

Klara Dygasiewicz*

Piotr Zapadka**

Zasady korzystania przez banki krajowe z usługi tzw. chmury obliczeniowej społecznościowej w czasach gospodarki COVID lub postCOVID w świetle komunikatu Komisji Nadzoru Finansowego

Streszczenie

Celem niniejszej publikacji jest pokazanie wybranych aspektów prawnych niezwykle aktualnego obecnie zagadnienia, jakim jest korzystanie przez banki krajowe z zewnętrznych usług tzw. chmury obliczeniowej społecznościowej, w obliczu ograniczeń związanych z tradycyjną pracą departamentów IT w bankach zarówno w czasach gospodarki COVID, jak i w okresie gospodarki postCOVID. Ograniczenia związane z powstrzymaniem rozprzestrzeniania się COVID sprawiły, że klienci zaczęli masowo korzystać z oferty bankowej za pośrednictwem dostępnych kanałów telekomunikacyjnych. Nadto z racji ryzyka związanego z zakazami dotyczącymi przebywania w pomieszczeniach biurowych przez pracowników departamentów IT banków, możliwości korzystania z „zewnętrznych serwerowni” (uplasowanych w chmurze) stają się węzłowo istotnym aspektem działalności banków krajowych zarówno w obecnej sytuacji gospodarczej, jak i w przyszłości. Co równie istotne, zagadnienie to jest przedmiotem wyraźnego zainteresowania ze strony Komisji Nadzoru Finansowego (KNF), co siłą rzeczy stanowi podstawę do dokonanej poniżej analizy materii regulacyjnej.

Słowa kluczowe: COVID-19, bank krajowy, chmura obliczeniowa

* Dr Klara Dygasiewicz, Katedra Prawa Finansowego, Wydział Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie.

** Dr hab. Piotr Zapadka, prof. UKSW, Katedra Prawa Finansowego, Wydział Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie.

Na wstępie należy wskazać, że model chmur obliczeniowej pozwala na dostarczanie zasobów informatycznych takich, jak sieci o odpowiedniej przepływności czy przechowywanie dużych zbiorów danych, a wszystkie te zasoby są dostępne na żądanie, w dowolnym miejscu¹. Decydując się na korzystanie z tego modelu, nie trzeba ponosić kosztów budowy i utrzymywania zaawansowanej infrastruktury informatycznej, a w razie takiej potrzeby powiększenie wykorzystywanych zasobów jest możliwe w każdej chwili, użytkownik chmury² płaci jedynie za wykorzystywane funkcjonalności infrastruktury informatycznej. Bez wątplenia w sektorze bankowym w ostatnich latach w coraz większym zakresie wykorzystywano nowe technologie, niemniej jednak pandemia znacznie przyspieszyła ten proces, ponieważ obecnie, w czasach gospodarki COVID i postCOVID, wykorzystywanie nowych technologii w działalności banku jest coraz istotniejszym elementem zapewnienia ciągłości i odpowiedniego poziomu oraz szybkości świadczonych usług.

Biorąc powyższe pod uwagę, na wstępie przywołać należy komunikat KNF z 23 stycznia 2020 roku dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej, który został wydany na skutek dostrzeżonej przez Komisję konieczności standaryzacji działalności w podejściu do korzystania z usług przetwarzania w chmurze obliczeniowej tych samych kategorii informacji przez podmioty nadzorowane sektora finansowego³.

Zgodnie z definicją zawartą w komunikacie, podmiotami nadzorowanymi są „[...] podmioty podlegające nadzorowi nad rynkiem finansowym zgodnie z ustawą z 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, art. 1 ust. 2 pkt. 1)–8)”. W odniesieniu do sektora bankowego oznacza to nadzór bankowy sprawowany zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 roku – Prawo bankowe, obejmujący zgodnie z art. 131 ust. 1 te same ustawy działalność banków⁴,

1 X. Konarski, *Przetwarzanie danych osobowych w chmurze obliczeniowej*, „Monitor Prawniczy” 2013, nr 8.

2 W niniejszym artykule określenie „użytkownik” należy rozumieć bank krajowy

3 Zgodnie z definicją legalną zawartą w komunikacie, chmura obliczeniowa jest 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

4 Zgodnie z art. 12 prawa bankowego, banki mogą być tworzone jako banki państwowe, spółdzielcze lub banki w formie spółek akcyjnych.

oddziałów i przedstawicielstw banków zagranicznych oraz oddziałów i przedstawicielstw instytucji kredytowych (dalej: podmioty nadzorowane).

