Partner strategiczny raportu

COMARCH

Partnerzy raportu

Google Cloud IBM pwc salesforce

Transformacja banku do chmury

Wydawcy raportu

Związek Banków Polskich 1991-2021

Centrum Prawa Bankowego i Informacji
www.cpb.pl

BANK 1992-2022

aleBank.pl

Comarch Cloud Factoring

Expand your business without having to think about the system capacity and performance. Comarch Cloud Factoring automatically adjusts resources to keep pace with your factoring business.

Key benefits:

- **Fast implementation**
- **Continuous improvement**
- **Excellent UX**
- **Support from specialists**

www.finance.comarch.com finance@comarch.com

COMARCH

DIGITAL BANKING ACADEMY 2022

Związek Banków Polskich

Centrum Prawa Bankowego i Informacji
www.cpb.pl

Organizatorzy

Weź udział w czwartej edycji interaktywnych warsztatów online z zakresu nowoczesnych rozwiązań cyfrowych!

TEMATYKA Najbardziej aktualne i przyszłościowe zagadnienia cyfrowe. Szczegółowe, pogłębione i przede wszystkim merytoryczne wystąpienia. Otwarta dyskusja. Czas na zadawanie pytań. Materiały szkoleniowe.

PRELEGENCI Wybitni eksperci i praktycy reprezentujący czołowe kancelarie prawne, największe banki, wyróżniających się dostawców technologii, pracowników uczelni, firm doradczych i najbardziej innowacyjne firmy z Polski i świata.

PERSPEKTYWY Każdy temat przewodni omawiamy z perspektywy prawnej, regulacyjnej, biznesowej i technologicznej. Dzięki temu w pełni zrozumiesz omawiany obszar, poznając korzyści, wyzwania i ograniczenia z kilku perspektyw.

CZAS Zaoszczędź czas. Dołącz do nas i zdobądź skondensowaną dawkę wiedzy podczas całodziennego, interaktywnego szkolenia online.

2019/2021

3 edycje | **34** warsztaty | **261** godzin wykładów | **300+** Ekspertów | **2600+** Uczestników

HARMONOGRAM 2022

Każdy z warsztatów online jest dostępny jako autonomiczny moduł, jednak rekomendowaną formą jest realizacja kursu w całości.

Wlecieć w chmurę – jak rozpocząć wdrażanie chmury w banku?/ styczeń
Nowe oblicze HR. Nowe technologie w HR/ luty
DeFi – zdecentralizowane finanse i rola blockchain w bankowości/ marzec
Otwarta bankowość w Polsce i globalnie/ kwiecień
Halo tu robot. Jak wykorzystać sztuczną inteligencję w banku?/ kwiecień
Monitoring legislacyjny 2022 – bankowość elektroniczna i nowe technologie/ maj
Jest internet rzeczy (IoT), czas na internet zachowań (IoB)/ maj
Naturalne interfejsy użytkownika, identyfikacja i uwierzytelnianie/ wrzesień
Uczenie maszynowe i inteligentne systemy/ wrzesień
Technologie w służbie ESG/ październik
Mobilna rewolucja/ listopad
Banki i fintechy – konkurencja, współpraca, banki hybrydowe/ grudzień

KOSZT

399 ZŁ MODUŁ/os.

299 ZŁ MODUŁ/os.
(zgł. grupowe – 3 os. i więcej)

~~4788 ZŁ~~
3000 ZŁ! PAKIET 12 SZKOLEŃ

WWW.DIGITALBANKINGACADEMY.COM.PL

Patroni medialni

aleBank.pl BANK

Kontakt:
Katarzyna Cechowska-Jastrzębska
k.cechowska@wydawnictwocpb.pl
tel. (22) 623 84 53; tel. kom. 885 885 923

Transformacja banku do chmury

Raport przygotowany przez
Związek Banków Polskich
oraz Centrum Prawa Bankowego i Informacji

© Copyright by Związek Banków Polskich
© Copyright by Centrum Prawa Bankowego i Informacji

Związek Banków Polskich

Centrum Prawa Bankowego i Informacji
www.cpb.pl

Warszawa, grudzień 2021
Wydawnictwo Centrum Prawa Bankowego i Informacji

Spis treści

Waluta XXI wieku 6

Transformacja banku do chmury 8

Wstęp – „z głową w chmurach” 9

Podsumowanie rekomendacji praktycznych 9

Chmura w bankowości - od miłego dodatku do must have 10

Rodzaje usług chmurowych i modele wdrożeń 11

Prawne aspekty outsourcingu chmurowego 12

Mapa wymagań regulacyjnych 12

Obszary krytyczne 14

Ograniczenie odpowiedzialności 14

Outsourcing zagraniczny 15

Kontrola nad podoutsourcingiem 15

Tajemnica bankowa 16

Projektowane zmiany dotyczące outsourcingu 16

Czy chmura zawsze będzie outsourcingiem bankowym? 17

Wymogi związane z outsourcingiem oraz przywileje outsourcerów 18

Usługi chmurowe a regulacja outsourcingu 18

Jak przygotować bank do migracji chmurowej? 19

Określenie strategii chmurowej 20

Zapewnienie wewnętrznych kompetencji i wsparcie zewnętrzne 20

Klasyfikacja informacji i data governance 21

Ocena informacji - dopuszczalność przetwarzania w chmurze 22

Outsourcing szczególny chmury obliczeniowej 22

Szacowanie ryzyka przetwarzania w chmurze - metodyka 23

Wybrane ryzyka - vendor lock-in i utrata ciągłości działania 24

Polityka outsourcingu chmurowego 24

Umowa z dostawcą usług chmurowych 24

Zagadnienia ogólne 24

Jak negocjować z większym od siebie? 26

Najlepsze prawo? Prawo państwa członkowskiego UE 27

Podział odpowiedzialności za bezpieczeństwo przetwarzanych danych 27

Lokalizacja przetwarzania danych 29

Podoutsourcing 29

Uprawnienia kontrolne banku i nadzoru (audyt) 30

Ciągłość działania, rozwiązanie umowy i exit plan 30

Zmiany umowy a zmiany dokumentacji technicznej 31

Notyfikacja wykorzystania rozwiązań chmurowych 32

Chmura? Tak, ale jaka? 34

Chmura jako cel strategiczny 40

IBM ułatwia transformację banków do chmury – rady ekspertów 48

Chmura z efektem biznesowym 52

Salesforce rozszerza swoją ofertę usług finansowych dla bankowości korporacyjnej i inwestycyjnej 58

Waluta XXI wieku

Tym mianem bywają określane dane, i nie ma w tym stwierdzeniu żadnej przesady. Wystarczy uświadomić sobie, jak wiele usług cyfrowych, z których korzystamy na co dzień, dostępnych jest po uprzednim wyrażeniu zgody na przetwarzanie danych osobowych użytkownika, co oznacza, iż – wbrew powszechnemu przeświadczeniu – nie są one darmowe.

Fot. W. Łączyński

Karol Mórawski
REDAKTOR PROWADZĄCY
MIESIĘCZNIK FINANSOWY BANK

Współczesna gospodarka bazuje na danych, a zdolność do obsługi olbrzymich zasobów informacji już dziś determinuje konkurencyjność. Dynamiczny ich przyrost sprawia, że zasoby IT nawet i najpotężniejszych organizacji nie nadążają z samodzielnym przetwarzaniem tych wszystkich informacji, które mogą stanowić o ich przewadze rynkowej. W tym kontekście migracja do chmury staje się koniecznością, zwłaszcza dla instytucji finansowych, które dysponując bogatą wiedzą o swych klientach mogą monetyzować ją na różne sposoby. Od dwóch lat procesowi temu sprzyja otoczenie regulacyjne – opublikowany w styczniu 2020 r. komunikat Komisji Nadzoru Finansowego w sprawie przetwarzania informacji w chmurze obliczeniowej przez instytucje rynku finansowego de facto umożliwił efektywne wdrażanie rozwiązań bazujących na cloud computingu w polskiej bankowości.

