jej poprzedniczka z 2003 r. nie odnoszą się bezpośrednio do kwestii korzystania przez zakłady ubezpieczeń z usług świadczonych w chmurze, jednocześnie nie zakazując korzystania z tego rodzaju rozwiązań. Analiza treści Wytycznych KNF z 2014 r. (KNF, 2014)[11] oraz uzupełniającego je Komunikatu UKNF z 2020 r. nie pozostawia wątpliwości, że podstawowym punktem odniesienia — w przypadku outsourcingu regulowanego (ubezpieczeniowego w reżimie u.d.u.r.) — będą relewantne przepisy ustawowe: „usługa przetwarzania informacji w chmurze obliczeniowej ma charakter powierzenia czynności przetwarzania i [...] może być traktowana jako outsourcing chmury obliczeniowej [...] Niniejszy komunikat nie wyłącza przepisów bezwzględnie obowiązujących w tym zakresie, natomiast celem jest zaprezentowanie, jak Nadzór rozumie te przepisy" (II.3 Komunikatu). W dalszej części artykułu zostaną poddane rozważaniom dwa główne aspekty, które można postrzegać jako problematyczne z perspektywy wdrożenia rozwiązań chmurowych.

Spośród wszystkich ustaw regulujących działalność podmiotów nadzorowanych sektora finansowego to w u.d.u.r. jako pierwszej zdefiniowano wprost instytucję powierzenia określonej działalności podmiotom zewnętrznym. Korzystanie z usług chmurowych jest przykładem outsourcingu, który, jak podaje definicja legalna z art. 3 ust. 1 pkt 27 u.d.u.r., oznacza „umowę między zakładem ubezpieczeń albo zakładem reasekuracji a dostawcą usług, na podstawie której dostawca usług wykonuje proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez zakład ubezpieczeń lub zakład reasekuracji, a także umowę, na podstawie której dostawca usług powierza wykonanie takiego procesu, usługi lub działania innym podmiotom, za pośrednictwem których wykonuje on dany proces, usługę lub działanie". W układzie powierzenia zakład wykorzystuje zewnętrzne zasoby do prowadzenia swojej działalności, opierając się na wykorzystaniu potencjału, sił i środków innego podmiotu. Przy czym będzie to taki ro-

dzaj zadań, które przed zawarciem i wejściem w życie postanowień umowy były wykonywane bezpośrednio przez outsourcera (zakład ubezpieczeń).

Pomimo, że pojęciem podoutsourcingu (inaczej: suboutsourcingu) nie posłużono się wprost w u.d.u.r., to bezpośrednio zostało ono wyartykułowane w definicji legalnej outsourcingu w Dyrektywie Wypłacalność II[12]. Ponadto art. 274 ust. 4 lit. k i l rozporządzenia delegowanego 2015/35[13] wskazuje, że umowa pomiędzy zakładem ubezpieczeń a zewnętrznym dostawcą powinna w stosownych przypadkach określać warunki, zgodnie z którymi można dokonać suboutsourcingu zleconych mu funkcji i czynności, a także zapewnienie w tych okolicznościach o nienaruszalności wynikających z niej zobowiązań. Wątpliwości w zakresie literalnego brzmienia art. 3 ust. 1 pkt 27 u.d.u.r. wyrazili komentatorzy P. Czublun i in. (2016), podnosząc, że przepis zawiera wiele pojęć nieostrych, budzących poważne wątpliwości interpretacyjne. Podobnie twierdzi D. Karwala, ponieważ ustawowa definicja odnosi się wyłącznie do dwóch rodzajów umów, tj. umowy zawieranej przez zakład ubezpieczeń z dostawcą usługi oraz umowy zawieranej przez dostawcę usługi z dalszym podwykonawcą (Karwala, 2016, s. 50). Jak przekonuje, mimo posłużenia się w definicji legalnej zwrotem „innym podmiotom", ustawodawca nie doprecyzował, czy pozwala to na dopuszczenie wprost modelu outsourcingu łańcuchowego (dalsi insourcerzy zawierają umowy z kolejnymi podwykonawcami) lub modelu gwiaździstego (bezpośredni dostawca jest związany umowami z wieloma dalszymi insourcerami). Zdaniem autorki uznanie dopuszczalności podoutsourcingu, ale tylko w jednej relacji poziomej (jednym łańcuchu podwykonawstwa), czyli bez dalszej możliwości powierzenia, podobnie jak uregulowano to w art. 6a ust. 7 pr.bank., byłoby zbyt rygorystyczne. Na gruncie praktyki konstrukcję tę postrzega się jako powszechną ze względu na specyfikę rozproszonej infrastruktury teleinformatycznej. Interpretując powyższą kwestię z perspektywy jak najlepszego zabezpieczenia interesu outsourcera, jako słuszne jawi się stanowisko P. Wajdy, który utrzymuje, że możliwość dokonania przez dostawcę usług dalszego powierzenia wykonywania czynności lub funkcji zakładu innym podmiotom należy wyłączyć w ogólności, gdyż w świetle postanowień z art. 73 u.d.u.r. takiego powierzenia może dokonać wyłącznie outsourcer (Wajda, 2017). Łańcuch outsourcingowy należy zatem uznać za dopuszczalny na gruncie u.d.u.r., jednakże może zostać zainicjowany tylko przez zakład ubezpieczeń, który w drodze zobowiązań umownych udziela podinsourcerowi mandatu do dostępu do przetwarzanych informacji. W praktyce pierwotny dostawca, chcąc zaangażować preferowanego podwykonawcę, a podmiot ten — kolejnego podinsourcera, zobowiązani są zwrócić się do zakładu o nawiązanie (zainicjowanie) relacji umownej w tym zakresie. Podzlecenie czynności outsourcingowych dokonane przez głównego dostawcę bez wiedzy i zaangażowania zakładu ubezpieczeń stałoby w opozycji do postanowień z art. 74 i 75 u.d.u.r.

Drugą kwestią, która może sprawiać trudności interpretacyjne z perspektywy uczestników rynku ubezpieczeniowego jest określenie podstawowych lub ważnych funkcji lub czynności operacyjnych działalności ubezpieczeniowej. Należy zgodzić się z tym, że u.d.u.r. wprowadza przez art. 75 ust. 1 dodatkowe ograniczenia w odniesieniu do outsourcingu „funkcji należących do systemu zarządzania oraz podstawowych lub ważnych czynności", nie definiując wprost tych pojęć, a w zamian nakładając na zakład obowiązek stosownego ich zdefiniowania. Nastąpi to w ramach art. 46 ust. 1 pkt 4 u.d.u.r., który obliguje do wyznaczenia i sporządzenia wykazu czynności uznawanych przez zakład ubezpieczeń za podstawowe lub ważne, sugerując pewnego rodzaju dowolność w tym zakresie. Jednakże nietrudno o bezpośrednie odniesienia i wskazówki pozwalające na wyeksplikowanie definicji wskazanych funkcji w przepisach unijnych i stanowisku EIOPA (Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych).