Korzystanie w bankowości (przez podmioty nadzorowane) z oferowanej przez zewnętrznych usługodawców usługi tzw. chmury obliczeniowej odbywa się przede wszystkim na zasadach przewidzianych dla outsourcingu działalności bankowej (art. 6a–6e prawa bankowego). Szczegółowy zakres normatywny dotyczący korzystania przez banki krajowe z chmury obliczeniowej wynika głównie z aktów niższego rzędu, rekomendacji, standardów, wytycznych, które łącznie można określić mianem *soft law*⁵. Powyższe jest konsekwencją tego, że jest to tematyka stosunkowo nowa, bardzo technologiczna, z dużą dynamiką zmian wynikającym z szybkiego rozwoju tego obszaru gospodarki i technologii, za którym nie nadąża ustawodawca kształtujący prawo powszechnie obowiązujące na poziomie ustawowym. Jednym z wyżej wymienionych aktów *soft law* jest właśnie przywołany uprzednio komunikat KNF z 23 stycznia 2020 roku. Reguły zawarte w tego rodzaju akcie normatywnym, jakkolwiek nieposiadające przymiotu prawa powszechnie obowiązującego, mają na celu wskazanie podmiotom nadzorowanym oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego sektora bankowego.

Takie rozumowanie potwierdzone jest *explicite* w treści komunikatu (II. Wprowadzenie pkt 1 i 2, s. 5 oraz pkt 7, s. 6), gdzie KNF wskazuje, że „[...] postęp technologiczny w obszarze chmury obliczeniowej powoduje wątpliwości ze strony podmiotów nadzorowanych w zakresie możliwości stosowania tej technologii oraz – w przypadku dopuszczalności takiego rozwiązania – zasad dokonywania outsourcingu, w szczególności podczas przetwarzania informacji prawnie chronionych”, co więcej, KNF „[...] dostrzega brak standaryzacji w podejściu do korzystania z usług przetwarzania w chmurze obliczeniowej w odniesieniu do tych samych kategorii informacji przez podmioty nadzorowane sektora finansowego, co może prowadzić do istotnych różnic w ocenie ryzyka technologicznego, a tym samym powodować zwiększenie ryzyka sektorowego”. W konsekwencji do powyższego „Nadzór oczekuje, że podmioty nadzorowane będą informowały UKNF o zamiarze przetwarzania informacji w usługach chmury obliczeniowej, na zasadach określonych w niniejszym komunikacie”.

5 Więcej zob. T. Czech, *Charakter prawny rekomendacji Komisji Nadzoru Finansowego*, „Podstawy Prawa Publicznego” 2009, nr 11, s. 63–80.

To, co w największym stopniu interesuje autorów niniejszego artykułu, to analiza w zakresie konieczności albo braku konieczności stosowania przez podmioty nadzorowane reguł wynikających z komunikatu, w przypadku korzystania ze świadczonej przez podmiot zewnętrzny (outsourcing) usługi chmury obliczeniowej społecznościowej.

Analiza ta może zostać przeprowadzona na podstawie usług świadczonych na rzecz banków krajowych przez wyspecjalizowane podmioty niebankowe (podmioty trzecie), co może zostać zaklasyfikowane jako rodzaj outsourcingu usług z zakresu teleinformatycznej infrastruktury banku w formie chmury obliczeniowej społecznościowej przeznaczonej dla sektora bankowego, na zasadach przewidzianych w art. 6a i następnym prawa bankowego.

Taka standardowa usługa w zakresie chmury obliczeniowej społecznościowej polega na tym, że bank krajowy wprowadza dane poprzez przeznaczone do tego aplikacje zainstalowane na maszynach dla danego banku poprzez szyfrowane łącza, a następnie dane te są zapisywane i przetwarzane na serwerach administrowanych przez zewnętrznego usługodawcę. W chmurze obliczeniowej zewnętrzny usługodawca dokonuje operacji na wprowadzonych danych, bank zaś przesyła do zewnętrznego usługodawcy dane z wykorzystaniem systemu bankowego, który obsługują pracownicy banku, lub systemu bankowości elektronicznej – dane wprowadzane są bezpośrednio przez klientów banku.

