Paweł Pelc*

„Komunikat chmurowy" Komisji Nadzoru Finansowego

Streszczenie

Komisja Nadzoru Finansowego wydała 23 stycznia 2020 roku nowy „komunikat chmurowy" adresowany do podmiotów nadzorowanych. Został on wydany bez stosownej podstawy prawnej, ale Komisja Nadzoru Finansowego, opierając się na tezie, że stanowi on uszczegółowienie obowiązków wynikających z obowiązujących przepisów sektorowych, w praktyce dysponuje narzędziami nadzorczymi, żeby wymusić jego stosowanie. Przedmiotem analizy jest zakres przedmiotowy i podmiotowy komunikatu, jego powiązanie z regulacją dotyczącą outsourcingu oraz zakres uwzględnienia w komunikacie kwestii cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo, instytucje finansowe, chmura obliczeniowa, nadzór nad rynkiem finansowym, soft law

* Paweł Pelc, Akademia Sztuki Wojennej w Warszawie, Centrum Badań nad Bezpieczeństwem, Ośrodek Centrum Studiów nad Cyberbezpieczeństwem, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

Wstęp

Komisja Nadzoru Finansowego (KNF) 23 stycznia 2020 roku wydała komunikat dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej[1], a następnie w związku z wybuchem pandemii COVID-19 dokonał zmian w określonych w nim terminów[2]. Zastąpił on wcześniejszy komunikat z 23 października 2017 roku dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej[3].

W komunikacie z 2017 roku Urząd Komisji Nadzoru Finansowego (UKNF) stał na stanowisku, „[...] że usługa przetwarzania danych w chmurze obliczeniowej […] ma charakter – powierzenia wykonywania czynności – i tym samym podlega właściwym dla danego sektora usług finansowych przepisom prawa w tym zakresie. Przedstawione poniżej stanowisko stanowi uszczegółowienie wybranych dobrych praktyk i zaleceń zawartych w Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (dalej: Rekomendacja D), Rekomendacji D-SKOK dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska w spółdzielczych kasach oszczędnościowo-kredytowych oraz Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji, powszechnych towarzystwach emerytalnych, towarzystwach funduszy inwestycyjnych, podmiotach infrastruktury rynku kapitałowego, firmach inwestycyjnych w zakresie outsourcingu, w odniesieniu do specyfiki usług przetwarzania danych w chmurze obliczeniowej”[4].

1 *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf.

2 *Zmiany postanowień zawartych w Komunikatu* [Komunikacie – P.P.] *UKNF z 23 stycznia 2020 r. dotyczącym przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, https://www.knf.gov.pl/knf/pl/komponenty/img/Zmiany_postanowien_zawartych_w_Komunikatu_UKNF_z_23_stycznia_2020.pdf.

3 *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej*, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_dot_korzystania_przez_podmioty_nadzorowane_z_uslug_przetwarzania_danych_w_chmurze_obliczeniowej_59626.pdf.

4 Ibidem, s. 1.

Charakter prawny „komunikatu chmurowego"

Komunikat chmurowy z 2020 roku „[...] jest podejściem krajowym do outsourcingu przetwarzania informacji w chmurze obliczeniowej dla sektora finansowego (model referencyjny)"[5]. W związku z tym do zagadnień w nim określonych nie mają zastosowania „[...] wytyczne, zalecenia lub inne dokumenty prezentujące stanowisko Europejskiego Urzędu Nadzoru Bankowego, Europejskiego Urzędu Nadzoru nad Ubezpieczeniami i Pracowniczymi Programami Emerytalnymi bądź Europejskiego Urzędu Nadzoru nad Rynkami i Papierami Wartościowymi, które odnoszą się do przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej"[6].

Komisja Nadzoru Finansowego stoi na stanowisku, że także jej komunikat z 2020 roku „[...] jest uzupełnieniem i uszczegółowieniem wybranych zaleceń w zakresie outsourcingu opisanych w: 1) rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach; 2) rekomendacji D-SKOK dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych; 3) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych; 4) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji; 5) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych; 6) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w podmiotach infrastruktury rynku kapitałowego; 7) wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych[7]".

Ani w komunikacie z 2017, ani w komunikacie z 2020 roku nie wskazano podstawy prawnej ich wydania. W konsekwencji pojawia się istotny problem charakteru prawnego tych komunikatów, a zwłaszcza komunikatu z 2020 roku.

5 *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*..., s. 6.
6 Ibidem, s. 6.
7 Ibidem, s. 5–6.