Pierwszej, generalnej wskazówki udziela motyw 31 preambuły Dyrektywy Wypłacalność II, w którym czytamy: „Funkcja to administracyjna zdolność podjęcia poszczególnych zadań z zakresu zarządzania. Określenie konkretnej funkcji nie stanowi dla zakładu przeszkody w swobodnym decydowaniu o sposobie jej zorganizowania w praktyce, chyba że przepisy dyrektywy stanowią inaczej. Nie powinno to powodować nadmiernej uciążliwości wymogów, gdyż należy uwzględnić charakter, złożoność i skalę działalności zakładu. Funkcje te mogą więc być wykonywane przez własny personel lub w oparciu o doradztwo ze strony ekspertów zewnętrznych, mogą też być zlecone ekspertom w drodze outsourcingu w granicach określonych w niniejszej dyrektywie". Funkcja należąca do systemu zarządzania została sprecyzowana także w definicji legalnej w art. 3 ust. 1 pkt 10 u.d.u.r. jako zdolność zakładu ubezpieczeń lub zakładu reasekuracji do wykonywania poszczególnych zadań w ramach systemu zarządzania. Za przyjęciem, że funkcjami należącymi do systemu zarządzania są: funkcja zarządzania ryzykiem, zgodności z przepisami, audytu wewnętrznego oraz funkcja aktuarialna, przemawiają postanowienia motywu 30 preambuły Dyrektywy Wypłacalność II. Ostatecznie wskazówki dostarcza także motyw 33, z którego dowiadujemy się że: „Funkcje należące do systemu zarządzania uważa się za funkcje kluczowe, a przez to również za funkcje ważne i podstawowe". Przy czym literalne brzmienie przepisu art. 75 poprzez spójnik „oraz" sugeruje odróżnienie outsourcingu funkcji należących do systemu zarządzania od outsourcingu „podstawowych lub ważnych czynności". W zakresie tych ostatnich wskazówek wydaje się dostarczać wytyczna 60 Wytycznych dotyczących systemu zarządzania EIOPA (EIOPA, 2014). Czytamy w niej, że: „Zakład powinien określać i udokumentować, czy funkcja lub czynność podlegająca outsourcingowi jest funkcją lub czynnością podstawową lub ważną, biorąc pod uwagę, czy dana funkcja lub czynność jest istotna dla działalności zakładu, tj. nie byłby on w stanie świadczyć swoich usług na rzecz ubezpieczających, jeżeli nie byłaby ona wykonywana". Europejski organ nadzoru nie podjął się jednak wskazania wprost, które z tych czynności każdorazowo należy zakwalifikować jako podstawowe lub ważne, co może oznaczać, że pozostawia decyzyjność w zakresie tego, co dany zakład uznaje

(i dlaczego) za istotne dla specyfiki jego działalności. Sięgając do wyjaśnień w anglojęzycznej wersji dokumentu, można zauważyć, że EIOPA powołuje się na dwa kryteria takiej kwalifikacji w postaci charakteru czynności będącej przedmiotem outsourcingu oraz tego, jaka część czynności danego rodzaju (w skali całego zakładu ubezpieczeń) jest objęta współpracą w ramach outsourcingu (EIOPA, 2015). Wydaje się, że w świetle stanowiska unijnego organu nadzoru znaczenie ma przede wszystkim kryterium przedmiotowe, gdyż podaje przykłady czynności lub funkcji, które powinny być „z definicji" uznawane za podstawowe lub ważne. Są to: tworzenie i taryfikacja oferty produktów ubezpieczeniowych; inwestowanie aktywów lub zarządzanie ich portfelem; likwidacja szkód; dostarczanie regularnego lub stałego wsparcia w zakresie *compliance*, audytu wewnętrznego, księgowości, zarządzania ryzykiem lub aktuariatu; zapewnianie bieżącego utrzymania lub wsparcia systemów IT; proces ORSA[14] oraz zapewnienie przechowywania (magazynowania) danych. Ostatnia ze wskazanych czynności wymaga pokreślenia, jako że do podstawowych lub ważnych czynności EIOPA zakwalifikował także usługi przechowywania danych, a więc również usługi świadczone w modelu chmury obliczeniowej. Drugie kryterium dotyczy skali współpracy między zakładem ubezpieczeń a dostawcą, co można wywnioskować z odpowiedzi organu udzielonej w serii pytań i odpowiedzi (Q&A) do Wytycznych dotyczących systemu zarządzania[15]. EIOPA potwierdził w kontekście outsourcingu czynności dotyczących zarządzania aktywami zakładu, że co do zasady będą to czynności podstawowe lub ważne (pkt 2.291). Jednak z zastrzeżeniem, że można przyjąć odmienną klasyfikację w sytuacji, gdy zakresem porozumienia objęta jest jedynie niewielka część portfela aktywów. EIOPA sugeruje więc, aby w ocenie dać pierwszeństwo skali współpracy przed samym charakterem outsourcowanej czynności. Biorąc pod uwagę te wskazówki, wydaje się, że główną wytyczną takiej kwalifikacji powinny być rezultaty oceny ryzyka w stosunku do poszczególnych umów z dostawcami z punktu widzenia stabilnego systemu zarządzania zakładem (tak także Mrozowska-Bartkiewicz & Wnęk, 2014, s. 6).

Komunikat chmurowy

Decydujące znaczenie w zakresie możliwości stosowania rozwiązań chmurowych na polskim rynku finansowym należy przypisać Komunikatowi UKNF z 2020 r., który z dniem publikacji 24.01.2020 r. zastąpił w całości Komunikat UKNF z 2017 r. Jednocześnie podkreślono na wstępie, że wszelkie wytyczne, zalecenia lub inne dokumenty prezentujące stanowisko europejskich organów nadzoru, w tym EIOPA, o tożsamym zakresie przedmiotowym nie mają zastosowania do podmiotów nadzorowanych[16]. Zdefiniowany przez UKNF model referencyjny jako podejście krajowe do outsourcingu przetwarzania informacji w chmurze obliczeniowej zawiera minimalne standardy obowiązujące podczas działań związanych z przygotowaniem, realizacją oraz zakończeniem przetwarzania. Komunikat zawiera wytyczne stosowania, klasyfikacji i oceny, szacowania ryzyka, minimalne wymagania techniczne i organizacyjne oraz obowiązki notyfikacyjne. W dalszej części przeanalizowane zostaną wybrane aspekty obecnie wiążącego stanowiska pod kątem zmian, jakie można postrzegać *in plus* w stosunku do podejścia UKNF sprzed stycznia 2020 r. Analizę uzupełniają w stosownych przypadkach wyjaśnienia interpretacyjne, jakie dotychczas pojawiły się w dwóch seriach pytań i odpowiedzi (Q&A)[17].