W wielu przypadkach tego rodzaju usług mamy do czynienia przede wszystkim ze swoistym backup'em (w chmurze obliczeniowej) operacji/czynności, jakie przeprowadzane są w banku krajowym.

Zważywszy na zawarte w komunikacie KNF definicje legalne: chmury obliczeniowej publicznej⁶, chmury obliczeniowej prywatnej⁷, chmury obliczeniowej hybrydowej⁸ oraz chmury obliczeniowej społecznościowej⁹, na potrzeby

6 Chmura obliczeniowa publiczna – chmura obliczeniowa dostępna do użytku publicznego, będąca w posiadaniu lub bezpośrednio zarządzana przez dostawcę usług chmury obliczeniowej.

7 Chmura obliczeniowa prywatna – chmura obliczeniowa dostępna do wyłącznego użytku jednego podmiotu, będąca w jego posiadaniu lub bezpośrednio zarządzana przez ten podmiot.

8 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.

9 Chmura obliczeniowa społecznościowa – chmura obliczeniowa dostępna do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy o współpracy, ze zdefiniowanymi wspólnymi wymaganiami i zasadami m.in. w obszarze zgodności i bezpieczeństwa przetwarzania informacji, będąca w posiadaniu lub bezpośrednio zarządzana przez podmiot(-y) z grupy lub na jego (ich) zlecenie.

niniejszego artykułu założyć należy, że w przypadku wyżej wymienionej usługi świadczonej przez zewnętrznego usługodawcę na rzecz banków krajowych mamy do czynienia z chmurą obliczeniową społecznościową – co zostanie rozwinięte w dalszej części niniejszego artykułu.

W tym miejscu wskazać należy, że chmura obliczeniowa społecznościowa odznacza się tym, że jest dostarczana grupie podmiotów mających te same wymagania, a także cel w zakresie korzystania z tej technologii¹⁰. Mowa tutaj o wymogach dotyczących zapewnianych funkcjonalności, standardów bezpieczeństwa, wspólnych zasad postępowania etc. Jako przykład najczęściej wskazuje się chmurę społecznościową, która obsługuje określoną grupę odbiorców¹¹, np. tylko państwowe uczelnie wyższe.

W analizowanym przypadku usług świadczonych na rzecz banków krajowych można mówić o stworzeniu specjalnej społecznościowej chmury obliczeniowej kierowanej do wysoce wyspecjalizowanego i hermetycznego sektora banków krajowych i spełniającej wszystkie wymagania niezbędne do wykonywania działalności nadzorowanej przez te instytucje.

Zasoby informatyczne udostępniane w ramach społecznościowej chmury obliczeniowej są udostępniane do wyłącznego użytku specyficznej, ściśle określonej grupy użytkowników, którzy podejmują jednolite rodzajowo decyzje w zakresie zarządzania, nadzoru i zabezpieczenia chmury. Ta jednolitość rodzajowa decyzji w zakresie zapewnienia najwyższego poziomu bezpieczeństwa korzystania z chmur obliczeniowych wynika z tego, że banki krajowe są podmiotami (unijnymi instytucjami kredytowymi), których działalność podlega nadzorowi ostrożnościowemu i ścisłej reglamentacji w każdym państwie członkowskim UE, co skutkuje koniecznością wykonywania zaleceń nadzorczych kierunkowo spójnych dla całego obszaru UE.

Przykładowo, zgodnie z definicją Europejskiego Urzędu Nadzoru nad Ubezpieczeniami i Pracowniczymi Programami Emerytalnymi zawartą w dokumencie „Outsourcing to the cloud: eiopa’s contribution to the european commission fintech action” z 31 grudnia 2018 roku „[...] zasoby chmury społecznościowej mogą należeć, być zarządzane i utrzymywane przez jedną z organizacji należących do danej społeczności lub przez usługodawcę zewnętrznego. Zapewniane w jej ramach zasoby IT mogą znajdować się w lokalizacji

10 A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018, s. 79.

11 Ibidem.

członka lub kilku członków danej społeczności lub w lokalizacji zewnętrznego dostawcy”¹².