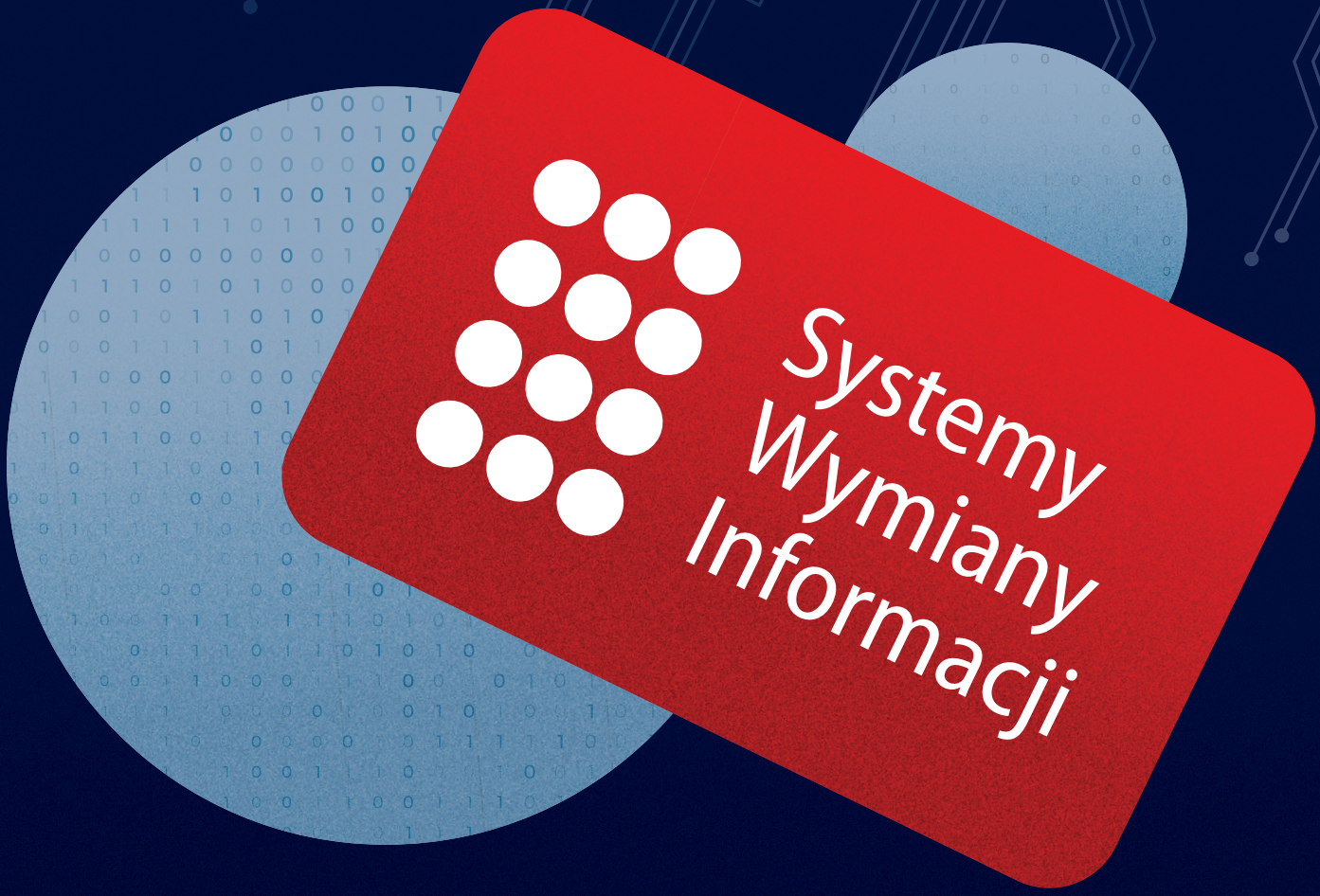
Obecnie niemal co czwarta polska firma dysponuje dostępem do usług cloudowych, jednak w pozostałych państwach UE średnia szacowana jest na 36%. Dodatkowo, wiele instytucji wykorzystuje dobrodziejstwa chmury na najniższym poziomie, używając poczty elektronicznej lub zewnętrznych magazynów danych. Banki, które w wielu obszarach uchodzą za liderów cyfrowej transformacji, w dziedzinie adopcji rozwiązań chmurowych w dalszym ciągu pozostają za innymi podmiotami branży finansowej, takimi jak instytucje rynku kapitałowego czy nawet ubezpieczyciele. Szacuje się, że potrzeba od dwóch do nawet pięciu lat, by cloud computing stał się elementem codziennego funkcjonowania każdego banku.

Rosnące potrzeby w zakresie obróbki danych to nie jedyny powód, dla którego we współczesnym biznesie nie ma alternatywy dla cloud computingu. Już dziś wiele rozwiązań IT dostępnych jest wyłącznie w modelu as a service, a na przestrzeni nadchodzących lat większość dostawców oprogramowania całkowicie zrezygnuje z wersji on premise. Trend ten jest zbieżny z oszałamiającym tempem rewolucji cyfrowej, która niekiedy przybiera nieprzewidywalne kierunki, sprawiając, że – jak w świecie przyrody – przetrwają tylko ci, którzy są w stanie szybko i sprawnie adaptować się do zmieniających się uwarunkowań. I tu znowu ujawnia się przewaga cloudowego outsourcingu, który pozwala na korzystanie z zewnętrznych zasobów „tu i teraz", i szybką zmianę używanego systemu w chwili, gdy nagle przestaje on odpowiadać aktualnym potrzebom. Trawestacja dewizy Legii Cudzoziemskiej – migruj do chmury albo giń – nie jest w żadnej mierze przesadą.

Rzecz w tym, by proces adopcji chmury przeprowadzić w sposób nie tylko odpowiadający potrzebom instytucji, ale i w pełni zgodny z wymogami prawnymi i oczekiwaniami regulatora. Kwestiom tym poświęcony jest niniejszy raport, który ukazuje praktyczne aspekty, związane z migracją zasobów instytucji finansowej do chmury. Znajdują się w nim odniesienia do kluczowych uregulowań dla tego modelu działania, a towarzyszą im wnioski i wskazówki o charakterze praktycznym, ukazujące jak powinno wyglądać tworzenie strategii dla chmury w banku, co należy zmienić w polityce data governance czy też na jakich zasadach zawierać umowy z dostawcami cloudu, tak by uwzględnić obszar prawny czy kluczowe dla instytucji bankowych kwestie bezpieczeństwa.

Szczególnie ważne jest zapewnienie w tym procesie odpowiednio wykwalifikowanych zasobów ludzkich, bez których cała transformacja skazana jest na porażkę. Wsparciem dla banków w tych niełatwych zadaniach może być zaprezentowany w opracowaniu standard Polish Cloud, który w październiku 2021 r. doczekał się swej drugiej odsłony. Dokument, przygotowany przez Związek Banków Polskich wspólnie z Forum Technologii Bankowych, stanowi kompendium praktycznej wiedzy o aktualnych uwarunkowaniach prawno-regulacyjnych dotyczących migracji do chmury, wraz z zaleceniami jak realizować ten niełatwy proces. •

ESENCJA BEZPIECZNEJ BANKOWOŚCI



System /DZ/
DOKUMENTY ZASTRZEŻONE

System /BR/
BANKOWY REJESTR

System /ZK/
ZASTRZEGANIA KART

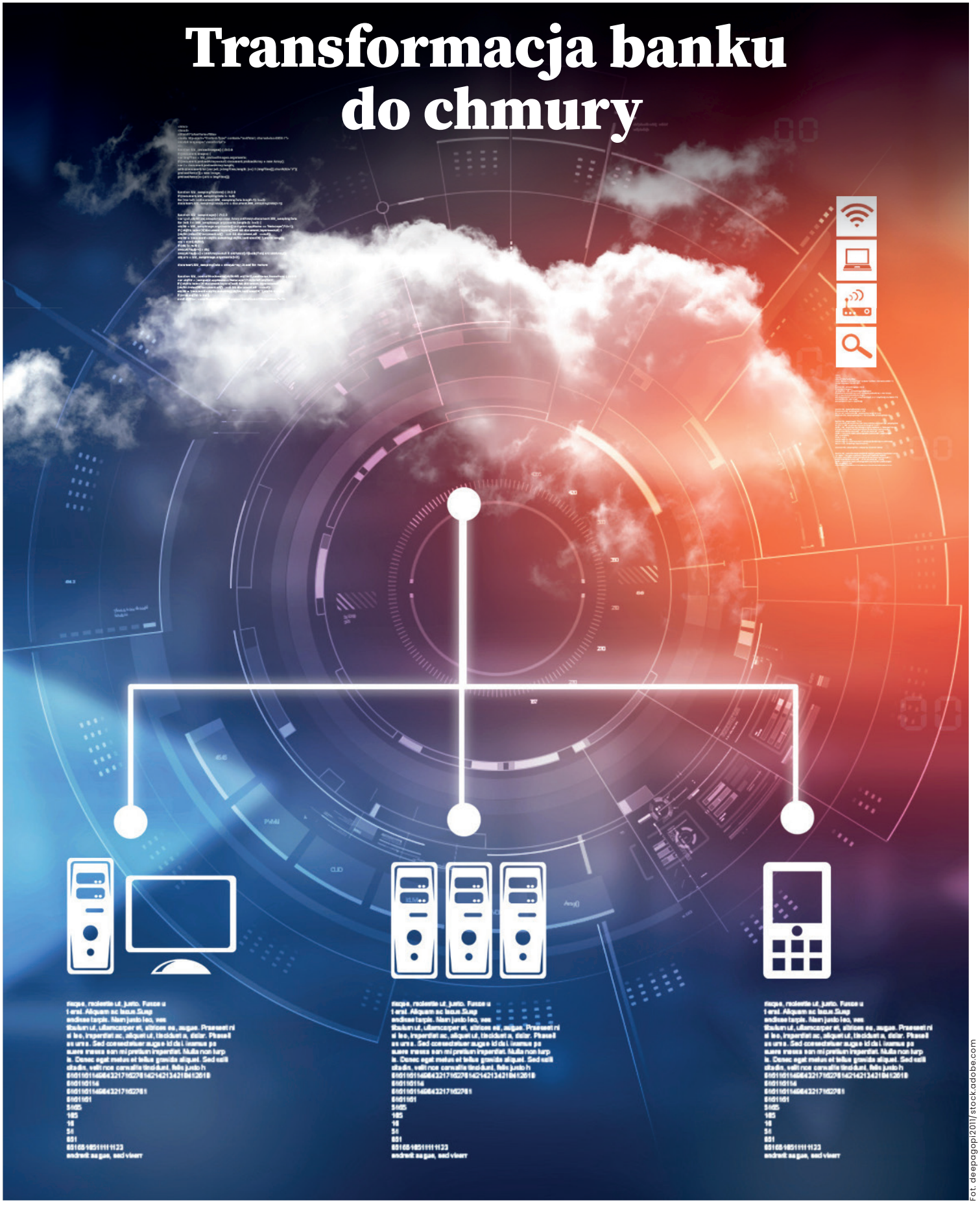
System /RRB/
REJESTR RACHUNKÓW BANKOWYCH