Na marginesie należy dodać, że w doktrynie podkreśla się niewładczy charakter rekomendacji KNF jako nieposiadających waloru powszechnego obowiązywania i charakteru aktów prawa wewnętrznego (Wajda & Pabian 2015, s. 109; Czech, 2009, s. 63; Olszak, 2010, s. 7–10). Rekomendacje KNF nie mogą stanowić samodzielnej podstawy decyzji administracyjnej wydawanej przez Komisję, choć z uwagi na jej przedmiot organ nadzoru w razie stwierdzenia ich naruszenia może zastosować władczy środek nadzoru. Podstawą w tym zakresie będzie jednak uchybienie poczynione przez podmiot nadzorowany względem ogólnego obowiązku stabilnego i ostrożnego zarządzania, a nie samej rekomendacji, chyba że pomimo niezastosowania się do rekomendacji do takiego naruszenia nie doszło. Podobnie w kategorii niewładczych form działania administracji postrzega się komunikaty UKNF, które nie są środkami prawnymi przewidzianymi w jakiejkolwiek normie prawnej. Służą wyklarowaniu pewnych kwestii interpretacyjnych względem obowiązujących przepisów prawa i sformułowaniu wskazówek dotyczących sposobu postępowania według oczekiwań nadzorczych. Natomiast zastosowanie się do nich przez podmioty nadzorowane może stać się przedmiotem kontroli UKNF.

Odpowiedzią na kluczowy deficyt pojęciowy na gruncie Komunikatu UKNF z 2017 r. wydaje się możliwie precyzyjne wyznaczenie zakresu stosowania zaktualizowanego stanowiska. Zakres podmiotowy został utożsamiony z zakresem nadzoru nad rynkiem finansowym sprawowanego przez KNF (art. 1 ust. 2 pkt. 1–8 u.n.r.f.[18]), w tym z nadzorem ubezpieczeniowym. Pełnym zakresem stosowania objęto także inne formy działalności, tj. oddziały zakładu ubezpieczeń (reasekuracji) z Unii Europejskiej, w tym oddziały zagraniczne, towarzystwa działające jako krajowe zakłady ubezpieczeń (reasekuracji) oraz działalność pośrednictwa ubezpieczeniowego (art. 3 ust. 1 pkt 15 u.d.u.[19]). Zakład ubezpieczeń został zobowiązany stosować Komunikat w relacjach z multiagentami oraz agentami wyłącznymi w zakresie, w jakim podmioty te wykonują proces, usługę lub działanie, które mogłyby zostać wykonane samodzielnie przez zakład oraz jest to outsourcing szczególny lub przetwarzanie informacji prawnie chronionych. Natomiast z obowiązku tego wyłączono relacje z zakładami reasekuracji i brokerami ubezpieczeniowymi, które ze względu na status podmiotów nadzorowanych będą samodzielnie wykonywać obowiązki wynikające z Komunikatu. Dla wzmocnienia względów bezpieczeństwa przed niepożądanym ujawnieniem informacji[20] przyjęto zasadę proporcjonalności, wykluczającą przyzwolenie na mniej efektywne zabez-

pieczenia w przypadku mniejszych podmiotów nadzorowanych. Ze względu na brak wyjaśnienia w Komunikacie należy przyjąć, że zakłady ubezpieczeń, zgodnie z art. 29 ust. 3 Dyrektywy Wypłacalność II, powinny stosować go, uwzględniając złożoność czynności lub funkcji zlecanych na zasadzie outsourcingu, ryzyko wynikające z umowy outsourcingu oraz potencjalny wpływ na ciągłość wykonywanej działalności, mając na uwadze przyświecające nadzorcy zapewnienie bezpieczeństwa przetwarzanych informacji.

Korzystając z chmury publicznej lub hybrydowej (w zakresie jej części opartej na chmurze publicznej) zakład ubezpieczeń powinien określić — w odniesieniu do każdej planowanej lub już wykorzystywanej usługi chmury obliczeniowej — po pierwsze, czy przetwarzane informacje należą do informacji prawnie chronionych, a po drugie, czy przetwarzanie informacji ma charakter outsourcingu szczególnego. W przeciwieństwie do Komunikatu UKNF z 2017 r. sprecyzowano znaczenie informacji prawnie chronionych, które nadzorca związał wprost z poszczególnymi tajemnicami danego sektora finansowego, w tym tajemnicą ubezpieczeniową. O ile w przypadku podstawowej formy outsourcingu, która odnosi się do informacji innych niż prawnie chronione, Komunikat może (a nie powinien) być stosowany, o tyle wybór ten nie dotyczy outsourcingu szczególnego (por. tabela IV.4 Komunikatu). Pojęcie to — dotąd nieznane — związano bardzo szeroko z powierzeniem dostawcy chmury krytycznych i istotnych funkcji, działań i procesów podmiotu nadzorowanego z perspektywy wykonywanej przezeń działalności regulowanej[21]. W tym względzie szczególnie zasadna wydaje się troska o monitorowanie w sposób ciągły, jakie procesy i w jakim zakresie są przetwarzane z wykorzystaniem chmury obliczeniowej, gdyż ich skala może zmieniać się w trakcie prowadzonej działalności. Komunikat pozostaje wobec u.d.u.r. w stosunku krzyżowania, tj. może znaleźć zastosowanie także w przypadku skorzystania przez zakład z usług *cloud computing* do outsourcingu poza reżimem tej ustawy. Usługa taka musiałaby mieć charakter outsourcingu szczególnego chmury obliczeniowej, w ramach którego nie są przetwarzane informacje prawnie chronione. Z zakresu stosowania Komunikatu wyłączono wprost chmurę prywatną, chmurę społecznościową o charakterze prywatnym, a także przetwarzanie danych (zanonimizowanych) podczas projektowania i eksploatacji środowisk testowych lub rozwojowych (IV.7 i 8 Komunikatu). Ostatnie z wyłączeń jawi się jako znaczące ułatwienie organizacyjne, spójne z wymogiem okresu testowego poprzedzającego uruchomienie produkcyjne usługi (por. VII.5.2 Komunikatu) oraz z zasadą minimalizacji przetwarzania danych osobowych[22].