W tak prezentowanym ujęciu, co warte podkreślenia, może być to nawet hostowanie (hosting) przez podmiot trzeci (usługodawcę) chmury społecznościowej, z której korzystają określone organizacje zlecające ten hosting. W realiach analizowanego zagadnienia można przyjąć, że zewnętrzny usługodawca, który posiada własną i adekwatną do świadczonych usług infrastrukturę teleinformatyczną, buduje chmurę obliczeniową społecznościową przeznaczoną wyłącznie dla wysoce wyspecjalizowanego i hermetycznego sektora reglamentowanych banków krajowych, co można potraktować jako hosting jednego rodzaju użytkowników. Oznacza to, że banki krajowe są wyłącznymi użytkownikami tej infrastruktury, zarządzanie zaś infrastrukturą pozostaje w gestii podmiotu trzeciego.

Powyższe nie zmienia, że to banki krajowe decydują o sposobie zarządzania usługą dostępową na podstawie zawartych umów z usługodawcą zewnętrznym (*vide*: możliwość rozszerzenia korzystania z zasobów infrastruktury usługodawcy czy też ze względu na nowe wymagania prawne, jakie nakładają na banki przepisy prawa lub zalecenia nadzorów ostrożnościowych).

Ze względu na to, że zewnętrzny usługodawca posiada swoją infrastrukturę informatyczną oraz odpowiednie oprogramowanie do świadczenia usług chmurowych, jego działalność polega na udostępnianiu tej infrastruktury informatycznej bankom krajowym, które są jej wyłącznym użytkownikiem. W takim ujęciu świadczenie usługi chmury na rzecz banków krajowych można uznać za chmurę obliczeniową społecznościową.

Komisja Nadzoru Finansowego w komunikacie zdefiniowała chmurę obliczeniową społecznościową jako chmurę obliczeniową dostępną do wyłącznego użytku grupy podmiotów powiązanych kapitałowo lub na mocy wspólnej umowy o współpracy ze zdefiniowanymi wspólnymi wymaganiami i zasadami m.in. w obszarze zgodności i bezpieczeństwa przetwarzania informacji, będącą w posiadaniu lub bezpośrednio zarządzaną przez podmiot(-y) z grupy lub na jego (ich) zlecenie (pkt I ust. 1 ppkt 7, s. 2).

12 The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises; Outsourcing to the cloud: eiopa's contribution to the european commission fintech action plan 31.12.2018 r, s. 8.

Przedstawiony powyżej model usług świadczonych przez usługodawcę zewnętrznego na rzecz banków krajowych wpisuje się w powyższą definicję, ponieważ oferowana chmura obliczeniowa społecznościowa: 1) jest przeznaczona do wyłącznego użytku banków krajowych; 2) prowadzenie przez banki krajowe działalności nadzorowanej wymaga tego samego poziomu bezpieczeństwa przetwarzania informacji (wspólne wymagania i zasady); 3) zarządzanie zasobami chmury dokonywane jest przez podmiot trzeci (zarządzana przez podmiot(-y) z grupy lub na jego (ich) zlecenie).

Powstaje zatem pytanie, czy chmura obliczeniowa społecznościowa jest objęta komunikatem KNF?

Zagadnienie, czy chmura obliczeniowa społecznościowa jest objęta zakresem normatywnym wynikającym z komunikatu nie jest proste z uwagi na zauważalną niespójność w treści tego komunikatu.

Bezspornie komunikat KNF dotyczy *explicite* chmury obliczeniowej publicznej i chmury obliczeniowej hybrydowej. Analogicznie skonstruowany został wzór informacji podmiotu nadzorowanego w sprawie przetwarzania w chmurze obliczeniowej informacji przekazywanej do UKNF, który to wzór stanowi załącznik nr 1 do komunikatu, a który również dotyczy chmury obliczeniowej publicznej i chmury obliczeniowej hybrydowej. To oznacza, że komunikat bezpośrednio nie dotyczy chmury obliczeniowej społecznościowej.