O ile w stosunku do niektórych podmiotów nadzorowanych KNF może wydawać rekomendacje lub wytyczne, o tyle nie dotyczy to całego rynku, a także zakres tych rekomendacji lub wytycznych jest określony w normach, na podstawie których są one wydawane. Nie mogą jednak mieć one charakteru prawotwórczego[8]. Zgodnie z art. 87 ust. 1 Konstytucji RP źródła prawa ograniczone są do Konstytucji, ustaw, ratyfikowanych umów międzynarodowych oraz rozporządzeń. Artykuł 93 Konstytucji RP przewiduje źródła prawa wewnętrznie obowiązującego, które obowiązują wyłącznie jednostki organizacyjnie podległe organowi wydającemu te akty. W świetle braku podległości organizacyjnej instytucji finansowych Komisji Nadzoru Finansowego, nie może ona wydawać aktów prawnych i nakładać obowiązków na ich adresatów[9].

W treści komunikatu z 2020 roku wskazano jedynie, że w „[...] celu zapewnienia prawidłowego funkcjonowania rynku finansowego, jego stabilności oraz bezpieczeństwa, na podstawie art. 4 ust. 1 ustawy o nadzorze nad rynkiem finansowym, Nadzór oczekuje od podmiotów nadzorowanych stosowania niniejszego modelu referencyjnego podczas działań związanych z przygotowaniem, realizacją oraz zakończeniem przetwarzania informacji w chmurze obliczeniowej, traktując go jako sprecyzowanie istniejących wymagań prawnych oraz bez uszczerbku dla tych wymagań”[10]. W art. 4 ust. 1 ustawy z 21 lipca 2006 roku o nadzorze nad rynkiem finansowym (t.j., Dz.U. 2020, poz. 180) określono zadania KNF. Do zadań tych należy: 1) sprawowanie nadzoru nad rynkiem finansowym określonym w art. 1 ust. 2 ustawy o nadzorze nad rynkiem finansowym; 2) podejmowanie działań służących prawidłowemu funk-

8 Więcej zob.: P. Pelc, *Nadzór Komisji Nadzoru Finansowego nad spółdzielczymi kasami oszczędnościowo-kredytowymi i Kasą Krajową oraz instrumenty nadzorcze Komisji w stosunku do kas i Kasy Krajowej*, [w:] *Prawo spółdzielcze. Zagadnienia materialnoprawne i procesowe*, red. A. Herbet, J. Misztal-Konecka, P. Zakrzewski, Lublin 2017, s. 255–260; Z. Ofiarski, *Rola Soft Law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego*, [w:] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, red. A. Jurkowka-Zeidler, M. Olszak, Warszawa 2016, s. 137–160; M. Olszak. *Wydawanie przez Komisję Nadzoru Finansowego wytycznych dotyczących sektora ubezpieczeniowego jako przykład zintegrowanego podejścia do wykonywania nadzoru nad rynkiem finansowym*, [w:] ibidem, s. 161–175; A. Jakubiak. *Rekomendacja nadzorcza w kontekście regulacji polskich i europejskich*, [w:] *Polityka i praktyka regulacji rynków finansowych*, red. W. Rogowski, Kraków–Warszawa 2015, s. 23–27; W. Oziębła. *Współczesne tendencje kształtowania się modelu nadzoru bankowego. Nadzór makro- i mikroostrożnościowy*. Warszawa 2020; P. Daniel, F. Geburczyk, *Akt informacyjny jako forma działania administracji publicznej*, Warszawa 2019.

9 T. Czech, *Charakter prawny rekomendacji Komisji Nadzoru Finansowego*, „Przegląd Prawa Publicznego” 2009, nr 11, s. 63–80.

10 *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej...*, s. 7.