Systemy /ZOR/
Z OBSZARU RYZYKA

30 Związek Banków Polskich

www.zbp.pl

Transformacja banku do chmury



Fot. deepagopi2011/stock.adobe.com

Fot. Arch. prywatne

Artur Bilski

JEST PREZESEM I WSPÓŁZAŁOŻYCIELEM FIRMY TOKEN ADVISORY, ŚWIADCZĄCEJ KOMPLEKSOWE DORADZTWO W OBSZARZE NOWYCH TECHNOLOGII, W TYM BLOCKCHAIN, KRYPTOAKTYWÓW I TOKENIZACJI.
JAKO RADCA PRAWNY OD LAT ZWIĄZANY Z POLSKIMI I MIĘDZYNARODOWYMI KANCELARIAMI PRAWNYMI (OSTATNIO JAKO COUNSEL W KOCHAŃSKI & PARTNERS, WCZEŚNIEJ CLIFFORD CHANCE, HOGAN LOVELLS), KTÓRYM DORADZAŁ W OBSZARZE REGULACJI FINANSOWYCH I PRAWA NOWYCH TECHNOLOGII. W RAMACH SWOJEJ PRAKTYKI WSPÓŁPRACOWAŁ TAKŻE Z NAJWIĘKSZYMI BANKAMI W POLSCE – PKO BP, ING ORAZ ALIOR, PRZY CZYM W OSTATNIM Z NICH SPRAWOWAŁ FUNKCJĘ DYREKTORA DZIAŁU OBSŁUGI PRAWNEJ BIZNESU. ZAJMOWAŁ RÓWNIEŻ STANOWISKO DYREKTORA DS. PRAWNYCH W RAMP NETWORK, WIODĄCEJ POLSKIEJ FIRMIE ZAJMUJĄCEJ SIĘ PŁATNOŚCIAMI I TECHNOLOGIĄ BLOCKCHAIN.
ABSOLWENT I PRACOWNIK NAUKOWY UNIWERSYTETU WARSZAWSKIEGO, EKSPERT INSTYTUTU ALLERHANDA ORAZ CZŁONEK CENTRUM BADAŃ NAD PRAWNYMI ASPEKTAMI TECHNOLOGII BLOCKCHAIN NA UNIWERSYTECIE WARSZAWSKIM.

Fot. Arch. prywatne

Mateusz Krakowski

PRAWNIK SPECJALIZUJĄCY SIĘ W PRAWIE OCHRONY DANYCH OSOBOWYCH ORAZ REGULACJACH FINTECH. EKSPERT W DZIEDZINIE BEZPIECZEŃSTWA INFORMACJI. OD KILKU LAT DORADZA PRZY PROJEKTACH IT ORAZ UCZESTNICZY WE WDROŻENIACH CHMURY OBLICZENIOWEJ CZOŁOWYCH DOSTAWCÓW W SEKTORZE FINANSOWYM. PREZES STOWARZYSZENIA INNOVATION FINANCE TECHNOLOGY ASSOCIATION (IFTA). ABSOLWENT STUDIÓW PODYPLOMOWYCH PRAWO NOWOCZESNYCH TECHNOLOGII. APLIKANT RADCOWSKI I DOKTORANT W AKADEMII IM. LEONA KOŹMIŃSKIEGO.

WSTĘP – „Z GŁOWĄ W CHMURACH"

Chmura obliczeniowa staje się coraz bardziej popularnym rozwiązaniem wykorzystywanym w działalności biznesowej w Polsce i na *świecie. Wygoda, bezpieczeństwo i oszczędności sprawiają, że atrakcyjność chmury jest nie* do przecenienia, a menedżerowie i zarządy wielu firm (w tym banków) już od jakiegoś czasu podejmują działania, których celem jest możliwie jak najszersza migracja do chmury.

Nie da się jednak ukryć, że wspomniana migracja może być problematyczna. Wynika to z wielu kwestii. Jedną z nich są wymogi regulacyjne i podejście nadzorcy. Inną *są* trudności związane z przekazywaniem danych objętych tajemnicą bankową. Jeszcze inną zaś wyzwania wynikające z umów zawieranych z dostawcami. Wszystko to sprawia, że wdrożenie rozwiązań chmurowych nie jest ani szybkie, ani bezproblemowe. Niniejszy raport jest opisem najważniejszych kwestii regulacyjnych z tym związanych i próbą identyfikacji najczęściej występujących spośród tych problemów i znalezieniem odpowiedzi na to, jak banki mogą sobie z nimi poradzić.

W niniejszym raporcie koncentrujemy się przede wszystkim na najbardziej istotnych zagadnieniach prawnych i organizacyjnych dotyczących wdrożeń chmurowych w bankowości. W dokumencie tym staraliśmy się Państwu przekazać najważniejsze naszym zdaniem kwestie odnoszące się do praktycznego zarządzania „przejściem do chmury". Zawartość raportu jest pochodną naszej wiedzy praktycznej, wyniesionej z doradztwa przy kilkudziesięciu projektach tego typu – zarówno dla banków, jak i innych podmiotów, w tym samych dostawców usług chmurowych. Mamy nadzieję, że przygotowany przez nas materiał pomoże Państwu w lepszym zrozumieniu funkcjonowania procesów wdrożeniowych oraz pozwoli na bardziej efektywne podejście do projektów chmurowych.

Celem dokumentu jest przybliżenie odbiorcy praktycznych aspektów związanych z migracją banku do chmury oraz poruszenie istotnych kwestii dotyczących m.in. zawierania umów z dostawcami chmurowymi, zarządzania określonymi ryzykami, czy zapewnienia zgodności prawnej. Zawiera on również rekomendacje w zakresie tego, w jaki sposób najlepiej podejść do wdrożenia w organizacji rozwiązań chmurowych i na jakie zagrożenia należy uważać zarówno w kontekście samych wdrożeń, jak i w odniesieniu do umów zawieranych z dostawcami.

Oprócz tego, poniżej znajdą Państwo krótkie podsumowanie kluczowych rekomendacji, które zawiera najważniejsze punkty odnoszące się do efektywnego wdrażania rozwiązań chmurowych w banku i zapewnienia zgodności tego typu technologii z obowiązującymi regulacjami. Jednocześnie zwracamy uwagę, że niniejszy dokument ma charakter ogólny i stanowi zestaw generalnych rekomendacji, wspólnych dla wdrożeń usług chmury obliczeniowej publicznej lub hybrydowej w bankowości. Zawarte poniżej uwagi powinny być zawsze interpretowane w kontekście konkretnego projektu, z uwzględnieniem rodzaju wdrażanych usług, zakresu informacji przetwarzanych w chmurze oraz specyfiki danej organizacji. Rekomendacji tych nie można zatem uznać za wyczerpujące.

PODSUMOWANIE REKOMENDACJI PRAKTYCZNYCH

Przed wdrożeniem usług chmury obliczeniowej w banku konieczne jest wzięcie pod uwagę następujących kwestii:

1. Transformacja banku do chmury powinna rozpocząć się od określenia strategii chmurowej banku. Ocena aktualnej dojrzałości chmurowej, identyfikacja głównych potrzeb biznesowych i celów, których realizację umożliwi wdrożenie określonych rozwiązań wykorzystujących usług chmury obliczeniowej, a także decyzja w zakresie środków na ich realizację stanowią warunek konieczny udanych wdrożeń chmurowych. Bank powinien zaadresować swoje potrzeby, wybierając konkretne rozwiązania dostępne na rynku i koncentrując się na wdrożeniu ich w zgodzie z obecnymi regulacjami.
2. Podstawą udanego wdrożenia chmury jest zapewnienie odpowiednich kompetencji. W zależności od specyfiki i wielkości konkretnego projektu zespół projektowy powinien składać się m.in. z: developerów, inżynierów DevOps, administratorów sieci/systemów, architektów infrastruktury, specjalistów ds. bezpieczeństwa, prawników

i specjalistów ds. compliance oraz opiekuna biznesowego. Braki w kompetencjach wewnętrznych należy zidentyfikować i uzupełnić poprzez podnoszenie kwalifikacji lub wsparcie specjalistów zewnętrznych.