Podobnie jest w przypadku przewidzianego *explicite* w treści komunikatu wyłączenia jego stosowania wobec chmury obliczeniowej prywatnej (pkt IV ust. 8 wytycznych stosowania – komunikat nie dotyczy przetwarzania informacji w chmurze obliczeniowej prywatnej). To oznacza, że komunikat bezpośrednio nie wyłącza stosowania wobec chmury obliczeniowej społecznościowej.

Można uznać, że autorzy komunikatu ani nie przesadzili o jego zastosowaniu w przypadku chmury obliczeniowej społecznościowej, ani też nie przesadzili o braku stosowania komunikatu w przypadku chmury obliczeniowej społecznościowej.

Tym samym odrębne zdefiniowanie chmury obliczeniowej społecznościowej (komunikat pkt I ust. 1 ppkt 7, s. 2) miało służyć wyłącznie dodefiniowaniu pojęcia chmury obliczeniowej hybrydowej (komunikat pkt I ust. 1 ppkt 6, s. 2), gdzie chmura hybrydowa została określona jako: „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”.

Jeżeli KNF ani nie przesądził o zastosowaniu komunikatu do chmury społecznościowej, ani też nie przesądził o wyłączeniu stosowania komunikatu do chmury społecznościowej, a nadto w treści komunikatu nie przysłał chmurze społecznościowej (odrębnymi postanowieniami/regulacjami) jakiegokolwiek szczególnej roli, należy uznać, że pojęcie chmury społecznościowej ma jedynie wspierać lepsze rozumienie, czym jest chmura hybrydowa, która może składać się z połączeniu różnych rodzajów chmur, w tym także chmury społecznościowej.

Innymi słowy, analiza postanowień komunikatu skłania do wniosku, że KNF zdefiniował pojęcie chmury społecznościowej jedynie po to, żeby ukazać różnorodność możliwości tworzenia chmury hybrydowej przez różne typy chmur – w tym także chmurę społecznościową. W treści komunikatu (oprócz definicji legalnej) pojęcie „chmura społecznościowa” pojawia się tylko raz, i to w marginalnym ujęciu na s. 16, gdzie określone są elementy umowy z dostawcą usług chmury obliczeniowej i wskazywane jest, że podmiot nadzorowany może korzystać z ramowych umów udostępnianych przez dostawców usług chmury obliczeniowej, w szczególności wówczas, gdy dotyczą one usług chmury obliczeniowej tworzonej dla grupy podmiotów (w tym podmiotu nadzorowanego) w ramach umów o charakterze korporacyjnym lub grupowym, w tym również chmury obliczeniowej społecznościowej.

W ten sposób widać wyraźnie, że KNF w komunikacie nie nadaje chmurze społecznościowej jakiegokolwiek istotnego i autonomicznego znaczenia, wręcz przeciwnie, jest ona zakamuflowana pod innymi pojęciami.

W konsekwencji do powyższego przyjąć należy, że jeżeli chmura społecznościowa tworzy/współtworzy chmurę hybrydową, która wówczas składa się z połączenia dwóch lub więcej osobnych chmur obliczeniowych (publicznej, prywatnej, społecznościowej), to w takim przypadku będą miały zastosowanie postanowienia komunikatu KNF, bo taki jest sens zdefiniowania chmury społecznościowej w jego treści.

W tym miejscu należy wskazać pewną niespójność w rozumowaniu KNF, gdyż na s. 7 komunikatu zaznacza on, że „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, jeżeli: 1) przetwarzane informacje należą do informacji prawnie chronionych w rozumieniu niniejszego komunikatu lub 2) przetwarzanie informacji ma charakter outsourcingu szczególnego chmury obliczeniowej w rozumieniu niniejszego komunikatu i przetwarzanie informacji jest realizowane w chmurze

obliczeniowej publicznej lub hybrydowej (w zakresie jej części opartej o chmurę obliczeniową publiczną)” (pkt IV. Wytyczne stosowania).

Niespójność komunikatu polega na tym, że albo celem zdefiniowania chmury społecznościowej jest swoiste dodefniowanie (lepiej i bardziej ilustratywne zrozumienie pojęcia) chmury hybrydowej, a tym samym rozszerzenie zakresu stosowania komunikatu albo (zgoła przeciwnie) celem jest zwężenie stosowania komunikatu w przypadku chmur hybrydowych wyłącznie do części opartej na chmurze publicznej.