cjonowaniu rynku finansowego; 3) podejmowanie działań mających na celu rozwój rynku finansowego i jego konkurencyjności; 4) podejmowanie działań mających na celu wspieranie rozwoju innowacyjności rynku finansowego; 5) podejmowanie działań edukacyjnych i informacyjnych w zakresie funkcjonowania rynku finansowego, jego zagrożeń oraz podmiotów na nim funkcjonujących w celu ochrony uzasadnionych interesów uczestników rynku finansowego, w szczególności poprzez nieodpłatne publikowanie – w formie i czasie przez siebie określonym – ostrzeżeń i komunikatów w publicznym radiu i telewizji w rozumieniu przepisów ustawy z dnia 29 grudnia 1992 roku o radiofonii i telewizji; 6) udział w przygotowywaniu projektów aktów prawnych w zakresie nadzoru nad rynkiem finansowym; 7) stwarzanie możliwości polubownego i pojednawczego rozstrzygania sporów między uczestnikami rynku finansowego, w szczególności sporów wynikających ze stosunków umownych między podmiotami podlegającymi nadzorowi Komisji a odbiorcami usług świadczonych przez te podmioty; 8) współpraca z Polską Agencją Nadzoru Audytowego, w tym udzielanie informacji, wyjaśnień i przekazywanie dokumentów, w zakresie niezbędnym do realizacji zadań związanych z monitorowaniem rynku w zakresie, o którym mowa w art. 27 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 537/2014 z 16 kwietnia 2014 roku w sprawie szczegółowych wymogów dotyczących ustawowych badań sprawozdań finansowych jednostek interesu publicznego, uchylającego decyzję Komisji 2005/909/WE; 9) wykonywanie innych zadań określonych ustawami.

Urząd w treści komunikatu nie wskazał konkretnego punktu z regulacji zawartej w art. 4 ust. 1 ustawy o nadzorze nad rynkiem finansowym, który byłby podstawą do oczekiwania od podmiotów nadzorowanych stosowania określonego przez Komisję Nadzoru Finansowego modelu referencyjnego zawartego w komunikacie. Wynika to z tego, że art. 4 ust. 1 ustawy o nadzorze nad rynkiem finansowym nie daje Komisji takich uprawnień[11]. Należy zatem przyjąć, że nie przysługuje jej uprawnienie do „[...] sprecyzowania istniejących wymagań prawnych", które prowadziłoby do nałożenia na podmioty nadzorowane nowych obowiązków wykraczających poza „istniejące wymagania prawne". Nie znaczy to, że KNF nie dysponuje narzędziami prawnymi do wymuszenia

11 Na gruncie podstaw do wydania zasad ładu korporacyjnego dla instytucji nadzorowanych, kwestię braku podstaw do oparcia ich na art. 4 ust. 1 ustawy o nadzorze nad rynkiem finansowym – A. Hajos-Iwańska, *„Zasady ładu korporacyjnego dla instytucji nadzorowanych" KNF – krok w kierunku budowy zunifikowanych zasad corporate governance sektora finansowego czy zbędne superfluum?*, [w:] *Polityka i praktyka regulacji rynków...*, s. 283–294.

stosowania się instytucji finansowych do wydanego przez siebie komunikatu, tak, jak to miało miejsce w przypadku wcześniej wydanych przez nią bez podstawy prawnej zasad ładu korporacyjnego dla instytucji nadzorowanych[12]. Służyć temu mogą w szczególności kontrole na miejscu i zalecenia pokontrolne, kontrola zza biurka i zalecenia, upomnienia i inne środki nadzorcze (w tym kary)[13] oraz w stosunku do części rynku także oceny BION. W ramach tych działań Komisja Nadzoru Finansowego może stać na stanowisku, że instytucja nadzorowana, która nie stosuje komunikatu, tak naprawdę nie stosuje wiążących ją przepisów prawnych tak, jak je rozumie KNF, nawet jeżeli z przepisów tych, przy zastosowaniu powszechnie używanych zasad interpretacji, nie da się wywieść norm nakładających takie obowiązki i zachowania, jakich oczekuje Komisja Nadzoru Finansowego w komunikacie. Sam komunikat, od strony formalnej, nie może być podstawą do zastosowania przez KNF przysługujących jej środków nadzorczych, gdyż nie może być uznany za źródło powstania obowiązku po stronie podmiotu nadzorowanego.

Zakres podmiotowy

Komunikat ma mieć zastosowanie do podmiotów nadzorowanych rozumianych jako podmioty podlegające nadzorowi nad rynkiem finansowym na podstawie art. 1 ust. 2 pkt 1–8[14], czyli podmioty podlegające nadzorom: bankowemu, emerytalnemu, ubezpieczeniowemu, nad rynkiem kapitałowym, nad instytucjami płatniczymi, nad agencjami ratingowymi, uzupełniającemu nadzorowi nad spółdzielczymi kasami oszczędnościowo-kredytowymi oraz nad pośrednikami kredytu hipotecznego.

Przy takim określeniu zakresu podmiotowego komunikat powinien mieć zastosowanie do banków, oddziałów i przedstawicielstw banków zagranicznych, oddziałów i przedstawicielstw instytucji kredytowych[15], funduszy emerytalnych (otwartych, dobrowolnych i pracowniczych) oraz towarzystw

12 *Zasady ładu korporacyjnego dla instytucji nadzorowanych*, https://www.knf.gov.pl/knf/pl/komponenty/img/knf_140904_Zasady_ladu_korporacyjnego_22072014_38575.pdf.