Do kluczowych zmian w stosunku do Komunikatu UKNF z 2017 r. z pewnością należy zaliczyć poszerzenie katalogu rodzajów chmur. Zgodnie z Komunikatem chmura obliczeniowa to „pula współdzielonych, dostępnych »na żądanie« przez sieci teleinformatyczne, konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowych, aplikacji, usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale ich dostawcy" (I.1.3 Komunikatu)[23]. Wyróżnienie 4 rodzajów chmur: publicznej, prywatnej, hybrydowej i społecznościowej wydaje się pożądanym wyjściem naprzeciw poszerzającej się ofercie produktowej dostawców usług chmurowych. Podobny walor praktyczny ma dopuszczenie podoutsourcingu, w tym zdefiniowanie pojęcia „łańcucha outsourcingowego" i „poddostawcy", gdyż częstokroć podmioty nadzorowane korzystają z usług dostawcy oprogramowania, który w celu realizacji umowy outsourcingowej korzysta z usług innego dostawcy chmury[24]. Zgodnie z Komunikatem, dla oceny możliwości skorzystania ze współpracy w formie podoutsourcingu, a więc dopuszczalności przekazania określonego rodzaju danych w ramach łańcucha outsourcingowego (liczby podmiotów w nim występujących), pierwszą, podstawową wytyczną będą przepisy ustaw sektorowych. Na gruncie u.d.u.r., jak już wskazano, choć definicja outsourcingu z art. 3 ust. 1 pkt 27 może budzić wątpliwości interpretacyjne w zakresie dalszego podzlecania, należy przyjąć, że outsourcing wtórny jest dopuszczalny, jednakże może zostać zainicjowany tylko przez zakład ubezpieczeń, który w drodze zobowiązań umownych udziela podinsourcerowi mandatu do dostępu do przetwarzanych informacji.

Pierwszeństwo przepisom szczególnym przypisano także w zakresie odpowiedzialności insourcerów (dostawców i poddostawców). Natomiast postanowienia Komunikatu pozwalają na jej ograniczenie lub wyłączenie (VI.6.b Komunikatu). Przepisy u.d.u.r. odnoszą się jedynie do odpowiedzialności zakładu — za szkody wyrządzone ubezpieczającym, ubezpieczonym, uprawnionym z umów ubezpieczenia lub cedentom wskutek niewykonania lub nienależytego wykonania outsourcingu — której nie można wyłączyć ani ograniczyć (art. 76 u.d.u.r.). W zakresie modyfikacji odpowiedzialności dostawcy istotną wskazówką interpretacyjną jest to, że nadzorca krytycznie ocenia wyłączenie lub ograniczenia w przypadkach, gdy w chmurze przetwarzane są informacje prawnie chronione, szyfrowane za pomocą kluczy szyfrujących dostarczonych lub zarządzanych przez dostawcę lub jego poddostawcę, a także gdy przetwarzanie ma charakter outsourcingu szczególnego (VI.6.b Komunikatu).

Komunikat UKNF z 2017 r. w rozdziale I zatytułowanym „Identyfikacja potrzeb biznesowych, podstawa do podjęcia decyzji, planowanie" nieco odmiennie ukształtował wymogi dotyczące fazy planowania wdrożenia usługi przetwarzania danych w chmurze obliczeniowej. Punktem wyjścia uczyniono zobowiązanie do dokonania analizy SWOT (I.1 Komunikatu UKNF z 2017 r.), z czego Komunikat UKNF z 2020 r. rezygnuje na rzecz pierwszeństwa udokumentowanej klasyfikacji i oceny informacji[25], począwszy od rozróżnienia informacji prawnie chronionych, przez te, których ochrona wynika z uregulowań prawnych nieuwzględnionych w Komunikacie, po informacje niepodlegające ochronie prawnej (V.1 Komunikatu). Proces ten należy opisać tak w zakresie przyjętego przez zakład ubezpieczeń standardu klasyfikacji danych, jak i uzyskanych na tej podstawie wyników, które następnie uwzględnia się w planie przetwarzania. Jako racjonalny należy postrzegać niezbędny element postępowania w postaci analizy ewentualnych wyłączeń. Zakład ubezpieczeń uwzględnienia przy tym: skalę

prowadzonej działalności; korporacyjne, grupowe lub inne modele lub metody oceny i klasyfikacji, które uwzględniałyby założenia wytycznych i są wspólne dla grupy podmiotów, do której należy odpowiedzialność za przetwarzane informacje (V.3 Komunikatu).

W kolejnym kroku zakład został zobowiązany do samodzielnego (zgodnie z przyjętą przez siebie metodyką) przeprowadzenia procesu szacowania ryzyka, składającego się z identyfikacji, analizy i oceny zagrożeń, możliwości ich wystąpienia oraz oddziaływania. UKNF dopuszcza wykorzystanie w tym celu standardów opracowanych w ramach zrzeszeń branżowych lub innych powszechnie przyjętych (UKNF, 2020/2021). W rezultacie kluczowe jest udokumentowanie wyników oceny ryzyka dla każdej wdrożonej usługi wraz z planem postępowania z opisanym ryzykiem. Szacowanie ryzyka prowadzone w sposób ciągły, z uwzględnieniem praktycznej implementacji zasady PDCA (*plan–do–check–act*), musi odbyć się zgodnie z wymaganiami aktualnego wydania normy PN-ISO 27 005 (zob. ISO, 2018) lub jej odpowiednika w europejskim systemie normalizacji lub na bazie innego, usystematyzowanego podejścia[26]. Choć obecnie obowiązujący Komunikat w kwestii zarządzania ryzykiem podobnie jak w wydaniu z 2017 r. zobowiązuje w formie katalogu otwartego do uwzględnienia wszelkiego rodzaju ryzyka związanego z usługą chmury obliczeniowej, to w sposób odmienny — *in plus* — podjęto się jego kwalifikacji. Komunikat UKNF z 2020 r. skonkretyzował i pogrupował poszczególne rodzaje istotnych zagrożeń, dodatkowo uszczegóławiając stanowisko w newralgicznych aspektach w obszernym rozdziale VI. Podobnie w kategoriach wyjścia naprzeciw interesom podmiotów nadzorowanych można postrzegać zrezygnowanie z obowiązku posiadania planów ciągłości działania dostawcy, o których w rozdziale poświęconym zarządzaniu ryzykiem usługi traktowała wytyczna II.3.e Komunikatu UKNF z 2017 r., a które obecnie obowiązują tylko podmiot nadzorowany (VII.5.4 Komunikatu). Wytyczne opowiadają się za przyjęciem jako zasady konieczności szyfrowania wszystkich danych przetwarzanych w chmurze, w tym informacji prawnie chronionych, *at rest* (w spoczynku)[27] oraz *in transit* (w trakcie transmisji)[28]. Fizyczne przetwarzanie danych odbywa się zatem w centrum przetwarzania danych (dalej — CPD) oraz w infrastrukturze telekomunikacyjnej służącej do przesyłania danych pomiędzy poszczególnymi CPD wskazanymi w umowie z dostawcą, oraz pomiędzy CPD a zakładem ubezpieczeń.

