Brykając wśród wirtualnych obłoków

czyli krócej o tym, jak sprawić, aby nad polskim rynkiem finansowym wreszcie pojawiły się chmury obliczeniowe

Bryk I – podstawy oraz na co zwrócić uwagę

Wprowadzenie

W styczniu 2020 roku Urząd Komisji Nadzoru Finansowego (KNF) wydał Komunikat, który wkrótce zaczął być określany jako Komunikat Chmurowy KNF (Komunikat). Jakiś czas później, KNF opublikował listę najczęściej zadawanych pytań i odpowiedzi (Q&A), które były aktualizowane w miarę ich zgłaszania przez różnych uczestników rynku finansowego w Polsce. Ostatnia aktualizacja Q&A miała miejsce pod koniec marca 2021 roku. Poniższa, praktyczna analiza i streszczenie informacji zawartych w treści Komunikatu pozwolą podmiotom nadzorowanym przez KNF, jak również potencjalnym dostawcom usług IT, którzy świadczą je na rzecz tych podmiotów, zrozumieć jego najważniejsze aspekty i wynikające z niego konkluzje. Ze względu na obszerność tematu, całość analizy została podzielona na dwie części:

- **Bryk I** – podstawy oraz na co zwrócić uwagę
- **Bryk II** – jak przygotować swój pierwszy krok w chmurach, a następnie z nich nie spaść

Źródło:

Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z dnia 23 stycznia 2020 roku link

Pytania i odpowiedzi (Q&A) w zakresie stosowania Komunikatu UKNF z dnia 23 stycznia 2020 roku link

MARCIN STADNIK
HEAD OF SII FINANCIAL SERVICES,
BANKING & INSURANCE INDUSTRY

Kogo rzecz dotyczy?

Zakres podmiotowy stosowania Komunikatu jest tożsamy z zakresem nadzoru nad rynkiem finansowym sprawowanym przez Komisję Nadzoru Finansowego. Wszystkie podmioty nadzorowane są zobowiązane do stosowania wytycznych Komunikatu. Zatem należy pamiętać, iż poza całkiem oczywistymi uczestnikami rynku zaliczają się do nich również:

- **agenci ubezpieczeniowi**, przetwarzający w chmurze obliczeniowej informacje prawnie chronione
- podmioty infrastruktury rynku kapitałowego, firmy inwestycyjne
- **fundusze inwestycyjne** – jeśli ich **agenci transferowi**, którzy prowadzą na zlecenie funduszy inwestycyjnych rejestr uczestników, wykorzystują do tej czynności usługę chmury obliczeniowej, to do takich funduszy również odnoszą się wytyczne Komunikatu. Obowiązek w tym zakresie, jako organ funduszu, realizuje TFI.
- **oddziały zagraniczne** zakładów ubezpieczeń i zakładów reasekuracji w rozumieniu Ustawy o Działalności Ubezpieczeniowej i Reasekuracyjnej (UDUR)
- **MIP, AISP i PISP***

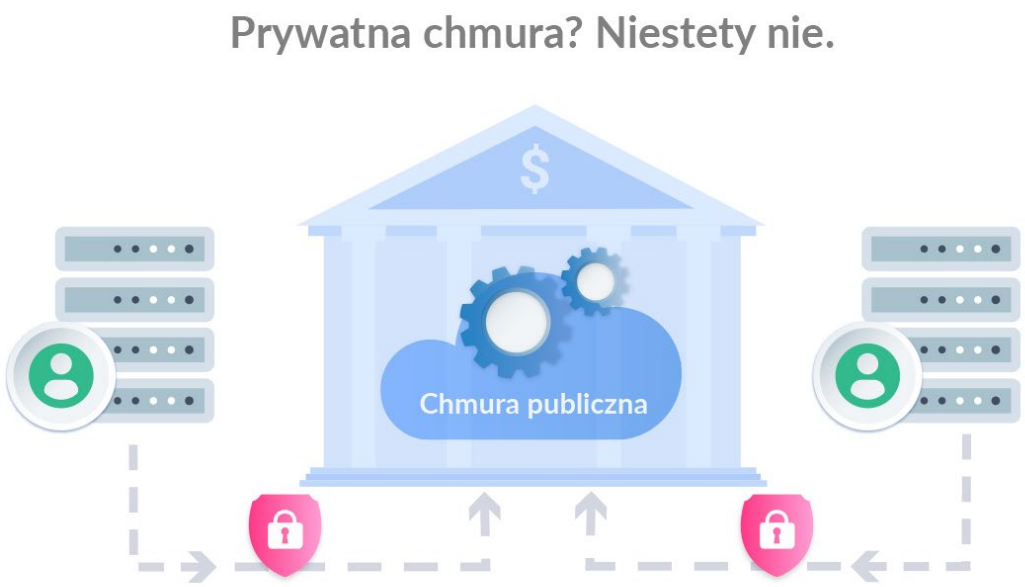
* W ramach PSD2, odpowiednio: Mała Instytucja Płatnicza, Account Information Service Provider, Payment Initiation Service Provider są podmiotami nadzorowanymi w rozumieniu Ustawy o nadzorze KNF, dlatego Komunikat ma do nich zastosowanie w całości.