13 Por. w odniesieniu do rynku spółdzielczych kas oszczędnościowo-kredytowych, P. Pelc, *Nadzór*..., s. 238–243.

14 *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*..., s. 1.

15 Por. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe, t.j., Dz.U. 2019, poz. 2357, art. 131, ust. 1.

emerytalnych (powszechnych i pracowniczych), zakładów ubezpieczeń, zakładów reasekuracji i pośredników ubezpieczeniowych[16], firm inwestycyjnych, agentów firm inwestycyjnych, banków powierniczych, spółek prowadzących rynek regulowany, Krajowego Depozytu Papierów Wartościowych SA, spółek prowadzących izbę rozliczeniową, spółek prowadzących izbę rozrachunkową, spółki, której Krajowy Depozyt Papierów Wartościowych S.A. przekazał wykonywanie czynności z zakresu zadań, o których mowa w art. 48 ust. 1 pkt 1–6 lub ust. 2 ustawy o obrocie instrumentami finansowymi, centralnego depozytu papierów wartościowych, emitentów dokonujących oferty publicznej papierów wartościowych lub emitentów, których papiery wartościowe są dopuszczone do obrotu na rynku regulowanym lub które są wprowadzone do alternatywnego systemu obrotu, a także emitentów, którzy ubiegają się o dopuszczenie lub wprowadzenie ich papierów wartościowych do takiego obrotu, funduszy inwestycyjnych, towarzystw funduszy inwestycyjnych, zarządzających alternatywnymi systemami obrotu, innych podmiotów prowadzących obsługę funduszy inwestycyjnych lub alternatywnych funduszy inwestycyjnych, w tym podmiotów, którym zostało powierzone wykonywanie obowiązków towarzystwa funduszy inwestycyjnych lub zarządzającego ASI, spółek prowadzących giełdy towarowe, towarowych domów maklerskich, zagranicznych osób prawnych prowadzących na terytorium Rzeczypospolitej Polskiej działalność maklerską w zakresie obrotu towarami giełdowymi, przedsiębiorstw energetycznych prowadzących na podstawie zezwolenia Komisji Nadzoru Finansowego rachunki lub rejestry towarów giełdowych, giełdowych izb rozrachunkowych, CCP, kontrahentów finansowych, finansowych spółek holdingowych mających siedziby na terytorium Rzeczypospolitej Polskiej, finansowych spółek holdingowych o działalności mieszanej mających siedzibę na terytorium Rzeczypospolitej Polskiej, spółek holdingowych o działalności mieszanej mających siedzibę na terytorium Rzeczypospolitej Polskiej, uczestników rynku uprawnień do emisji, podmiotów świadczących usługi w zakresie udostępniania informacji o transakcjach, administratorów w rozumieniu art. 3 ust. 1 pkt 6 rozporządzenia 2016/1011[17], instytucji płatniczych, małych instytucji płatniczych, dostawców świadczących wyłącznie usługę dostępu do informacji o rachunku, biur usług płatniczych, instytucji pieniądza elektronicznego,

16 Por. Ustawa z dnia 22 maja 2003 r. o nadzorze ubezpieczeniowym i emerytalnym, t.j., ibidem, poz. 207, art. 2, ust. 2.

17 Por. Ustawa z dnia 29 lipca 2005 r. o nadzorze nad rynkiem finansowym, t.j., ibidem 2020, poz. 1400, art. 5.

oddziałów zagranicznych instytucji pieniądza elektronicznego[18], agencji ratingowych[19], instytucji kredytowych, zakładów ubezpieczeń, zakładów reasekuracji i firm inwestycyjnych wchodzących w skład konglomeratu finansowego[20], spółdzielczych kas oszczędnościowo-kredytowe i Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej[21] oraz pośredników kredytu hipotecznego i ich agentów[22]. Z zestawienia tego wynika, że nie wszystkie podmioty nadzorowane w rozumieniu komunikatu są instytucjami finansowymi, dotyczy on także m.in. emitentów dokonujących oferty publicznej papierów wartościowych, emitentów, których papiery wartościowe są dopuszczone do obrotu na rynku regulowanym lub które są wprowadzone do alternatywnego systemu obrotu, a także emitentów ubiegających się o dopuszczenie lub wprowadzenie ich papierów wartościowych do takiego obrotu. Wydaje się, że w stosunku do tej kategorii podmiotów brak jest podstaw do stosowania komunikatu chmurowego i powinno mieć do nich zastosowanie wyłączenie analogiczne, jak w przypadku zasad ładu korporacyjnego dla instytucji nadzorowanych[23]. Komunikat ma zastosowanie także do małych podmiotów będących insourcerami lub agentami instytucji finansowych, których skala działania może być ograniczona.