3. Przeprowadzenie odpowiedniej klasyfikacji i oceny informacji, a także systemowa zmiana podejścia do data governance często będą warunkowały powodzenie projektów chmurowych. Konieczne mogą okazać się: dokładne zmapowanie przepływów danych, identyfikacja właścicieli i szacunkowe określenie wartości poszczególnych zasobów informacyjnych w organizacji, a także ustalenie wymagań prawnych i minimalnych środków bezpieczeństwa odnoszących się do każdej ze zdefiniowanych klas informacji. Bank powinien wiedzieć, jakie dane przetwarza lub zamierza przetwarzać w chmurze i jakie negatywne konsekwencje będzie oznaczać naruszenie bezpieczeństwa tych danych.
4. Kluczowym elementem wdrożeń chmurowych jest szacowanie ryzyka i ciągłe zarządzanie zidentyfikowanym ryzykiem. W zależności od poziomu zidentyfikowanego ryzyka bank może je zaakceptować lub wdrożyć odpowiednią strategię zmierzającą do jego mitygacji. W przypadku negatywnej zmiany poziomu ryzyka bank, powinien mieć możliwość rezygnacji z usług chmurowych przy zapewnieniu ciągłości działania. Opracowanie scenariuszy wyjścia z chmury powinno mieć miejsce przed podjęciem finalnej decyzji w zakresie implementacji tej technologii. Scenariusze te należy testować i w razie potrzeby aktualizować.
5. Umowa chmurowa ze względu na swój bardzo szeroki i interdyscyplinarny zakres powinna być przedmiotem weryfikacji nie tylko działu prawnego, ale również innych departamentów banku, takich jak compliance, ryzyko, bezpieczeństwo i oczywiście IT.
6. Umowa chmurowa powinna przewidywać, że:
   a) Centrum Przetwarzania Danych powinno w pierwszej kolejności znajdować się na terenie Europejskiego Obszaru Gospodarczego;
   b) Umowa dotycząca chmury obliczeniowej dla banku powinna zawierać kompletną listę poddostawców.
7. W projektach chmurowych bardzo istotnym aspektem jest odpowiednie zarządzanie dokumentacją na potrzeby rozliczalności. Należy zadbać o udokumentowanie spełnienia każdego z wymagań regulacyjnych, wyników przeprowadzonych ocen i analiz, a także sporządzić szczegółowy plan przetwarzania informacji w chmurze obliczeniowej, plan ciągłości działania banku oraz strategie wyjścia z chmury. Dokumentacja powinna być regularnie przeglądana i w razie potrzeby aktualizowana. W przypadkach outsourcingu szczególnego chmury obliczeniowej lub przetwarzania informacji prawnie chronionej konieczne jest dokonanie notyfikacji do Urzędu Komisji Nadzoru Finansowego (UKNF) w terminie 14 dni przed rozpoczęciem przetwarzania w chmurze obliczeniowej zgodnie z wymaganiami komunikatu chmurowego.

Chmura w bankowości – od miłego dodatku do must have

Pomimo rosnącej popularności chmury obliczeniowej, wykorzystanie usług chmurowych w Polsce wciąż pozostaje na poziomie niższym niż średnia w Unii Europejskiej. Choć według informacji Głównego Urzędu Statystycznego w ubiegłym roku z płatnych usług chmury obliczeniowej korzystało już 24,4% krajowych przedsiębiorstw[1], to Polska nadal znajduje się poniżej średniej europejskiej, która wyniosła w ubiegłym roku 36%[2]. W większości mowa tu jednak głównie o usługach poczty elektronicznej i przechowywaniu plików[3].

Sektor bankowy nadal jest na wczesnym etapie wdrażania technologii chmurowych – szacuje się[4], że o powszechnym stosowaniu

1 Warto podkreślić dynamikę wzrostu w tym obszarze. W roku 2019 z usług chmurowych korzystało 17,5%, a rok wcześniej zaledwie 11%. Główny Urząd Statystyczny, informacje sygnalne „Społeczeństwo informacyjne w Polsce w 2020 r." (https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2020-roku,2,10.html#:~:text=W%202020%20r.,internetowe%20(68%2C5%25), dostęp 30.11.2021).

2 Niekwestionowanymi liderami w tym zakresie są kraje skandynawskie. Spośród Państw Członkowskich UE Polska wyprzedza jedynie Łotwę, Grecję, Rumunię i Bułgarię. Eurostat, Cloud computing - statistics on the use by enterprises (https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises, dostęp 30.11.2021).

3 M. Marszycki, Chmura obliczeniowa w Polsce: dwukrotnie wzrosło wykorzystanie cloud computing w firmach, I Twiz (https://itwiz.pl/chmura-obliczeniowa-w-polsce-dwukrotnie-wzroslo-wykorzystanie-cloud-computing-w-firmach/#:~:text=Najwa%C5%BCniejsze%20informacje-,W%202020%20roku%20z%20p%C5%82atnych%20us%C5%82ug%20chmury%20obliczeniowej%20korzysta%C5%82o%2024,komunikacja%20(63%2C5%25). dostęp 30.11.2021).

4 Chmura obliczeniowa w sektorze bankowym na świecie, w Europie i w Polsce, raport (https://zbp.pl/getmedia/5484bb19-70c8-41d3-8533-c6bb512428bc/Raport-Cloud, dostęp 30.11.2021).

chmury w bankowości będziemy mogli mówić dopiero w perspektywie najbliższych 2–5 lat. Lepiej sytuacja wygląda na rynkach kapitałowych, a nawet w ubezpieczeniach, nie wspominając o szeroko rozumianej branży IT. Widoczny jest zatem bardzo duży potencjał wykorzystania chmury obliczeniowej w bankowości. Pomimo istotnego przyspieszenia w ostatnich latach (zwłaszcza w ostatnim roku, za sprawą m.in. liberalizacji stanowiska nadzoru w tym zakresie), polskie banki mają nadal dużo do zrobienia, aby nadgonić pozostałych uczestników rynku.

Na przestrzeni ostatnich lat oferta usług chmury obliczeniowej, przede wszystkim w zakresie usług wykorzystujących chmurę obliczeniową dostępnych na rynku, uległa gwałtownemu poszerzeniu. Usługi te, traktowane początkowo jako nowinka technologiczna, są coraz częściej wykorzystywane przez biznes, stopniowo wypierając lokalne (on-premis'owe) rozwiązania informatyczne. Już teraz trudno wyobrazić sobie nowoczesną firmę, która w ogóle nie korzysta z chmury obliczeniowej.

Przyczyna tego zjawiska jest prosta. Usługi chmurowe mają przewagę nad rozwiązaniami on-premise w aspekcie komercyjnym. Oczywiście, z wykorzystaniem usług chmurowych wiążą się liczne ryzyka, które zostaną omówione w dalszej części raportu, jednakże wszystko wskazuje na to, że są to ryzyka, którymi organizacje będą musiały nauczyć się zarządzać (wydaje się, że wiele z nich to już potrafi). Korzyści z zastosowania chmury są na tyle istotne, że całkowita rezygnacja z wykorzystania tej technologii będzie zjawiskiem coraz rzadszym. Z czasem stanie się to wręcz niemożliwe, gdyż nowe rozwiązania zakładające przetwarzanie informacji, przestają w zasadzie korzystać z innych rozwiązań niż rozwiązania chmurowe.

Przyczyną stosowania rozwiązań chmurowych jest także ich przewaga technologiczna, która zaspokaja potrzeby związane z rosnącym wolumenem przetwarzanych danych i rosnącym znaczeniu big data w poszczególnych sektorach gospodarki – również w bankowości. Choć szeroko rozumiana jakość danych w wielu organizacjach jest jeszcze na dosyć niskim poziomie, a potencjał ich wykorzystania nadal może być trudny do oszacowania, to już dzisiaj można z całą pewnością stwierdzić, że skuteczna monetyzacja posiadanych danych stanowi nierzadko o przewadze konkurencyjnej nad innymi przedsiębiorstwami. Dotyczy to również (a może i przede wszystkim) sektora finansowego.