Rodzaje chmur według Komunikatu

Najważniejsze definicje::

- **chmura** obliczeniowa **publiczna** – chmura obliczeniowa dostępna do użytku publicznego, będąca w posiadaniu lub bezpośrednio zarządzana przez dostawcę usług chmury obliczeniowej; zasoby chmury są współdzielone z innymi podmiotami
- **chmura** obliczeniowa **prywatna** – chmura obliczeniowa dostępna do wyłącznego użytku jednego podmiotu, będąca w posiadaniu lub bezpośrednio zarządzana przez ten podmiot
- **chmura** obliczeniowa **hybrydowa** – chmura obliczeniowa, składająca się z połączenia dwóch lub więcej osobnych chmur obliczeniowych (publicznej, prywatnej, społecznościowej), która pozwala na przenoszenie czynności przetwarzania informacji pomiędzy chmurami obliczeniowymi, które ją tworzą
- **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; może mieć charakter publiczny lub prywatny – zależnie od tego, kto posiada lub bezpośrednio zarządza infrastrukturą chmury:
    - jeśli dostawca, to chmura jest publiczna
    - jeśli podmiot nadzorowany (samodzielnie lub we współpracy z innymi podmiotami nadzorowanymi w ramach umowy o współpracy lub grupy kapitałowej), to chmura jest prywatna

Chmura społecznościowa **prywatna nie może być zarządzana przez podmiot trzeci** w imieniu podmiotów nadzorowanych.



Kluczowe aspekty rozróżniające chmury obliczeniowe:

- wyłączność dostępu do chmury lub brak wyłączności po stronie podmiotu nadzorowanego
- posiadanie lub bezpośrednie zarządzanie chmurą przez podmiot nadzorowany
- **Posiadanie lub bezpośrednie zarządzanie** oznacza w szczególności (choć nie wyłącznie):
    - możliwość wprowadzania zmian w infrastrukturze (w tym wymianę sprzętu, aktualizację oprogramowania),
    - decydowanie o zasadach fizycznego dostępu do infrastruktury,
    - decydowanie o zasadach ochrony fizycznej i logicznej infrastruktury.

Posiadanie chmury obliczeniowej **nie oznacza**, że podmiot nadzorowany powinien być jednocześnie jej właścicielem. Podmiot nadzorowany powinien natomiast zapewnić bezpieczne, pod względem prawnym i faktycznym, posiadanie chmury obliczeniowej przez okres korzystania z niej, uwzględniając przy tym czas potrzebny do bezpiecznego zrealizowania migracji do innej chmury obliczeniowej lub wycofania się z chmury obliczeniowej do infrastruktury *on-premise*.