Zasada proporcjonalności

Komisja Nadzoru Finansowego w swoim działaniu kieruje się zasadą proporcjonalności, która ma na celu uwzględnienie skali działalności i poziomu ryzyka podejmowanego przez poszczególne instytucje finansowe. W przypadku komunikatu postanowiono także zastosować tę zasadę, Komisja Nadzoru Finansowego jednak rozumie ją w sposób szczególny: „Zasada proporcjonalności powinna znaleźć swoją konkretyzację na etapie szacowania ryzyka związanego z planowaniem czynności przetwarzania oraz adekwatnością stosowanych

18 Por. ibidem, art. 1, ust. 2, pkt 5 w związku z art. 99, 117d, 129, 132 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j., ibidem 2020, poz. 794).
19 Por. Ustawa z dnia 29 lipca 2005 r. o nadzorze nad rynkiem finansowym..., art. 1, ust. 2, pkt 5a.
20 Por. ibidem, art. 1, ust. 2, pkt 6.
21 Por. ibidem, art. 1, ust. 2, pkt 7.
22 Por. ibidem.
23 Zasad określonych w „Zasadach ładu korporacyjnego" nie stosuje się również do emitentów dokonujących ofert publicznych lub których papiery wartościowe są dopuszczone do obrotu na rynku regulowanym. Zob. *Zasady ładu korporacyjnego dla instytucji nadzorowanych*..., s. 5.

zabezpieczeń przetwarzanych informacji. Urząd KNF podkreśla, że zasada proporcjonalności nie powinna być interpretowana jako przyzwolenie na zastosowanie przez mniejsze podmioty nadzorowane mniej efektywnych zabezpieczeń przetwarzanych informacji niż opisane w niniejszym komunikacie"[24]. Oznacza to *de facto*, że bez względu na skalę prowadzonej działalności i poziom ryzyka podejmowanego przez podmioty nadzorowane instrumenty stosowane do zabezpieczenia przetwarzanych informacji muszą być na tym samym poziomie i mniejsze podmioty nie mogą ich ograniczyć. W efekcie należy uznać, że w tym przypadku zasada proporcjonalności będzie w praktyce iluzoryczna, gdyż za jej zastosowanie uznane będzie przy szacowaniu ryzyka związanego z planowaniem czynności przetwarzania uwzględnienie skali działania podmiotu i związanego z tym ryzyka w jego działalności. W efekcie mniejsze podmioty mogą mieć, ze względu na ograniczone zasoby kadrowe i finansowe, znacząco utrudnione korzystanie w swojej działalności z chmury obliczeniowej publicznej lub hybrydowej.

Zakres przedmiotowy

Przedmiotem komunikatu jest przetwarzanie informacji w chmurze obliczeniowej publicznej lub hybrydowej, jeżeli przetwarzane informacje należą do informacji prawnie chronionych (czyli informacja związana z tajemnicami sektora finansowego wymienionymi w ustawach sektorowych, tj. prawie bankowym; ustawie o obrocie instrumentami finansowymi; ustawie o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi; ustawie o giełdach towarowych; ustawie o działalności ubezpieczeniowej i reasekuracyjnej; ustawie o dystrybucji ubezpieczeń; ustawie o organizacji i funkcjonowaniu funduszy emerytalnych; ustawie o pracowniczych planach kapitałowych; ustawie o usługach płatniczych; ustawie o spółdzielczych kasach oszczędnościowo-kredytowych[25]) lub przetwarzanie informacji ma charakter outsourcingu szczególnego chmury obliczeniowej. Ponadto w przypadku przetwarzania informacji innych niż prawnie chronione Komisja Nadzoru Finansowego dopuszcza stosowanie komunikatu[26]. Komisja Nadzoru Finansowego

24 *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*..., s. 7.
25 Ibidem, s. 1.
26 Ibidem, s. 8.