Potencjalne zasoby danych wydają się nieograniczone[5]. Ponadto, wartość danych będzie rosła wraz ze wzrostem ich wolumenu. Olbrzymie ilości przetwarzanych danych wymagają nie tylko bardzo dużej przestrzeni dyskowej do ich przechowywania, ale także gigantycznych zasobów mocy obliczeniowej. Dane mają realną wartość jedynie wtedy, gdy są aktywnie przetwarzane, a w gwałtownie zmieniającym się świecie ich „termin przydatności" jest dość ograniczony. Pomijając powszechnie znany aspekt związany z koniecznością redukcji kosztów przetwarzania tak dużych ilości informacji i utrzymaniem infrastruktury, można zaryzykować tezę, że w przyszłości jedynie dostawcy usług chmury obliczeniowej będą w stanie dostarczyć zasoby umożliwiające efektywne przetwarzanie danych i czerpanie z tego tytułu korzyści.

Chmura obliczeniowa to również elastyczność –rozumiana jako coś więcej niż tylko skalowalność istniejących usług i możliwość czasowego, dynamicznego zwiększenia zasobów obliczeniowych np. na potrzeby operacji związanych ze zwiększoną liczbą zapytań kredytowych w elektronicznym kanale komunikacji. Elastyczność możliwa dzięki chmurze obliczeniowej wyraża się bowiem również w łatwości adaptacji do nowych realiów rynkowych poprzez redukcję kosztów początkowych i szybkie uruchamianie nowych usług oraz procesów wewnątrzorganizacyjnych. Na przykładzie ostatniego roku i pandemii COVID-19 widać doskonale, jak istotnym aspektem dla zachowania ciągłości działania organizacji jest chociażby jej zdolność do szybkiego przejścia na model pracy zdalnej, czy też posiadanie sprawnego kanału sprzedaży internetowej, alternatywnie do sprzedaży realizowanej w placówkach stacjonarnych.

Chmura obliczeniowa i digitalizacja procesów biznesowych nie są już tylko przejawem innowacji, pozwalającym wyróżnić się na tle konkurencji. Nierzadko decydują one o dalszej obecności na rynku jako element konieczny do prowadzenia działalności w XXI wieku. Również w bankowości, w której poziom adaptacji chmury jest jeszcze na relatywnie niskim poziomie w porównaniu z innymi branżami, technologia ta przestaje być miłym dodatkiem. Chmura obliczeniowa to obecnie „must have", a zarządzanie ryzykami związanymi z jej wykorzystaniem musi zostać wpisane w DNA nowoczesnego banku.

Rodzaje usług chmurowych i modele wdrożeń

W ofercie dostawców spotkać się można z coraz większą różnorodnością usług świadczonych

5 Według raportu IDC w samym 2020 roku globalnie wygenerowanych zostało ok. 64 zettabajty (ZB; 10^21) danych - w dużej mierze za sprawą pandemii COVID-19 oraz dramatycznego wzrostu liczby osób pracujących i uczących się zdalnie. W latach 2020-2025 IDC przewiduje coroczny wzrost objętości wytwarzanych danych średnio o 23%, co w 2025 roku będzie oznaczało ok. 180 ZB generowanych rocznie. (Worldwide Global StorageSphere Forecast, 2021–2025: To Save or Not to Save Data, That Is the Question, Doc #US47509621, https://www.idc.com/getdoc.jsp?containerId=prUS47560321, dostęp 30.11.2021).

„as a service"[6].W obszarze chmury obliczeniowej nadal możemy jednak mówić o trzech podstawowych rodzajach usług[7]:

- Software as a Service (SaaS);
- Platform as a Service (PaaS); oraz
- Infrastructure as a Service (IaaS).

Pozostałe usługi świadczone w tym modelu będą najczęściej stanowiły pochodne jednej z wyżej wymienionych kategorii – najczęściej SaaS.

Zarówno w Europie, jak i na świecie zdecydowanie największy udział w rynku usług chmurowych notują usługi typu SaaS. Warto zwrócić jednak uwagę, że prognozuje się stopniowy wzrost wykorzystania dwóch pozostałych modeli – IaaS i PaaS[8]. Wynika to z systematycznego wzrostu dojrzałości organizacji, które po przeprowadzeniu wdrożeń wybranych usług chmurowych w poszczególnych obszarach działalności stopniowo przechodzą do dużych projektów, obejmujących zmiany systemowe (w tym systemów core'owych) w ramach całych platform, a nawet infrastruktury.

Wykorzystanie usług SaaS umożliwia dostęp do innowacyjnych i wysoce skalowalnych rozwiązań. Będą one najczęściej wystandaryzowane, a możliwość ich zaawansowanej konfiguracji czy kastomizacji (indywidualizacji) ograniczona.

Wdrożenia PaaS czy IaaS będą na pewno bardziej złożonymi projektami, wymagającymi większych nakładów w fazie początkowej, jednak dopiero te rozwiązania umożliwią bankom pełne wykorzystanie potencjału chmury obliczeniowej poprzez zwiększenie elastyczności organizacji w zakresie wprowadzania nowych usług i procesów oraz istotne zmniejszenie kosztów stałych infrastruktury. Większa konfigurowalność usług PaaS/IaaS to także możliwość zaadresowania wymagań regulacyjnych i utrzymanie zgodności z wymaganiami prawnymi.

PRAWNE ASPEKTY OUTSOURCINGU CHMUROWEGO

Mapa wymagań regulacyjnych

Wymagania prawne i regulacyjne dotyczące outsourcingu chmury obliczeniowej są rozproszone i znajdują się nie tylko w prawie bankowym[9], ale także w wydanych przez nadzór rekomendacji D[10] dotyczącej zarządzania i bezpieczeństwa IT oraz tzw. komunikacie chmurowym[11]. Odmienny charakter oraz zakres przedmiotowy źródeł wymagań może prowadzić niekiedy do wątpliwości interpretacyjnych.

W prawie bankowym (art. 6a–6d) ustawowo uregulowano dopuszczalny zakres powierzenia przez bank wykonywania określonych czynności podmiotom trzecim (outsourcing regulowany). W zależności od modelu i zakresu świadczonych usług outsourcing IT, w tym również usługi chmury obliczeniowej, będzie najczęściej mieścił się w zakresie czynności faktycznych związanych z działalnością bankową (art. 6a ust. 1 pkt 2 prawa bankowego).

Rekomendacja D dotyczy z kolei całego obszaru IT w bankach – zarówno zasobów i procesów własnych, jak i outsourcowanych, więc wymagania w niej zawarte należy stosować odpowiednio również do wykorzystania usług chmury obliczeniowej oraz bez-

6 Nurt *Everything as a Service* (XaaS) dotyczy możliwości outsourcingu właściwie wszelkich zasobów, najczęściej w oparciu o usługi chmury obliczeniowej. Spotkać można choćby takie usługi jak Blockchain as a Service (BaaS), Data as a Service (DaaS), czy Robot as a Service (RaaS). Więcej przykładów można znaleźć choćby na stronie Wikipedii (https://en.wikipedia.org/wiki/As_a_service, dostęp 30.11.2021).

7 Peter Mell; Timothy Grance (September 2011). The NIST Definition of Cloud Computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce. doi:10.6028/NIST.SP.800-145. Special publication 800-145. (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, dostęp 30.11.2021).

8 W raporcie pt. "Chmura obliczeniowa w sektorze bankowym na świecie, w Europie i w Polsce" przygotowanym przez Accenture pod auspicjami Związku Banków Polskich wskazano m.in., że w 2018 roku udział SaaS w globalnym rynku chmury obliczeniowej wynosił 66%, ale w 2023 roku będzie to już 53%. Zgodnie z prognozami udział IaaS w tym okresie odnotuje wzrost z 20% do 29%, a PaaS z 14% do 19% (https://zbp.pl/getmedia/5484bb-19-70c8-41d3-8533-c6bb512428bc/Raport-Cloud, dostęp 30.11.2021).

9 Ustawa z dnia 29 sierpnia 1997 r. prawo bankowe (Dz.U. 1997 Nr 140, poz. 939 z późn. zm.).

10 Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, Warszawa, styczeń 2013 r. (https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf, dostęp 30.11.2021).

11 Komunikat Urzędu Komisji Nadzoru Finansowego z dnia 23 stycznia 2020 r. 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, dostęp 30.11.2021).

Fot. jirsak/stock.adobe.com

pieczeństwa tych usług. Komunikat chmurowy stanowi natomiast podejście nadzoru finansowego do outsourcingu przetwarzania informacji w chmurze obliczeniowej publicznej i hybrydowej dla całego sektora finansowego, w tym oczywiście banków.

Komunikat będzie znajdował zastosowanie, gdy przetwarzaniu w usługach chmury obliczeniowej podlegały będą informacje prawnie chronione (objęte tajemnicą sektorową, czyli w przypadku banków – tajemnicą bankową) lub w przypadku tzw. outsourcingu szczególnego chmury obliczeniowej, o którym mowa w niniejszym opracowaniu. Należy jednak mieć na uwadze rozbieżności w sposobie uregulowania outsourcingu dla poszczególnych podmiotów nadzorowanych (niekiedy bardzo istotne np. w zakresie dopuszczalności outsourcingu zagranicznego). W przypadku wykorzystania chmury obliczeniowej przez bank wymagania zawarte w komunikacie chmurowym trzeba zatem czytać zawsze w kontekście przepisów prawa bankowego oraz Rekomendacji D.