Jednakże nawet zauważalna niespójność w treści komunikatu nie zmienia faktu, że jeżeli uznać, że chmura społecznościowa oferowana przez spółkę na rzecz instytucji kredytowych, od strony funkcjonalnej i technologicznej nie współtworzy chmury hybrydowej, czyli nie łączy się z innymi chmurami, to jako odrębna chmura społecznościowa nie jest objęta zakresem normatywnym komunikatu, gdyż nie jest on do tego rodzaju chmury adresowany *explicite*.

W konsekwencji do powyższych konkluzji, jeżeli przyjąć, że ofertowana przez spółkę chmura społecznościowa nie jest funkcjonalnie (technologicznie) powiązana z innymi chmurami i tym samym nie współtworzy chmury hybrydowej, to nie jest objęta zakresem normatywnym wynikającym z komunikatu, a tym samym podmioty nadzorowane nie muszą w przypadku tej chmury wypełniać obowiązków informacyjnych, o jakich stanowi rozdział VIII komunikatu.

Odrębny rozdział VIII tego komunikatu zatytułowany „Zasady informowania UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej” (s. 21–22) nakłada obowiązki informacyjne na te podmioty nadzorowane, które komunikatem tym są objęte¹³.

Nie zmienia to faktu, że obowiązek ten nie ma wtedy zastosowania, gdyż podmiot nadzorowany zamierza skorzystać z przetwarzania informacji w chmurze obliczeniowej społecznej, która (jak to zostało wskazane wyżej) w ogóle nie podlega komunikatowi.

Konkludując powyższe rozważania, należy podkreślić, że: 1) według autorów *soft law* w postaci omawianego komunikatu KNF zawiera zespół norm

13 W tym rozdziale KNF wskazuje *explicite*, że w przypadkach outsourcingu szczególnego chmury obliczeniowej lub przetwarzania informacji prawnie chronionej podmiot nadzorowany, w terminie 14 dni przed rozpoczęciem przetwarzania informacji w chmurze obliczeniowej, informuje UKNF o: 1) rodzaju i zakresie informacji planowanych do przetwarzania/przetwarzanych w chmurze obliczeniowej; 2) nazwie dostawcy usług chmury obliczeniowej oraz rodzaju planowanych do używania/używanych usług chmury obliczeniowej.

przesądających o braku konieczności stosowania przez podmioty nadzorowane reguł wynikających z komunikatu w przypadku korzystania ze świadczonej przez podmiot zewnętrzny (outsourcing) usługi chmury obliczeniowej społecznościowej; 2) powyższe (w konsekwencji) powoduje, że banki krajowe korzystające z usługi chmury obliczeniowej społecznościowej nie podlegają obowiązkom sprawozdawczym wobec KNF; 3) to zaś w swoich skutkach powoduje, że tego rodzaju outsourcing jest i będzie stale rozwijany w działalności banków krajowych zarówno w realiach gospodarki COVID, jak i gospodarki postCOVID.

Bibliografia

- Czech T., *Charakter prawny rekomendacji Komisji Nadzoru Finansowego*, „Podstawy Prawa Publicznego” 2009, nr 11.
- Konarski X., *Przetwarzanie danych osobowych w chmurze obliczeniowej*, „Monitor Prawniczy” 2013, nr 8.
- Krasuski A., *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018.
- Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe, t.j., Dz.U. 2019, poz. 2357, z późn. zm.

The principles of using the so-called social cloud computing service by national banks in the times of COVID and post-COVID economy, in the light of the Communication published by the Polish Financial Supervision Authority

Abstract

The purpose of this paper is to illustrate selected legal aspects of the highly relevant issue these days, namely using external services of the so-called social cloud computing by national banks, in the face of restrictions on the traditional operations of IT departments in banks, in the times of COVID and post-COVID economy. The restrictions imposed to contain COVID-19 made the bank products offered through the available communication and information systems highly popular among customers. Moreover, due to the risk concerning restrictions on the employees of IT departments staying in office space, the opportunity to use “external server rooms” (placed in the cloud) is an important aspect of operations of national banks, both in the present economic situation and in future. Importantly, this issue is the object of a definite interest of the Polish Financial Supervision Authority which, necessarily, forms the basis for analysing the regulations discussed below.

Key words: COVID-19, national bank, computing cloud