przez chmurę obliczeniową rozumie pulę 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. Chmura obliczeniowa publiczna – według KNF – to chmura obliczeniowa dostępna do użytku publicznego, będąca w posiadaniu lub bezpośrednio zarządzana przez dostawcę usług chmury obliczeniowej, chmura obliczeniowa hybrydowa – chmura obliczeniowa składająca się z połączenia dwóch lub więcej osobnych chmur obliczeniowych (publicznej, prywatnej, społecznościowej), która poprzez standaryzację użycia lub odpowiednią technologię pozwala na przenoszenie czynności przetwarzania informacji pomiędzy chmurami obliczeniowymi, które ją tworzą. Według Komisji Nadzoru Finansowego, outsourcing szczególny chmury obliczeniowej oznacza outsourcing chmury obliczeniowej, w ramach którego podmiot nadzorowany powierza dostawcy usług chmury obliczeniowej wykonanie za pomocą usługi chmury obliczeniowej czynności lub funkcji podmiotu nadzorowanego, których brak lub przerwa w realizacji spowodowana awarią lub naruszeniem zasad bezpieczeństwa usługi chmury obliczeniowej, w ocenie podmiotu nadzorowanego: 1) wpływałaby w sposób istotny na ciągłość wypełniania przez podmiot nadzorowany warunków stanowiących podstawę uprawnienia prowadzenia działalności nadzorowanej lub jej wykonywania, lub 2) zagrażałaby w sposób istotny wynikom finansowym podmiotu nadzorowanego, niezawodności lub ciągłości wykonywania działalności nadzorowanej[27].

Outsourcing

Matryca stosowania komunikatu		Outsourcing chmury obliczeniowej	
		inny niż szczególny	szczególny
Informacje	inne niż prawnie chronione	Komunikat może być stosowany	Komunikat powinien być stosowany
	prawnie chronione	Komunikat powinien być stosowany	

27 Ibidem, s. 1–3.

Komunikat Komisji Nadzoru Finansowego ocenia przetwarzanie przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej w kontekście outsourcingu. Poszczególne regulacje sektorowe dopuszczają w różnym zakresie i na zróżnicowanych zasadach powierzenie wykonywania części czynności faktycznych związanych ze świadczeniem usług finansowych przez poszczególne instytucje finansowe podmiotom zewnętrznym, przy czym zakres i charakter dopuszczalnego outsourcingu, poziom szczegółowości regulacji, wymagania dotyczące rozwiązań umownych, charakteru insourcera, jego odpowiedzialności, dopuszczalności podoutsourcingu i zakresu ingerencji nadzorczej w ten proces jest zróżnicowany. Wydaje się, że najbardziej restrykcyjne są regulacje dotyczące sektorów bankowego i spółdzielczych kas oszczędnościowo-kredytowych, a znacznie łagodniejsze dotyczą rynku kapitałowego czy sektora ubezpieczeniowego. W stosunku do części podmiotów objętych komunikatem brak jest w ogóle ograniczeń w tym zakresie. W komunikacie Komisja Nadzoru Finansowego rozpatruje usługę chmury obliczeniowej właśnie przez pryzmat outsourcingu chmury obliczeniowej i łańcucha outsourcingowego. W tym kontekście praktyczne stosowanie komunikatu przez poszczególne instytucje finansowe musi się odbywać przy uwzględnieniu przez nie sektorowej regulacji dotyczącej outsourcingu mającej do nich zastosowanie. Może to w istotnym stopniu ograniczać stosowanie części rozwiązań przez podmioty, których ustawy sektorowe zakazują podoutsourcingu lub outsourcingu łańcuchowego.

Kwestie cyberbezpieczeństwa

Funkcjonowanie instytucji finansowych jest istotne dla krajowego systemu cyberbezpieczeństwa. Część z nich stanowi element infrastruktury krytycznej. Ponadto znaczna część przetwarzanych przez nie informacji stanowi informacje prawnie chronione, w tym objęte poszczególnymi odmianami tajemnicy zawodowej[28]. W komunikacie Komisja Nadzoru Finansowego wskazała, że „Nadzór uznaje ochronę przetwarzania informacji istotnych dla procesów lub działalności podmiotu nadzorowanego lub stanowiących informacje prawnie