Z perspektywy prawnej, celowe wydaje się uregulowanie wymagań dotyczących outsourcingu chmury obliczeniowej na poziomie ustawowym, a także wystandaryzowanie zasad outsourcingu regulowanego i dopuszczalności ujawnienia informacji prawnie chronionych (tajemnica sektorowa). Tym bardziej że charakter prawny samego komunikatu, który obecnie stanowi źródło większości wymagań, nie jest do końca jasny, a regulacje ustawowe w bieżącym kształcie nierzadko nie przystają do nowoczesnych rozwiązań i modeli biznesowych.

Problematyczne, szczególnie dla banków wchodzących w skład międzynarodowych grup kapitałowych, może okazać się również stosowanie wytycznych Europejskiego Urzędu Nadzoru Bankowego(EBA) w sprawie outsourcingu[12]. Komunikat chmurowy wprost wyłącza bowiem stosowanie wytycznych, zaleceń i innych dokumentów europejskich organów nadzorczych, w tym EBA, które odnoszą się do przetwarzania informacji w chmurze obliczeniowej. W wyniku wprowadzenia takiego postanowienia, część banków znalazła się w sytuacji, w której z jednej strony krajowy organ nadzoru wymaga dostosowania się do wymagań komunikatu i niestosowania wytycznych EBA, a z drugiej strony

12 Sprawozdanie końcowe na temat wytycznych Europejskiego Urzędu Nadzoru Bankowego (ang. European Banking Authority, EBA) z dnia 25 lutego 2019 r. w sprawie outsourcingu, EBA/GL/2019/02 (https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/7551b-1c5-534d-44aa-b524-61eb8929154d/EBA%20revised%20Guidelines%20on%20outsourcing_PL.pdf?retry=1, dostęp 30.11.2021).

grupa kapitałowa i spółka matka prowadząca działalność w ramach Europejskiego Obszaru Gospodarczego oczekiwać będzie spójności i globalnego wdrożenia wymagań Europejskiego Urzędu Nadzoru Bankowego.

Urząd Komisji Nadzoru Finansowego doprecyzował wprawdzie, że wytyczne unijnych organów nadzoru nie mają zastosowania do podmiotów nadzorowanych jedynie w zakresie w jakim są sprzeczne z komunikatem[13], jednakże nie wskazano konkretnych postanowień, które zdaniem nadzoru nie powinny mieć zastosowania. Choć sprostanie tym oczekiwaniom teoretycznie nie jest niemożliwe, to na pewno takie podejście w praktyce nie ułatwia poruszania się po i tak już skomplikowanym krajobrazie regulacyjnym. Być może harmonizacja regulacji dotyczących outsourcingu chmury obliczeniowej na poziomie unijnym mogłaby nieco wyklarować obecną sytuację, jednakże na ten moment polski organ nadzoru finansowego (KNF) wykazuje większą chęć regulowania omawianego obszaru w sposób odmienny niż organy w innych Państwach Członkowskich[14]. Niezależnie jednak od tych rozważań, banki stoją przed wyzwaniem dostosowania się do pokaźnej liczby wymagań (prawnych, technicznych, a także organizacyjnych) – i to zanim jeszcze zaczną korzystać z usług chmurowych. Przygotowanie listy wymagań i właściwa ich interpretacja w całym zespole projektowym powinny być jednym z pierwszych kroków w procesie transformacji banku do chmury.

Obszary krytyczne

W ramach wymagań prawnych można wyróżnić kilka obszarów krytycznych. Wynika to m.in. z różnego charakteru źródeł tych wymagań oraz różnic w ewentualnych konsekwencjach niespełnienia poszczególnych obowiązków. Inaczej bowiem postrzegać należy naruszenie bezwzględnej normy ustawowej niż częściowe niewdrożenie któregoś z wymagań określonych w komunikacie chmurowym czy rekomendacji D. Te ostatnie należy bowiem stosować w kontekście wyników szacowania ryzyka (*risk-based approach*), stosując generalną regułę zastosuj lub wyjaśnij, dlaczego nie możesz zastosować (*complyor explain*).

Ograniczenie odpowiedzialności

Pierwszym z takich obszarów jest bezwzględny zakaz ograniczenia odpowiedzialności dostawcy wobec banku za szkody wyrządzone klientom banku (art. 6b ust. 1 prawa bankowego). Jeszcze jakiś czas temu w niemal wszystkich umowach z dostawcami usług chmurowych można było spotkać bardzo szerokie wyłączenia i ograniczenia odpowiedzialności dostawcy, sprowadzające się właściwie do tego, że dostawca rzeczywiście zobowiązywał się do świadczenia usług, ale co do zasady nie ponosił odpowiedzialności w przypadku nienależytego wykonania umowy (np. na skutek wprowadzenia niezwykle szerokiej definicji siły wyższej do umowy).

W najlepszym razie, podmiot korzystający z chmury obliczeniowej mógł liczyć na obniżenie ceny za usługi nabywane w przyszłości od danego dostawcy (tzw. kredyty). Wyłączenia i ograniczenia odpowiedzialności nierzadko obejmowały również ewentualne szkody wyrządzone klientom banku, co w sposób oczywisty nie spełniało wymagań prawa bankowego.

Organ nadzoru rekomenduje w tym zakresie włączenie do umowy odniesienia do poszczególnych przepisów prawa albo inkorporowanie treści konkretnych przepisów regulujących zasady i zakres odpowiedzialności za szkody wyrządzone klientom[15].

W ostatnich latach widzimy zmianę w kształcie umów zawieranych przez największych dostawców chmurowych i swoistą „liberalizację" podejścia w tym zakresie, rozumianą jako zgadzanie się przez dostawców na większe ustępstwa w stosunku do swoich klientów z sektora finansowego w Polsce. Co prawda, jeśli chodzi o odpowiedzialności dostawcy względem banku nadal spotyka się klauzule ograniczające odpowiedzialność (abstrahując od ich skuteczności i zgodności z prawem), a próby wprowadzenia odmiennych postanowień, czy też wpisania do umowy z dostawcą kar umownych za niewykonanie lub nienależyte wykonanie umowy wciąż spotykają się ze zdecydowanym sprzeciwem dostawców usług chmurowych. Niemniej, coraz częściej zgadzają się oni na nieograniczoną odpowiedzialność względem klientów banku, uznając konieczność dostosowania się do restrykcyjnych wymagań prawnych – w innym

13 Zob. 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 30.11.2021).

14 Zjawisko tzw. „gold-platingu", kiedy państwa członkowskie wprowadzają dodatkowe, bardziej surowe restrykcje, niż te przewidziane przez przepisy unijne.

15 Zob. 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 30.11.2021).

wypadku banki nie są bowiem w stanie podjąć współpracy w zakresie usług chmurowych.

W praktyce, pociągnięcie dostawcy do odpowiedzialności za szkody wyrządzone klientom może okazać się nie lada wyzwaniem (odpowiedzialność na zasadzie winy, konieczność wykazania ciągu przyczynowo-skutkowego), ale formalne wymaganie prawne coraz częściej będzie można uznać za spełnione, co otwiera drzwi do szerszego zastosowania chmury w bankowości.

Outsourcing zagraniczny

Obecne regulacje dotyczące outsourcingu zagranicznego właściwie wykluczają możliwość korzystania z rozwiązań świadczonych przez podmioty spoza Europejskiego Obszaru Gospodarczego (EOG). Mimo że prawo bankowe nie zakazuje wprost takiego powierzenia realizacji czynności, to obowiązek uzyskania uprzedniego zezwolenia Komisji Nadzoru Finansowego skutecznie blokuje tego typu projekty ze względu na wysoką czasochłonność procesu uzyskiwania zgody i liczne związane z tym niedogodności.

Dostosowując się do realiów rynkowych, więksi dostawcy usług chmury obliczeniowej posiadają już spółki z siedzibą w EOG i lokalne centra przetwarzania danych w EOG, dzięki czemu w niektórych przypadkach możliwe będzie spełnienie wymagań w tym zakresie. Należy jednak pamiętać, że obowiązek uzyskania zgody KNF na outsourcing zagraniczny dotyczy nie tylko bezpośredniego dostawcy banku, ale także jego poddostawców (tj. dostawców świadczących dla dostawców usługi wykorzystywane w realizacji outsourcowanych czynności). Wiele firm dostarczających rozwiązań chmurowych, szczególnie świadczonych w modelu SaaS, korzysta z zagranicznych podwykonawców, a także z centrów przetwarzania danych (CPD) zlokalizowanych poza terytorium państw członkowskich EOG. Problemem może okazać się jednak chociażby świadczenie usług wsparcia w modelu 24/7 (*follow the sun*). Najczęściej opiera się ono bowiem na usługach konsultantów pracujących z różnych stref czasowych, w tym takich zlokalizowanych poza EOG (chociażby w Indiach).