Bezpośrednie zarządzanie chmurą obliczeniową oznacza, że podmiot nadzorowany **bez udziału podmiotu trzeciego** kontroluje chmurę obliczeniową **w ramach zasobów personalnych pozostających w jego wyłącznej dyspozycji i pod jego kontrolą**. Osoby zarządzające chmurą obliczeniową powinny wykonywać czynności na rzecz podmiotu nadzorowanego w relacji bezpośredniej, tj. bez pośrednictwa podmiotów trzecich, np.::

- kadra IT nie może świadczyć usług na rzecz podmiotu nadzorowanego poprzez agencję pracy,
- wykonywanie czynności nie może się odbywać poprzez oddelegowanie konkretnej osoby przez spółkę informatyczną, z którą podmiot nadzorowany ma podpisaną umowę na obsługę IT,
- czynności nie mogą być wykonywane poprzez oddelegowanie konkretnej osoby przez spółkę IT w ramach grupy kapitałowej, do której należy podmiot nadzorowany.

Nieoczywiste przykłady chmury publicznej, które z pozoru wydają się prywatne

Jeżeli:

- miejscem fizycznej instalacji infrastruktury IT jest serwerownia własna podmiotu nadzorowanego lub wybrane przez podmiot nadzorowany centrum przetwarzania danych

oraz

- zarządzanie chmurą jest zdalne, wykonywane poprzez bezpieczne połączenie internetowe przez dostawcę usługi chmury obliczeniowej lub podmiot trzeci,

to tak skonfigurowana usługa stanowi **chmurę publiczną**.

Jeżeli:

- infrastruktura chmury nie jest przeznaczona do wyłącznego użytku jednego podmiotu,
- podmiot nadzorowany może utworzyć wirtualną chmurę prywatną na skalowalnej infrastrukturze dostawcy usług chmury obliczeniowej (np. Virtual Private Cloud),

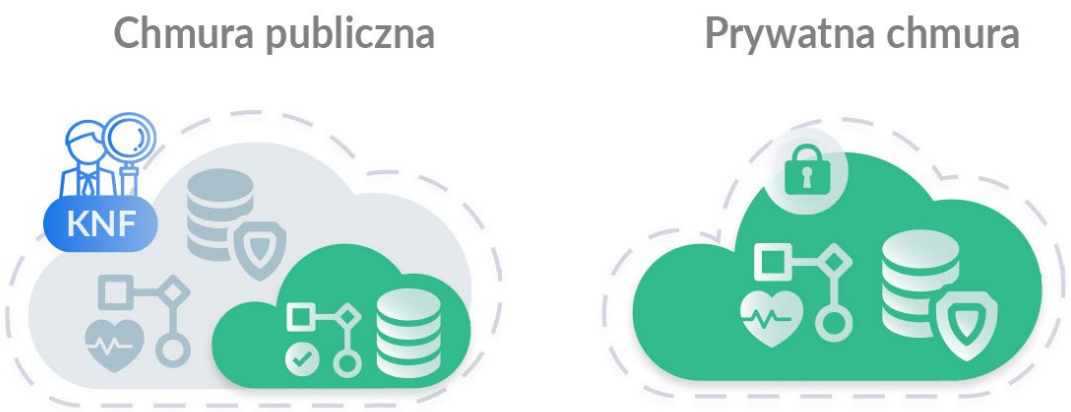
to tak skonfigurowana usługa jest świadczona jako **chmura publiczna**.

Korzystanie przez podmiot nadzorowany z serwerów wirtualnych z gwarancją zasobów (VPS – Virtual Private Server), które polegają na wirtualnym podziale maszyny fizycznej na kilka mniejszych serwerów wirtualnych, **nie może zostać uznane za korzystanie z chmury prywatnej** w rozumieniu Komunikatu. Korzystając z serwerów wirtualnych, podmiot nadzorowany nie zarządza bezpośrednio infrastrukturą chmurową, na której funkcjonuje serwer wirtualny, zatem mamy do czynienia z **chmurą publiczną**.

Korzystanie z chmury obliczeniowej przez podmioty nadzorowane w opisany powyżej sposób **jest dozwolone**, jednak **wiąże się z obowiązkiem stosowania Komunikatu**.

Tylko **bezpośrednie zarządzanie chmurą przez podmiot nadzorowany** (wraz z wyłącznym użytkowaniem infrastruktury w modelu IaaS, ale nie w modelach **PaaS i SaaS**) skutkuje uznaniem usługi za **chmurę prywatną**.