28 Więcej zob. P. Pelc, *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, nr 2, s. 151–164.

chronione za zagadnienie o charakterze priorytetowym”[29]. Komisja wskazuje m.in. na ryzyko koncentracji przetwarzania informacji prawnie chronionych znacznej części sektora finansowego fizycznie w tych samych obiektach, a także ryzyka związane z ochroną przetwarzanych informacji. W ocenie Komisji Nadzoru Finansowego „Nadrzędnym zadaniem podmiotu nadzorowanego podczas przetwarzania informacji w chmurze obliczeniowej jest zapewnienie bezpieczeństwa przetwarzanych informacji oraz zgodności sposobu i zakresu tego przetwarzania z prawem”[30]. Na podstawie tak zidentyfikowanego ryzyka Komisja Nadzoru Finansowego zawarła w komunikacie wytyczne do szacowania ryzyka, które ma być prowadzone w sposób ciągły. W ramach tego procesu podmioty nadzorowane powinny oceniać m.in. podatność interfejsów, awarie mechanizmów izolacji zasobów, a także kwestię podziału odpowiedzialności za bezpieczeństwo przetwarzanych informacji między dostawcę usług chmury obliczeniowej a podmiot nadzorowany, mechanizmy uwierzytelniania oraz ich słabości, możliwości korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego, a także wartość przetwarzanych informacji dla podmiotu nadzorowanego oraz skutki bezpośrednie i pośrednie utraty kontroli nad ich przetwarzaniem. Oceniając kwestie szyfrowania, KNF wskazała, że brak jest gwarancji do uznania danego algorytmu szyfrowania za „całkowicie bezpieczny”. W komunikacie Komisja wskazuje, że „Podmiot nadzorowany w procesie szacowania ryzyka powinien uwzględnić potencjalną możliwość: 1) korzystania ze zweryfikowanych, aktualizowanych źródeł informacji o zagrożeniach specyficznych dla stosowania usług chmury obliczeniowej, w tym również w odniesieniu do konkretnych (nazwanych) usług; 2) korzystania z pomocy ze strony podmiotów lub osób o specjalistycznych kompetencjach zarówno w obszarze cyberbezpieczeństwa, jak i usług chmury obliczeniowej, szczególnie w sytuacji braku takich kompetencji wewnątrz własnej organizacji podmiotu nadzorowanego; 3) przeanalizowania dostępnych wyników audytów zewnętrznych dostawców usług chmury obliczeniowej w odniesieniu do usług chmury obliczeniowej oraz procesu zarządzania bezpieczeństwem informacji, poszerzając zakres analizy o dostępne certyfikaty wystawione dostawcy usług chmury obliczeniowej potwierdzające spełnienie wymagań; 4) uprzedniego testowania usług chmury obliczeniowej, także przy wykorzystaniu scenariuszy

29 *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*..., s. 5.
30 Ibidem, s. 7.

warunków skrajnych, zarówno w zakresie sposobu działania usługi jak i jej konfiguracji"[31].

Komisja Nadzoru Finansowego oczekuje, że podmiot nadzorowany zapewni, że informacje przetwarzane w chmurze obliczeniowej będą szyfrowane zgodnie z zasadami określonymi w wydanym przez nią komunikacie, a także, że będzie on zbierał i zabezpieczał logi związane z przetwarzaniem informacji w chmurze obliczeniowej. Podmiot nadzorowany powinien także posiadać dokumentację zawierającą m.in. „[...] organizację pracowników lub współpracowników odpowiedzialnych za cyberbezpieczeństwo, w tym stanowisk lub funkcji związanych z monitorowaniem, analizowaniem i raportowaniem incydentów związanych z informacjami przetwarzanymi w chmurze obliczeniowej, wraz z opisanymi wymaganymi kompetencjami, uprawnieniami i odpowiedzialnościami"[32] oraz procesy, procedury lub instrukcje dotyczące m.in. zarządzania incydentami bezpieczeństwa i przeprowadzania audytów wewnętrznych bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki chmury obliczeniowej.

Zawarte w komunikacie zapisy związane z cyberbezpieczeństwem są szerokie i niewątpliwie znacząco wykraczają poza obowiązujące regulacje prawne dotyczące poszczególnych podmiotów nadzorowanych. Jednakże nie wyłącza to przydatności zaproponowanych przez Komisję Nadzoru Finansowego rozwiązań w działalności podmiotów nadzorowanych.

Zakończenie

Komunikat chmurowy Komisji Nadzoru Finansowego dotyczy istotnej sfery funkcjonowania instytucji finansowych. Wydany został bez podstawy prawnej, co jednak nie wyklucza w praktyce możliwości przymuszenia podmiotów nadzorowanych do jego stosowania przy zastosowaniu narzędzi nadzorczych pozostających w gestii Komisji Nadzoru Finansowego i uznawania przez nią rozwiązań zawartych w komunikacie jako interpretacji obowiązujących przepisów w zakresie outsourcingu czy zarządzania ryzykiem. Wydaje się, że zakres podmiotowy komunikatu jest zbyt szeroki, gdyż obejmuje także podmioty, które nie są instytucjami finansowymi, a nawet nie przetwarzają informacji