W kontekście powyższego należy również wziąć pod uwagę, że weryfikacji podlegać powinny także określone usługi świadczone przez przedsiębiorców mających siedzibę w Wielkiej Brytanii lub realizujące część zadań (np. wykorzystujące CPD) na terytorium Zjednoczonego Królestwa. Po wystąpieniu Wielkiej Brytanii z Unii Europejskiej jest ona bowiem traktowana jak państwo trzecie zarówno w świetle regulacji outsourcingowych, jak i w przypadku transferów danych osobowych, co wiąże się z dodatkowymi wymaganiami.

Kontrola nad podoutsourcingiem

Obszarem szczególnie istotnym dla outsourcingu usług chmury obliczeniowej, a nabierającym krytycznego znaczenia w przypadku korzystania z usług wykorzystujących chmurę obliczeniową, jest kwestia tzw. łańcucha outsourcingowego. Prawo bankowe dopuszcza możliwość korzystania z podwykonawców przez outsourcera (art. 6a ust. 7). W przypadku, w którym powierzenie poddostawcy outsourcowanych czynności nie ma charakteru jednorazowego, zmierzającego do usunięcia przyczyn uniemożliwiających świadczenie outsourcowanych usług, wymagana jednak będzie uprzednia zgoda banku.

W umowach z większymi dostawcami usług chmurowych mechanizm uprzedniej zgody na poddostawców jest coraz częściej spotykany, choć nadal można spotkać się z rozwiązaniami zakładającymi jedynie informowanie o zmianach na liście poddostawców. Część dostawców będzie ponadto informować wyłącznie poprzez zamieszczenie stosownej informacji na swojej stronie internetowej – niekiedy poprzez samą aktualizację listy, nie wskazując szczegółowych zmian. Taki mechanizm bez doprecyzowania go w umowie dodatkowymi postanowieniami trudno będzie uznać za spełniający wymaganie uzyskania uprzedniej zgody banku na powierzenie outsourcowanych czynności. Ponadto, może on prowadzić do niezamierzonego outsourcingu zagranicznego, co również powinno zostać uwzględnione w analizie ryzyka.

> ***Zbyt łagodne podejście do długości łańcucha outsourcingowego mogłoby prowadzić do utraty faktycznej kontroli nad outsourcingiem, niezamierzonego i bezprawnego ujawnienia tajemnicy bankowej oraz nieplanowanych transferów danych, czy też outsourcingu zagranicznego bez odpowiedniej uprzedniej analizy.***

W kwestii dalszego powierzenia outsourcowanych czynności zgodnie ze stanowiskiem UKNF[16], dopuszczalność łańcucha outsourcingowego powinna być postrzegana na dwóch płaszczyznach:

16 Zob. 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 30.11.2021).

- dopuszczalności powierzenia przetwarzania danych podmiotowi trzeciemu oraz oceny ryzyka ujawnienia informacji w kontekście udostępnienia lub powierzenia informacji prawnie chronionych na każdym etapie łańcucha outsourcingowego; oraz
- rzeczywistej kontroli wypełniania wymogów dotyczących powierzenia przetwarzania informacji prawnie chronionych zarówno przez dostawcę chmurowego, jak i innego dostawcę, który korzysta z usług chmurowych do świadczenia usług na rzecz podmiotu nadzorowanego.

Zbyt łagodne podejście do długości łańcucha outsourcingowego mogłoby prowadzić do utraty faktycznej kontroli nad outsourcingiem, niezamierzonego i bezprawnego ujawnienia tajemnicy bankowej oraz nieplanowanych transferów danych, czy też outsourcingu zagranicznego bez uprzedniej analizy i spełnienia szeregu wymagań prawnych w tym zakresie. Nie można jednak nie zauważyć, że w obecnych realiach rynkowych liberalizacja zasad tworzenia łańcucha outsourcingowego wydaje się być koniecznością z uwagi na praktykę panującą na rynku. Coraz więcej usług bazuje bowiem na wystandaryzowanych rozwiązaniach dostarczanych przez wysoce wyspecjalizowane podmioty. Wiele firm korzysta z podwykonawców, w tym także z innych spółek z własnych grup kapitałowych – świadczenie usługi end-to-end przez wyłącznie jeden podmiot stało się rzadkością.

Problem ten nasila się w przypadku usług wykorzystujących chmurę obliczeniową (dostawca banku niebędący dostawcą chmury; dostawca usług chmury obliczeniowej jako poddostawca). Rzadkością jest bowiem sytuacja, w której dostawca usług chmury obliczeniowej sam nie korzysta z usług żadnych poddostawców.

Tajemnica bankowa

Wśród obszarów krytycznych z punktu widzenia migracji chmurowej banku nie sposób nie wspomnieć o zasadach związanych z przetwarzaniem i ujawnianiem informacji objętych tajemnicą bankową, a więc wszystkich danych dotyczących czynności bankowej, uzyskanych w czasie negocjacji lub w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje – w szczególności danych klientów. O ile ujawnienie informacji chronionych tajemnicą bankową dostawcom i poddostawcom wykonującym czynności na podstawie umowy outsourcingowej jest zasadniczo możliwe (art. 104 ust. 2 pkt 2 prawa bankowego), o tyle pamiętać należy, że może to nastąpić jedynie w zakresie niezbędnym do należytego wykonywania tych czynności. Informacje objęte tajemnicą bankową należy również odpowiednio zabezpieczyć przed nieuprawnionym ujawnieniem.

Jako regułę należy przyjąć szyfrowanie informacji chronionych zarówno „at rest" – w trakcie przechowywania, jak i „in transit" – podczas przesyłania między poszczególnymi systemami. Zarządzanie (generowanie, przechowywanie, niszczenie) kluczami szyfrującymi powinno natomiast znajdować się po stronie banku. Chyba że z oszacowania ryzyka wynika, iż dopuszczalne lub wskazane jest używanie kluczy szyfrujących generowanych lub zarządzanych przez dostawcę usług chmury obliczeniowej. Szyfrowanie informacji nie zmniejsza jednak ważności informacji, nie zmienia też jej klasyfikacji i oceny[17].

W świetle wymagań zawartych w komunikacie chmurowym brak identyfikowanego dostępu do informacji chronionej (a więc np. dostęp wyłącznie do informacji zaszyfrowanych, bez możliwości ich odszyfrowania) przesądzał będzie o tym, czy dany podmiot może zostać uznany za poddostawcę w ramach łańcucha outsourcingowego. Poddostawcą jest w tym przypadku jedynie podmiot, który taki identyfikowany dostęp posiada. Komunikat nie modyfikuje jednak przepisów prawa.

W szczególności zaszyfrowanie danych powierzonych do przetwarzania dostawcy nie będzie wpływało na konieczność uzyskania zezwolenia na outsourcing zagraniczny (w przypadku, w którym dostawca będzie realizował powierzone zadania lub posiadał siedzibę w państwie trzecim)[18], jak również konieczność zawarcia umowy powierzenia przetwarzania danych osobowych, jeśli przetwarzane informacje stanowić będą dane osobowe.

W zakresie obowiązku zachowania poufności informacje chronione tajemnicą bankową powinny zostać również zabezpieczone poprzez ograniczenie dostępu do informacji jedynie do tych pracowników dostawcy, którzy potrzebują dostępu do wykonywania outsourcowanych czynności zgodnie z zasadą najmniejszego uprzywilejowania. Zarządzanie dostępami powinno być natomiast monitorowane przez bank i aktualizowane w przypadku zmian osobowych lub w zakresie usług. Równie istotne będzie także logowanie czynności dokonywanych na danych chronionych i monitorowanie zapisanych logów.

Projektowane zmiany dotyczące outsourcingu

20 lipca 2021 r. Minister Finansów zgłosił projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem rozwoju rynku

17 Zob. pkt VI.2.5.a Komunikatu.

18 Zob. 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 30.11.2021).

Fot. peshkov/stock.adobe.com

finansowego oraz ochrony inwestorów na tym rynku[19]. Oprócz zmian odnoszących się do rynku kapitałowego czy usług płatniczych, projektowany akt prawny wprowadza istotne modyfikacje związane z outsourcingiem w prawie bankowym. Mają one na celu w szczególności dostosowanie polskich przepisów do Wytycznych EBA, jak również umożliwienie bardziej efektywnego oraz elastycznego korzystania przez banki z instytucji outsourcingu.