Natomiast w sytuacji, gdy świadczona przez podmiot trzeci usługa wykorzystuje usługi **chmury obliczeniowej prywatnej** (posiadanej i zarządzanej przez podmiot trzeci), podmiot nadzorowany korzysta z **chmury publicznej**.



Kiedy outsourcing chmury jest szczególny?

Usługa przetwarzania informacji w chmurze obliczeniowej ma charakter powierzenia czynności przetwarzania i – zależnie od kategorii przetwarzanych informacji oraz faktycznie realizowanych czynności przetwarzania – może być traktowana jako outsourcing chmury obliczeniowej lub outsourcing szczególny chmury obliczeniowej.

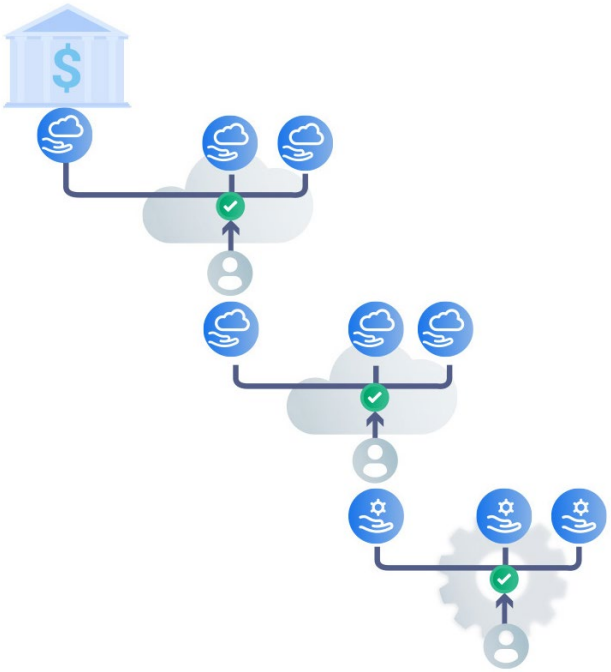
- **outsourcing chmury obliczeniowej** oznacza umowę, na mocy której dostawca usług chmury obliczeniowej dostarcza podmiotowi nadzorowanemu usługę, która służy do wsparcia realizacji procesu, usługi lub zadania, które podmiot nadzorowany realizowałby samodzielnie, gdyby usługa chmury obliczeniowej była niedostępna.
- **outsourcing szczególny chmury obliczeniowej** oznacza outsourcing, 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 **wpływałaby w sposób istotny na ciągłość** wypełniania przez podmiot nadzorowany warunków stanowiących podstawę uprawnienia do prowadzenia działalności nadzorowanej lub jej wykonywania lub **zagrażałaby w sposób istotny wynikom finansowym** podmiotu nadzorowanego, **niezawodności lub ciągłości** wykonywania działalności nadzorowanej..

Podstawą definicji **outsourcingu szczególnego** jest zatem pojęcie krytycznych i istotnych funkcji, działań i procesów podmiotu nadzorowanego z perspektywy wykonywanej działalności nadzorowanej.

Podmiot nadzorowany powinien w sposób ciągły monitorować, jakie procesy i w jakim zakresie są przetwarzane z wykorzystaniem chmury obliczeniowej na wypadek, gdyby zmieniła się **skala ocenianego proces**u. Proces, który wyjściowo nie był oceniany jako krytyczny i istotny, może z biegiem czasu zwiększyć swoją skalę i w rezultacie powinien zostać przekwalifikowany jako kluczowy i krytyczny.

KNF zastrzega sobie możliwość weryfikacji oceny dokonanej przez podmiot nadzorowany w zakresie krytyczności i istotności danego procesu. Dlatego **podmiot nadzorowany powinien posiadać udokumentowane uzasadnienie dotyczące kwalifikacji wszystkich procesów i funkcji w kontekście ich krytyczności i istotności**.

Łańcuchy outsourcingowe



W jakich przypadkach należy stosować wytyczne Komunikatu?