Po zatwierdzonych wynikach szacowania ryzyka ubezpieczyciel dostosowuje mechanizmy do określonego przez KNF minimalnego zestawu wymagań organizacyjno-technicznych. W sposób szczególny różnice w podejściu nadzorcy są widoczne w wymaganiach w zakresie umowy z dostawcą usług chmurowych, począwszy od zrezygnowania z przymusu zawierania w umowie wszystkich wymaganych dotąd elementów, takich jak „parametry jakości (w trybie SLA) Usługi oraz parametry ciągłości działania Usługi (RTO i RPO)" (III.o Komunikatu UKNF z 2017 r.). Wymóg ten przeformułowano w taki sposób, aby powierzyć zobowiązanemu ocenę co do zasadności „z uwzględnieniem parametrów RTO i RPO tam, gdzie to zasadne, oraz deklarowanego SLA", choć podmioty nadzorowane będą musiały wskazać źródła dokumentacji technicznej i deklaracji zgodności (VII.4.1.k Komunikatu).

Następnie uwagę zwraca liberalizacja podejścia do określenia lokalizacji CPD jako ułatwienie skierowane przede wszystkim do dostawców usług chmurowych. Komunikat UKNF z 2017 r. zobowiązywał do wskazania w umowie dokładnej lokalizacji wykorzystywanych przez dostawcę usługi serwerowni (III.n Komunikatu UKNF z 2017 r.). Odmienne stanowisko — bliższe realiom rynkowym — zaprezentował Komunikat UKNF z 2020 r., podkreślając, że precyzyjne oznaczenie CPD może rodzić zagrożenie dla bezpieczeństwa fizycznego przetwarzanych informacji, dlatego jako minimum należy operować pojęciami strefa dostępu, region lub innymi równoważnymi, z podaniem co najmniej kraju oraz przybliżonej lokalizacji CPD, którymi dostawca usług chmury obliczeniowej posługuje się w standardowej komunikacji, np. podając miejscowość lub region kraju[29]. Natomiast, jeśli nie jest to możliwe lub — z uwagi na skalę działania i liczbę miejsc przetwarzania informacji — jest niezasadne, należy podać obszar EOG lub inne równoważne określenie[30]. W praktyce może oznaczać to także umowne odesłanie do konsoli administracyjnej, w której to klient samodzielnie dokonuje wyboru lokalizacji przetwarzania danych, czy też do dokumentacji publikowanej przez dostawcę usługi chmury obliczeniowej.

W dalszej kolejności warto poświęcić uwagę modyfikacji uprawnień kontrolnych. Prawo „do przeprowadzenia audytu lub certyfikacji przez podmiot nadzorowany i upoważnione przez niego firmy trzecie, łącznie z prawem do przeprowadzenia inspekcji na miejscu w lokalizacjach przechowywania i przetwarzania danych" (por. III.g Komunikatu UKNF z 2017 r.) zamieniono na uprawnienia z podziałem na te przysługujące podmiotowi nadzorowanemu oraz organowi nadzoru. Zakład ubezpieczeń zapewnia sobie wśród klauzul umownych prawo do „przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji, w tym prawo do przeprowadzenia audytu 2-giej lub 3-ciej strony na zlecenie podmiotu nadzorowanego (o ile taka potrzeba wynika z szacowania ryzyka)" (VII.4.4.1.m Komunikatu). Natomiast organ nadzoru zachowuje prawo do „wykonania obowiązków kontrolnych, w tym kontroli pomieszczeń i dokumentacji związanej z przetwarzaniem informacji podmiotu nadzorowanego, procesów i procedur, organizacji i zarządzania oraz potwierdzeń zgodności" (VII.4.4.1.n Komunikatu). Co istotne, w odpowiedzi na wątpliwości w przedmiocie tego, czy wystarczające jest opieranie się wyłącznie na raportach i certyfikatach na zgodność z właściwymi normami bezpieczeństwa, np. normami ISO, KNF wypowiada się jednoznacznie przecząco (zob. UKNF, 2020/2021). Jednocześnie nadzorca dopuszcza, z uwzględnieniem zastrzeżeń wskazanych w Komunikacie, możliwość wykorzystania przez podmiot nadzorowany (a także przez dostawcę innego niż dostawca usług chmurowych) audytu drugiej lub trzeciej strony tylko wówczas, gdy druga lub trzecia strona zagwarantuje w umowie, że audyt zostanie przeprowadzony na podstawie fizycznych inspekcji w lokalizacjach przetwarzania informacji, a także gdy dostawca chmurowy zapewni

w umowie pełną współpracę przy wykonaniu audytu (zob. UKNF, 2020/2021).

Zweryfikowanie założeń Komunikatu UKNF z 2017 r. przyczyniło się także do potrzebnej zmiany rozkładu akcentów pomiędzy wymogami skierowanymi wprost do podmiotu nadzorowanego a tymi skierowanymi do dostawcy usług chmurowych. Zapis wytycznej II.3 zobowiązywał zakład do posiadania katalogu dokumentów poświadczających poziom skuteczności mechanizmów kontrolnych po stronie dostawcy i jego podwykonawców. Tymczasem Komunikat czytelnie rozdziela redakcyjnie wymogi skierowane wprost do dostawcy i jego CPD (VII.6), pozostawiając podmiotowi nadzorowanemu decyzyjność co do konieczności i zakresu ich spełnienia (VII.6.1), od części poświęconej dokumentowaniu działań *sensu stricto* (VII.9). Wylistowanie wymagań stawianych insourcerowi, które zakład ubezpieczeń zobowiązany jest uwzględnić w szczególności w procesie szacowania ryzyka (przypis do VII.6 Komunikatu), wydaje się mieć niebywały walor praktyczny. Podrozdział VII.6 pełni funkcję swoistej listy kontrolnej pomocnej tak na etapie wyboru oferty, projektowania postanowień umownych, jak i uzgadniania z dostawcą kwestii zarządzania planami naprawczymi i monitorowania ich realizacji w razie wykazania nieprawidłowości. Przy czym istotne jest, aby zakres ten obejmował tak całość świadczonej usługi, jak i wszystkie CPD przetwarzające dane usługobiorcy. Dostarczenie dokumentacji certyfikacyjnej przez dostawcę usługi przed zawarciem umowy, w tym zapewnienie o dostępie oraz informowanie o każdej aktualizacji w trakcie jej trwania, pozwoli zakładowi ubezpieczeń na regularną weryfikację, a w przypadku niezgodności — na uruchomienie procedury naprawczej.