31 Ibidem, s. 12.
32 Ibidem, s. 20.

chronionych tajemnicą zawodową, a także podmioty o bardzo ograniczonej skali działalności, wobec których Komisja Nadzoru Finansowego oczekuje zapewnienia takiego samego poziomu ochrony informacji, jak od podmiotów większych i o większym zakresie działania. Komisja Nadzoru Finansowego ocenia kwestie przetwarzania danych w chmurze obliczeniowej publicznej lub hybrydowej pod kątem regulacji dotyczących outsourcingu. Ich sektorowe zróżnicowanie będzie w istotny sposób wpływać na możliwość stosowania rozwiązań przyjętych w komunikacie przez poszczególne typy podmiotów nadzorowanych. Komunikat zawiera wiele rozwiązań nakierowanych na kwestie cyberbezpieczeństwa, co jest szczególnie istotne ze względu na system bezpieczeństwa cybernetycznego państwa oraz zaliczanie części podmiotów nadzorowanych do infrastruktury krytycznej. Informacje będące w posiadaniu instytucji finansowych są szczególnie ważne dla prawidłowego funkcjonowania państwa, a korzystanie z chmury pozbawia te instytucje bezpośredniej kontroli nad danymi przetwarzanymi w chmurze, zapewnienie zatem odpowiednych mechanizmów i procedur ich zabezpieczenia jest szczególne istotne, zwłaszcza w razie zakłócenia prawidłowego działania chmury obliczeniowej.

Bibliografia

Literatura

Czech T., *Charakter prawny rekomendacji Komisji Nadzoru Finansowego*, „Przegląd Prawa Publicznego" 2009, nr 11.

Daniel P., Geburczyk F., *Akt informacyjny jako forma działania administracji publicznej*, Warszawa 2019.

Hajos-Iwańska A., *„Zasady ładu korporacyjnego dla instytucji nadzorowanych" KNF – krok w kierunku budowy zunifikowanych zasad corporate governance sektora finansowego czy zbędne superfluum?*, [w:] *Polityka i praktyka regulacji rynków finansowych*, red. W. Rogowski, Kraków–Warszawa 2015.

Jakubiak A., *Rekomendacja nadzorcza w kontekście regulacji polskich i europejskich*, [w:] *Polityka i praktyka regulacji rynków finansowych*, red. W. Rogowski, Kraków-Warszawa 2015.

Ofiarski Z., *Rola Soft Law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego*, [w:] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, red. A. Jurkowka-Zeidler, M. Olszak, Warszawa 2016.

Olszak M., *Wydawanie przez Komisję Nadzoru Finansowego wytycznych dotyczących sektora ubezpieczeniowego jako przykład zintegrowanego podejścia do wykonywania nadzoru nad rynkiem finansowym*, [w:] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, red. A. Jurkowka-Zeidler, M. Olszak, Warszawa 2016.

Oziębła W., *Współczesne tendencje kształtowania się modelu nadzoru bankowego. Nadzór makro- i mikroostrożnościowy*, Warszawa 2020.

Pelc P., *Nadzór Komisji Nadzoru Finansowego nad spółdzielczymi kasami oszczędnościowo-kredytowymi i Kasą Krajową oraz instrumenty nadzorcze Komisji w stosunku do kas i Kasy Krajowej*, [w:] *Prawo spółdzielcze. Zagadnienia materialnoprawne i procesowe*, red. A. Herbet, J. Misztal-Konecka, P. Zakrzewski, Lublin 2017.

Pelc P., *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, nr 2.

Akty prawne

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe, t.j., Dz.U. 2019, poz. 2357.
Ustawa z dnia 22 maja 2003 r. o nadzorze ubezpieczeniowym i emerytalnym, t.j., Dz.U. 2019, poz. 207.
Ustawa z dnia 29 lipca 2005 r. o nadzorze nad rynkiem finansowym, t.j., Dz.U. 2020, poz. 1400.

'Cloud Communication' of Polish Financial Supervisory Authority

Abstract

On January 23, 2020, the Polish Financial Supervisory Authority issued a new „cloud communication" addressed to regulated entities. It was issued without an appropriate legal basis, but the Polish Financial Supervisory Authority, based on the thesis that it is a detailed specification of obligations under applicable sectoral regulations, in practice has supervisory tools to enforce its application. The subject of the analysis is the objective and subjective scope of the communication, its relationship with the outsourcing regulation and the scope of including cybersecurity issues in the communication.

Keywords: cyber security, financial institutions, cloud computing, financial market supervision, soft law