Zakres przedmiotowy – podmiot nadzorowany powinien określić – w odniesieniu do każdej planowanej lub już wykorzystywanej usługi chmury obliczeniowej – czy przetwarzane są **informacje prawnie chronione**, oraz, czy czynność przetwarzania może być definiowana jako **outsourcing szczególny** chmury obliczeniowej. Jeżeli chmura obliczeniowa jest wykorzystywana do czynności mających związek z działalnością regulowaną, to Komunikat ma zastosowanie.

KNF oczekuje od podmiotów nadzorowanych stosowania modelu referencyjnego, określonego w Komunikacie, jeżeli:

- przetwarzane informacje należą do **informacji prawnie chronionych**

  lub
- przetwarzanie informacji ma charakter **outsourcingu szczególnego** chmury obliczeniowej

  i
- przetwarzanie informacji jest realizowane w chmurze obliczeniowej **publicznej** lub **hybrydowej** (w zakresie jej części opartej o chmurę obliczeniową publiczną).

Komunikat nie dotyczy przetwarzania informacji w chmurze obliczeniowej prywatnej.

Podmiot nadzorowany powinien określić, czy przetwarzane są **informacje prawnie chronione** oraz czy czynność przetwarzania może być definiowana jako **outsourcing szczególny** chmury obliczeniowej.

» Zatem, jeśli przetwarzanie dotyczy informacji innych niż prawnie chronione i outsourcing nie kwalifikuje się jako szczególny, to Komunikat może, ale nie musi być stosowany.

W przypadku wątpliwości, należy przyjąć do stosowania wymaganie bardziej rygorystyczne.

Stosowanie Komunikatu powinno odbywać się z poszanowaniem **zasady proporcjonalności** przy równoległym uwzględnieniu modelu referencyjnego. Zasada proporcjonalności powinna być zastosowana na etapie szacowania ryzyka związanego z planowaniem czynności przetwarzania oraz adekwatnością stosowanych zabezpieczeń przetwarzanych informacji. Zasada proporcjonalności nie powinna być interpretowana jako przyzwolenie na zastosowanie przez **mniejsze podmioty nadzorowane mniej efektywnych zabezpieczeń** przetwarzanych informacji niż opisane w Komunikacie. Innymi słowy, chodzi o stosowanie tej zasady proporcjonalnie do oszacowanego ryzyka, a nie do skali podmiotu nadzorowanego.

Komunikatu nie stosuje się, gdy odpowiednie, szczególne przepisy prawa nakładają wymóg spełnienia określonych wymagań technicznych lub organizacyjnych dotyczących przetwarzania określonych informacji, które wykluczałyby możliwość spełnienia wymagań Komunikatu. Czyli inaczej mówiąc:

» Komunikat stanowi „nakładkę" na szczególne przepisy prawa obowiązujące daną kategorię podmiotów nadzorowanych, jednak w przypadku sprzeczności wymagań Komunikatu ze specyficznymi postanowieniami tych przepisów, nadrzędną wytyczną stanowią te przepisy prawa.

Komunikat nie musi być stosowany podczas projektowania i eksploatacji **środowisk testowych lub rozwojowych** w chmurze obliczeniowej, o ile w środowiskach tych **nie są przetwarzane informacje prawnie chronione**.

Informacje prawnie chronione muszą być szyfrowane zawsze at rest oraz in transit.

Ale co z regulacjami UE dotyczącymi outsourcingu i chmury obliczeniowej?

Komunikat jest podejściem krajowym do outsourcingu przetwarzania informacji w chmurze obliczeniowej dla sektora finansowego (**model referencyjny**). Wytyczne, zalecenia lub inne dokumenty prezentujące stanowisko europejskich organów nadzorczych, które odnoszą się do przetwarzania informacji w chmurze obliczeniowej publicznej lub hybrydowej, **nie mają zastosowania do podmiotów nadzorowanych** w zakresie, w jakim są sprzeczne z Komunikatem. **Obowiązujące** w takiej sytuacji **jest krajowe podejście określone w Komunikacie**.

Łańcuchy w chmurach, czy chmury w łańcuchach?