Podsumowanie

Nieodłącznym elementem transformacji cyfrowej branży teleinformatycznej stała się tendencja do ustępowania rozwiązań *on premises* (oprogramowania na własnej infrastrukturze) na rzecz usług wykorzystujących wyłącznie chmurę obliczeniową (usługi IaaS, SaaS, PaaS). Powodem tego jest ich dostępność, elastyczność i konkurencyjność kosztowa. W ciągu ostatniej dekady w sposób szczególny zwrócono uwagę na czerpanie potencjalnych korzyści z technologii *cloud computing* także w sektorze finansowym. Analizując wskazane we wstępie wybrane aspekty regulacyjne relewantne z perspektywy wdrażania narzędzi chmurowych do zakładów ubezpieczeń, nie sposób nie przyznać, po pierwsze, że dotychczasowy brak odniesienia wprost w ustawie oraz wątpliwości interpretacyjne w istotnych także dla outsourcingu chmurowego kwestiach zdradzają nieprzygotowanie w pełni obecnej regulacji do potrzeb wynikających z nieuchronnego procesu implementacji rozwiązań z zakresu nowych technologii do sektora ubezpieczeniowego. Po drugie, propozycja zaktualizowania stanowiska UKNF przybrała postać praktycznej mapy dla sektora regulowanego w procesie migracji do chmury. Komunikat z jednej strony wyszedł naprzeciw oczekiwaniom bezpośredniego wsparcia podmiotów nadzorowanych, z drugiej obrał sobie za cel zniwelowanie wątpliwości interpretacyjnych powstałych na gruncie poprzedniego dokumentu. Skonkretyzowano wiele pojęć, tworząc nowe definicje i doprecyzowując dotychczasowe wymogi, odnosząc się przy tym do większości postulatów podnoszonych w dyskusjach branżowych.

Odpowiedzią na kluczowy deficyt pojęciowy stało się możliwie precyzyjne wyznaczenie zakresu podmiotowego i przedmiotowego. Wprowadzona niezbędna siatka pojęciowa, w tym m.in. poszerzenie katalogu rodzajów chmur, zdefiniowanie pojęcia „outsourcingu szczególnego chmury obliczeniowej", „informacji prawnie chronionych", „łańcucha outsourcingowego", pełni rolę praktycznej matrycy i odpowiednio racjonalizuje zakres usług chmurowych. Wychodząc kompleksowo naprzeciw aspektom związanym z bezpieczeństwem, kluczowym etapem wdrażania usług chmurowych uczyniono proces szacowania ryzyka. Skonkretyzowano i pogrupowano przy tym poszczególne rodzaje istotnych zagrożeń, dodatkowo uszczegóławiając stanowisko UKNF w newralgicznych aspektach, m.in. w aspekcie szyfrowania informacji (szyfrowanie informacji prawnie chronionych jako zasada) czy tworzenia łańcucha outsourcingowego. Zakłady ubezpieczeń, a także ich potencjalni dostawcy zostali wyposażeni w praktyczne zalecenia dotyczące tego, w jaki sposób odpowiednie środki techniczne i organizacyjne mogą minimalizować ryzyka związane z przetwarzaniem informacji w chmurze[31]. Przez wzgląd na przywołane zmiany w podejściu nadzorcy Komunikat wydaje się zdecydowanym krokiem naprzód w kierunku możliwie najpełniejszego ułatwienia transferu technologii *cloud computing* w praktyce krajowych zakładów ubezpieczeń.

Przypisy/Notes

[1] Ustawa z 11.09.2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2019 r. poz. 381, 730 ze zm.) — dalej jako u.d.u.r.

[2] Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z 25.11.2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.Urz. UE L 335 z 17.12.2009 r. s. 1–155 ze zm.) — dalej jako Dyrektywa Wypłacalność II.

[3] Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z 23.01.2020 r. — dalej jako Komunikat UKNF z 2020 r., Komunikat (zob. UKNF, 2020).

[4] Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej z 23.10.2017 r. — dalej jako Komunikat UKNF z 2017 r. (zob. UKNF, 2017).

[5] Termin ten można przetłumaczyć jako „udostępnianie mocy obliczeniowej". Rozważania nad ideą *utility computing* zapoczątkował J. McCarthy w 1961 r., który po raz pierwszy opowiedział się za potencjałem technologii *time-sharingu* komputerów. Zdaniem prekursora spieniężenie zwiększającej się mocy obliczeniowej komputerów czy korzystanie z obsługi określonych aplikacji miało stać się w przyszłości dochodową inwestycją dla przedsiębiorstw użyteczności publicznej (*utility business model*). Por. Dupre, 2008.

[6] Termin wywodzi się od *electricity grid*, co oznacza elektryczną sieć przesyłową. Według koncepcji opracowanej przez I. Fostera, *grid* był systemem koordynującym zasoby, które nie podlegały scentralizowanej kontroli; wykorzystywał przy tym standardowe, otwarte protokoły i interfejsy ogólnego przeznaczenia w celu dostarczania usług. Docelowo miał zapewniać dostęp do złożonych zasobów teleinformatycznych na podobnych zasadach jak codzienne wykorzystywanie usług

komunalnych — wzorowany na sieciach przesyłowych. W praktyce dało to możliwość wykorzystywania na żądanie zasobów nienależących do danej organizacji, choć wykazującej zapotrzebowanie na nie. Zob. Foster, 2002, s. 22–25.

[7] Umownie przyjmuje się, że przemiany te dały fundament pod współczesną postać *cloud computing*. 13.03.2006 r. miało miejsce pierwsze uruchomienie usługi chmury publicznej ogólnego przeznaczenia (*Simple Storage Service*), a 24.08.2006 r. najbardziej obecnie znany dostawca tego modelu przetwarzania danych, firma Amazon Web Services, udostępniła do publicznego użytkowania *Elastic Compute Cloud* (EC2). Zob. https://aws.amazon.com/releasenotes/122, https://aws.amazon.com/ec2/ (pobrano 18.09.2019). Por. Kratzke & Quint, 2017, s. 1.

[8] Według Komisji Europejskiej, zob. pkt 1 uzasadnienia wniosku w sprawie dyrektywy Parlamentu Europejskiego i Rady ustanawiającej Europejski kodeks łączności elektronicznej z 12.12.2016 r., COM(2016) 590 final, 2016/0288 (COD) — dalej jako Uzasadnienie, http://eurlex.europa.eu/legalcontent/PL/TXT/HTML/?uri=CELEX:52016PC0590&from=EN, (pobrano 19.09.2019).