Łańcuch outsourcingowy

- relacja polegająca na powierzeniu przez dostawcę usług chmury obliczeniowej części czynności (służących dostarczaniu usługi chmury obliczeniowej dla podmiotu nadzorowanego) swojemu poddostawcy i dalszym (kolejnym) poddostawcom

lub

- relacja polegająca na dostarczaniu przez dostawcę usług chmury obliczeniowej usługi chmury obliczeniowej innemu dostawcy, który wykorzystuje usługę chmury obliczeniowej do świadczenia własnej usługi dla podmiotu nadzorowanego

Oczywiście wszystko w granicach outsourcingu dopuszczalnego przez przepisy prawa, obowiązujące dany podmiot nadzorowany. Podmiot nadzorowany powinien dokonać oceny dopuszczalności przekazania określonego rodzaju danych w zakresie dopuszczalnego przepisami łańcucha outsourcingowego, tj. np. liczby podmiotów w nim występujących.

Admissibility and scope Dopuszczalność i zakres powierzenia czynności dotyczących **informacji prawnie chronionych** przez podmiot nadzorowany powinna być interpretowana w ten sposób, że **brak zakazu poszczególnych działań nie jest dopuszczeniem** do wykonywania określonej działalności.

- **Poddostawca** to podmiot, który świadczy usługi dla dostawcy usług chmury obliczeniowej, służące dostarczaniu usługi chmury obliczeniowej dla podmiotu nadzorowanego i posiada albo może posiadać identyfikowalny dostęp do informacji przetwarzanych przez podmiot nadzorowany.

Jeżeli nie posiada lub nie może posiadać dostępu do informacji, to nie jest poddostawcą.

- **Tenant** – instancja usług chmury obliczeniowej przypisanych do podmiotu nadzorowanego. Najważniejszą właściwością tenantu jest jego domyślna, **logiczna separacja (konfiguracji oraz przetwarzanych informacji)** od innych tenantów.

Każdy podmiot nadzorowany może posiadać wiele tenantów u tego samego dostawcy usług chmury obliczeniowej, jednak wszystkie wymagania związane z separacją tenantów muszą być zachowne.

SaaS – jeżeli dostawca (inny niż chmurowy) oferuje usługę polegającą na dostarczaniu oprogramowania w modelu SaaS na rzecz wielu podmiotów nadzorowanych, a **dane tych podmiotów są separowane tylko w sposób logiczny**, tj. każdy podmiot nadzorowany posiada własną niezależną instancję systemu, to z punktu widzenia podmiotu nadzorowanego, niezależnie od modelu innych usług, z których korzysta dostawca (inny niż chmurowy), usługa jest oferowana w modelu chmury publicznej.

Fakt nieposiadania przez podmiot nadzorowany **relacji umownych z poddostawcą nie zwalnia z realizacji powinności określonych w Komunikacie**. Podmiot nadzorowany powinien więc samodzielnie upewnić się, jakie zabezpieczenia prawne, korporacyjne lub logiczne pozwolą na skuteczne zastosowanie postanowień Komunikatu i przepisów prawa przez poddostawcę. KNF rekomenduje, aby w proces oceny zapewnienia bezpieczeństwa przetwarzania **informacji prawnie chronionych** i informacji objętych **outsourcingiem szczególnym** zaangażowany był bezpośrednio poddostawca chmurowy.

- **Ujawnienie informacji** oznacza sytuację, w 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.

Na koniec bardzo istotne stanowisko KNF, wyraźnie i kilkukrotnie podkreślone w Komunikacie i zestawieniu Q&A:

» szyfrowanie informacji nie zmniejsza ważności informacji, nie zmienia też jej klasyfikacji i oceny (np. jako informacji prawnie chronionych), w tym, w szczególności, **szyfrowanie nie może zostać uznane za usunięcie danych** z infrastruktury dostawcy usług chmurowych.

Jeśli chcesz dowiedzieć się więcej o praktycznych aspektach wytycznych KNF odnośnie tego, jak przygotować się do migracji do chmury, czego oczekiwać od dostawców chmury, a także, jak prawidłowo powiadomić KNF o swoich planach migracji do chmury, zapoznaj się z drugą częścią opracowania, którą opublikujemy wkrótce.