[9] Z ang. „usługa świadczona ponad siecią". Do podmiotów świadczących usługi OTT zalicza się: usługodawców oferujących szeroki zakres treści, usług i aplikacji za pośrednictwem sieci Internet, bez bezpośredniego zaangażowania dostawcy usługi dostępu do Internetu. Zob. pkt 1 Uzasadnienia.

[10] Dyrektywa Wypłacalność II odnosi się do outsourcingu w pkt 31 i 37 preambuły oraz przepisach: art. 13 pkt 28 (rozdział I sekcja 3 „Definicje"), art. 34 ust. 7, art. 38 (w rozdziale III „Organy nadzoru i zasady ogólne), art. 41 ust. 3, art. 49 (rozdział IV sekcja 2 „System zarządzania"), art. 50 ust. 1 lit. d (rozdział IV sekcja 3 „Publiczne ujawnianie informacji"). Szerzej na temat problematyki wejścia w życie dyrektywy: Grzeszczak, 2015.

[11] Pojęcie *cloud computing* dokument stosuje tylko raz w pkt 10.6. Wytycznych KNF z 2014 r.: „W przypadku, gdy usługi świadczone przez podmiot zewnętrzny obejmują przetwarzanie danych o wysokim stopniu poufności lub istotności dla towarzystwa poza infrastrukturą teleinformatyczną towarzystwa (np. w modelu *Cloud Computing* lub innych formach modelu *Application Service Provision*, w zewnętrznych centrach przetwarzania danych itp.), towarzystwo powinno w szczególności...", s. 37–38.

[12] Art. 13 pkt 28 Dyrektywy Wypłacalność II.

[13] Rozporządzenie delegowane Komisji (UE) 2015/35 z 10.10.2014 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2009/138/WE w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.Urz. UE L12/1 z 17.01.2015 r.) — dalej jako rozporządzenie delegowane 2015/35.

[14] Z ang. *own risk solvency assessment*, czyli proces własnej analizy strategicznej ryzyka i wypłacalności zakładu ubezpieczeń, który łączy wszystkie III filary wynikające z założeń Dyrektywy Wypłacalność II.

[15] Dostępne na stronie: https://www.eiopa.europa.eu/content/qa-regulation-0_en.

[16] Zapis ten można postrzegać jako problematyczny w przypadku projektów w ramach międzynarodowych grup kapitałowych obejmujących polskie podmioty nadzorowane.

[17] Odpowiednio z 17.12.2020 r. (pierwsza tura) i 25.03.2021 r. (druga tura). *Pytania i odpowiedzi (Q&A) w zakresie stosowania Komunikatu UKNF z 23 stycznia 2020 r. dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, https://www.knf.gov.pl/dla_rynku/fin_tech/chmura_obliczeniowa/Q&A, dostęp 25.03.2021. (zob. UKNF, 2020/2021).

[18] Ustawa z 21.07.2006 r. o nadzorze nad rynkiem finansowym (Dz.U. z 2019 r., poz. 298 ze zm.).

[19] Ustawa z 15.12.2017 r. o dystrybucji ubezpieczeń (Dz.U. z 2019 r., poz. 1881).

[20] Zgodnie z definicją wprowadzoną na potrzeby Komunikatu jest to sytuacja, podczas której informacje są przetwarzane w chmurze obliczeniowej: w sposób nieszyfrowany albo w sposób zaszyfrowany *at rest* lub *in transit*, ale dostęp do kluczy szyfrujących i szyfrowanej tymi kluczami informacji posiada albo może posiadać dostawca usług chmury obliczeniowej lub jego poddostawca w łańcuchu outsourcingowym (I.1.23 Komunikatu).

[21] Przetwarzanie informacji prawnie chronionych nie jest warunkiem koniecznym tej kwalifikacji.

[22] Zgodnie z art. 5. ust. 1 pkt c) rozporządzenia 2016/679 dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane, co oznacza, że nie należy przetwarzać więcej danych, aniżeli jest to niezbędne do osiągnięcia celu przetwarzania.

[23] Zaproponowana definicja jest tożsama z tą zaproponowaną przez NIST, por. Mell & Grance, 2011, s. 4.

[24] Jako usługę oferowaną w modelu chmury publicznej należy postrzegać także sytuację, w której dostawca (inny niż chmurowy) oferuje usługę polegającą na dostarczaniu oprogramowania w danym modelu na rzecz wielu podmiotów nadzorowanych (wykorzystywane elementy infrastruktury są wspólne), a dane podmiotów są separowane tak, że każdy podmiot nadzorowany posiada własną niezależną instancję systemu.

[25] Por. V.1–5 Komunikatu. Wytyczna I. 2 Komunikatu UKNF z 2017 r. wskazywała na „inwentaryzację i klasyfikację informacji".

[26] Por. VI.1 Komunikatu. W tym miejscu organ nadzoru sugeruje możliwość oparcia procedury szacowania ryzyka na udokumentowanej i właściwie wdrożonej metodzie, uwzględniając standard, normę lub inne wyspecyfikowane podejście, np. model NIST. Por. NIST, 2018.

[27] Zgodnie z I.1.14 Komunikatu: szyfrowanie informacji „w spoczynku" (np. przechowywanych kopii zapasowych, informacji w bazie danych, systemów plików).

[28] Zgodnie z I.1.15 Komunikatu: szyfrowanie w trakcie transmisji informacji (np. podczas przesyłania informacji z/do chmury obliczeniowej).

[29] Przypis do VII.4.4.1.b Komunikatu.

[30] Tamże.

[21] Warto odnotować, że ukazał się pierwszy standard branżowy skierowany do sektora ubezpieczeniowego. Zob. Polska Izba Ubezpieczeń, 2021.

Bibliografia/References

Literatura/Literature

Czech, T. (2009). Charakter prawny rekomendacji Komisji Nadzoru Finansowego. *Przegląd Prawa Publicznego*, (11).

Czublun, P. (red.) (2016). *Ustawa o działalności ubezpieczeniowej i reasekuracyjnej. Komentarz*. C.H.Beck.

Dillon, T., Wu, C. & Chang, E. (2010). Cloud computing: Issues and challenges. W: *Proceedings of the 24th IEEE international conference on advanced information networking and applications*. Institute of Electrical and Electronics Engineers Computer Society. http://dx.doi.org/10.1109/AINA. 2010.187

Dupre, F. (2008), *Utility (cloud) computing... flashback to 1961 Prof. John McCarthy*. https://computinginthecloud.wordpress.com/2008/09/25/utility-cloud-computingflashback-to-1961-prof-john-mccarthy/

EIOPA (2014). Wytyczne dotyczące systemu zarządzania, EIOPA-BoS-14/253, https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa_guidelines_on_system_of_governance_pl.pdf

EIOPA (2015). Final Report on Public Consultation No. 14/017 on Guidelines on system of governance, nr EIOPA-BoS-14/253. https://register.eiopa.europa.eu/Publications/Consultations/EIOPA_EIOPA-BoS-14-253-Final%20report_Governance.pdf

Foster, I. (2002). What is the grid? *Daily News And Information For The Global Grid Community*, *1*(6).

Grzeszczak, R. (2015). Implementacja dyrektywy Wypłacalność II — perspektywa prawa europejskiego. *Wiadomości Ubezpieczeniowe*, (1).

ISO (2018). *Information technology — Security techniques — Information security risk management*, https://www.iso.org/standard/75281.html (pobrano 10.02.2020).

Karwala, D. (2016). Chmura obliczeniowa a nowa ustawa o działalności ubezpieczeniowej i reasekuracyjnej. *Prawo Asekuracyjne*, *1*(86).

KNF (2014). *Wytyczne Komisji Nadzoru Finansowego dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji z 16 grudnia 2014 r.*, https://www.knf.gov.pl/knf/pl/komponenty/img/ZU_Wytyczne_IT_16_12_2014_40004.pdf

Komisja Europejska (2016). *Uzasadnienie wniosku w sprawie dyrektywy Parlamentu Europejskiego i Rady ustanawiającej Europejski kodeks łączności elektronicznej z dnia 12 października 2016 r.*, COM(2016) 590 final, 2016/0288 (COD), 12.10.2016. http://eurlex.europa.eu/legalcontent/PL/TXT/HTML/?uri=CELEX:52016PC0590&from=EN

Kratzke, N., & Quint, P. C. (2017). Understanding cloud-native applications after 10 years of cloud computing — A systematic mapping study. *Journal of Systems and Software*, *126*. https://doi.org/10.1016/j.jss.2017.01.001

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-145

Mrozowska-Bartkiewicz, B., & Wnęk, A. (2014). Problematyka ochrony konkurencji rynku ubezpieczeniowego, *Prawo Asekuracyjne*, (2).

NIST (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy*. Special Publication 800–37 Rev. 2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Olszak, M. (2010). Rekomendacje organu nadzoru bankowego — geneza, przedmiot regulacji, charakter prawny. *Przegląd Ustawodawstwa Gospodarczego*, (11).

Polska Izba Ubezpieczeń (2021). *Standard wdrożeń przetwarzania informacji w chmurze obliczeniowej*, https://piu.org.pl/wp-content/uploads/2021/06/standard-chmura-obliczeniowa-1.pdf

Szczepańska, M., & Wajda, P. (red.) (2017). *Ustawa o działalności ubezpieczeniowej i reasekuracyjnej. Komentarz*. Wolters Kluwer.

UKNF (2017). Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej z 23.10.2017 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_dot_korzystania_przez_podmioty_nadzorowane_z_uslug_przetwarzania_danych_w_chmurze_obliczeniowej_59626.pdf

UKNF (2020). Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z 23.01.2020 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf

UKNF (2020/2021). Pytania i odpowiedzi (Q&A) w zakresie stosowania Komunikatu UKNF z 23 stycznia 2020 r. dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, https://www.knf.gov.pl/dla_rynku/fin_tech/chmura_obliczeniowa/Q&A

Wajda, P., & Pabian, S. (2015). Natura prawna i skutki rekomendacji Komisji Nadzoru Finansowego do zakładów ubezpieczeń i zakładów reasekuracji. *Wiadomości Ubezpieczeniowe,* (1).

Akty prawne/Legal acts

Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z 25.11.2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) Dz.Urz. UE L 335 z 17.12.2009 r. s. 1–155 ze zm., https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32009L0138&from=EN

Rozporządzenie delegowane Komisji (UE) 2015/35 z 10.10.2014 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2009/138/WE w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II), Dz.Urz. UE L12/1 z 17.01.2015 r., https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:02015R0035-20170409&from=SL

Ustawa z 21.07.2006 r. o nadzorze nad rynkiem finansowym, Dz.U. z 2019 r. poz. 298 ze zm., http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20190000298/U/D20190298Lj.pdf

Ustawa z 11.09.2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, Dz.U. z 2019 r., poz. 381, 730 ze zm., https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20150001844/U/D20151844Lj.pdf

Ustawa z 15.12.2017 r. o dystrybucji ubezpieczeń, Dz.U. z 2019 r., poz. 1881, http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20170002486/U/D20172486Lj.pdf

Mgr Weronika Wojturska

Laureatka stypendiów i programów grantowych Ministerstwa Nauki Szkolnictwa Wyższego „Diamentowy Grant", „Najlepsi z najlepszych!" dla wybitnie uzdolnionych młodych naukowców, nagrodzona „Studenckim Noblem" w Ogólnopolskim Konkursie na Najlepszego Studenta RP dziedzinie nauk społeczno-ekonomicznych oraz laurem „Pro Juvenes" w kategorii wybitny „Student naukowiec" podczas VIII Gali Nagród Środowiska Studenckiego, obecnie doktorantka w Szkole Doktorskiej Nauk Społecznych UW w dyscyplinie nauki prawne, związana z Katedrą Prawa i Postępowania Administracyjnego WPiA UW. Praca magisterska, na podstawie której powstał artykuł, zajęła III miejsce w konkursie na najlepszą pracę magisterską lub rozprawę doktorską organizowanym przez Polskie Wydawnictwo Ekonomiczne w Warszawie oraz redakcję miesięcznika „Przegląd Ustawodawstwa Gospodarczego".

Mgr Weronika Wojturska

Laureate of scholarships and grant programs of the Ministry of Science and Higher Education "Diamond Grant", "The best of the best!" for exceptionally gifted young scientists; a winner of the "Student Nobel Prize" in 2019 in the 10th National Competition for the Best Student of the Republic of Poland in the field of socio-economic sciences and the "Pro Juvenes" award in the category of outstanding "Student Scientist" during the 8th Gala of the Student Community Awards of the Students' Parliament of the Republic of Poland in 2020; currently a PhD candidate at the Doctoral School of Social Sciences in the discipline of legal science associated with the Department of Law and Administrative Procedure, Faculty of Law and Administration, University of Warsaw. The master's thesis, on the basis of which the article was prepared, took the third place in the competition for the best master's thesis or doctoral dissertation organized by the Polish Economic Publishing House in Warsaw and the editors of the "Przegląd Ustawodawstwa Gospodarczego".