Wśród najważniejszych zmian wyróżnić można:

1) Doprecyzowanie, że regulacji outsourcingu podlegają, oprócz umów o kartę płatniczą których stroną jest konsument oraz mikroprzedsiębiorca i mały przedsiębiorca, również umowy o inny instrument płatniczy.
2) Umożliwienie dalszego powierzania czynności innych niż tylko te służące realizacji głównego świadczenia wynikającego z umowy outsourcingowej (rozszerzenie zakresu czynności możliwych do powierzenia w ramach podoutsourcingu na wszystkie czynności wynikające z umowy outsourcingowej) – dzięki temu możliwe będzie szersze przekazywanie outsourcerom zadań innych niż tylko te stanowiące „główną" czynność poddaną outsourcingowi.
3) Ułatwienie powierzenia czynności outsourcerom spoza Europejskiego Obszaru Gospodarczego – obecnie wymaga to zgody KNF, jeśli zaś projekt ustawy wejdzie w życie w niezmienionym kształcie, to będzie to wymagało jedynie notyfikacji.
4) Dalsze odformalizowanie outsourcingu realizowanego przez inny bank i bank zagraniczny (ulga dla usług świadczonych w ramach grup kapitałowych i dla banków hipotecznych).

Należy pamiętać, że powyższe propozycje stanowią wciąż jedynie projekt zmian. Jednakże, biorąc pod uwagę fakt, że zgłaszającym jest podmiot rządowy, a zmiany stanowią w dużej mierze dostosowanie polskich przepisów do standardów unijnych, wejście w życie najbardziej istotnych z powyższych zmian jest wysoce prawdopodobne.

Czy chmura zawsze będzie outsourcingiem bankowym?

Jednym z istotnych zagadnień w kontekście usług świadczonych dla banków przez dostawców chmurowych jest kwestia outsourcingu. Outsourcing oznacza w tym przypadku powierzenie dostawcom zewnętrznym (tzw. outsourcerom) wykonywania czynności związanych z czynnościami bankowymi – poprzez pośrednictwo w ich wykonywaniu (np. udzielanie kredytów za pośrednictwem agentów)[20] albo wykonywanie czynności faktycznych związanych z czynnościami bankowymi[21].

19 Projekt dostępny jest na stronie: https://legislacja.gov.pl/projekt/12349203/katalog/12803524#12803524(dostęp 30.11.2021).

20 Art. 6a ust. 1 pkt. 1 prawa bankowego.

21 Art. 6a ust. 1 pkt. 2 prawa bankowego.

Pośród najważniejszych regulacji bankowych w kontekście outsourcingu należy wymienić następujące, z których część została już wcześniej wspomniana:

1) ustawa z dnia 29 sierpnia 1997 r. prawo bankowe;
2) wytyczne EBA z dnia 25 lutego 2019 r. w sprawie outsourcingu;
3) stanowisko UKNF z 16 września 2019 r dotyczące wybranych zagadnień związanych z wejściem w życie wytycznych EBA w sprawie outsourcingu i ich uwzględnianiem w działalności banków[22];
4) rozporządzenie Ministra Rozwoju i Finansów z dnia 10 maja 2017 r. w sprawie wykazu dokumentów dołączanych przez bank do wniosku o wydanie zezwolenia na powierzenie przedsiębiorcy lub przedsiębiorcy zagranicznemu wykonywania pośrednictwa w zakresie niektórych czynności[23];
5) pismo Narodowego Banku Polskiego (Generalnego Inspektoratu Nadzoru Bankowego) z dnia 21 grudnia 2004 r. ws. outsourcingu[24]; oraz
6) komunikat chmurowy.

Wymogi związane z outsourcingiem oraz przywileje outsourcerów

Powierzenie czynności na zasadzie outsourcingu podlega szczególnym ograniczeniom. Przykładowo, nie można powierzyć outsourcerom czynności związanych z zarządzaniem bankiem, oceną ryzyka oceną zdolności kredytowej czy przeprowadzaniem audytu wewnętrznego banku. Świadczenie na rzecz banków usług w modelu outsourcingowym wiąże się też z koniecznością spełnienia określonych obowiązków. Do najważniejszych spośród nich należą:

1) zapewnienie, że powierzenie określonych czynności dostawcy nie wpłynie negatywnie na zgodność z przepisami prawa, ostrożne i stabilne zarządzanie bankiem, skuteczność systemu kontroli wewnętrznej w banku, możliwość wykonywania obowiązków przez biegłego rewidenta upoważnionego do badania sprawozdań finansowych banku na podstawie zawartej z bankiem umowy oraz ochronę tajemnicy prawnie chronionej;
2) posiadanie (przez bank i dostawcę) planów działania zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym outsourcingiem;
3) brak możliwości wyłączenia odpowiedzialności outsourcera wobec banku za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy outsourcingowej;
4) w określonych przypadkach – uzyskanie zezwolenia Komisji Nadzoru Finansowego, po uprzednim przedstawieniu dokumentów dotyczących m.in. działalności gospodarczej dostawcy, projektu umowy outsourcingowej, planów ciągłości czy opisu rozwiązań technicznych i zasad zarządzania ryzykiem;
5) w przypadku, gdy dostawca posiada siedzibę poza terenem Unii Europejskiej albo outsourcing obejmuje powierzenie czynności technicznych – zawiadomienie Komisji Nadzoru Finansowego;

Ponadto, Komisja Nadzoru Finansowego posiada szczególne uprawnienia w zakresie nadzoru nad relacjami banków z outsourcerami. Zaliczają się do nich uprawnienia kontrolne w zakresie spełniania przez banki i dostawców wymogów prawnych, możliwość żądania od banków określonych dokumentów związanych ze **świadczeniem tych** usług oraz uprawnienie do wydania decyzji w sprawie zmiany lub rozwiązania umowy outsourcingowej.

Usługi chmurowe a regulacja outsourcingu

Jednym z zagadnień rozważanych przy okazji świadczenia usług z zakresu technologii chmury obliczeniowej jest kwestia podlegania przez dostawców pod przepisy o outsourcingu. Jak wskazano powyżej, outsourcing dotyczy m.in. „czynności faktycznych związanych z działalnością bankową”[25], co potwierdzają także stosowne pisma wydane przez nadzór finansowy[26].

W kontekście powyższego należy rozróżnić typowe czynności wykonywane w ramach outsourcingu (a więc inherentnie związane z czynnościami bankowymi) oraz te, które są powierzane podmiotem trzecim, lecz nie są związane z czynnościami bankowymi[27]. Pytaniem pozostaje, gdzie należy zakreślić różnicę między jednymi i drugimi czynnościami oraz w jaką kategorię wpisują się usługi chmurowe.

Co do zakresu czynności faktycznych związanych z czynnościami bankowymi wypowiedział się Główny Inspektorat Nadzoru Bankowego, który odwołuje się do „funkcjonalnego związku”. Jednocześnie, GINB wskazuje, że mowa tu jedynie o czynnościach, które mają „bezpośredni związek” z prowadzoną działalnością bankową. Mowa tu o następujących typach usług:

22 Dostępne na stronie: https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_outsourcingu_67075.pdf (dostęp 30.11.2021).

23 Dostępne na stronie: http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20170000960 (dostęp 30.11.2021).

24 Sygn. NB-BPN-I-022-70/04.

25 Art. 6a ust. 1 pkt. 2 prawa bankowego.

26 Patrz pismo GINB z dnia 21 grudnia 2004 r. ws. outsourcingu.

27 Np. usługa polegająca na sprzątaniu biura.

1) usługi stanowiące część składową świadczonej czynności bankowej[28];
2) usługi niezbędne ze względu na istotę lub charakter czynności bankowej[29]

W przypadku usług tego drugiego typu bardzo trudne jest praktyczne wyodrębnienie tego, jaka czynność stanowi „usługę niezbędną". Jest to bowiem pojęcie ocenne. W dokonaniu ewaluacji tego, czy dana czynność faktyczna z zakresu technologii informatycznych pomagają wytyczne wskazane w piśmie GINB. W pierwszej kolejności konieczna jest ocena tego, czy dane czynności rzeczywiście mają bezpośredni związek z regulowanymi czynnościami bankowymi. Oprócz tego, istotne jest to, czy wykonawca uzyskuje dostęp do informacji „wrażliwych" z punktu widzenia banku (w szczególności tajemnicy bankowej) oraz czy czynności te mają na celu zapewnienie ciągłego i niezakłóconego działania systemów informatycznych służących bezpośrednio do wykonywania działalności bankowej. Wśród przykładowego zakresu usług technologicznych, jakie powinny być traktowane jako podlegające regulacji outsourcingu GINB wymienia m.in.:

- obsługa systemów bankowych służących do rejestracji operacji dokonywanych na rachunkach klientów banku;
- obsługa systemów obsługi kredytów służących do gromadzenia danych o klientach oraz o produktach bankowych, z którymi wiąże się ryzyko kredytowe;
- obsługa systemów składania zleceń przez klientów banku drogą elektroniczną;
- obsługa systemów służących do oceny zdolności kredytowej klientów banku; lub
- obsługa systemów służących do zarządzania ryzykiem bankowym.

Jednocześnie, GINB bezpośrednio wskazuje, że outsourcingiem nie są następujące usługi:

- nabywanie sprzętu komputerowego;
- nabywania i instalacja oprogramowania;
- tworzenie, rozwój i modyfikacja licencjonowanego oprogramowania;
- serwis sprzętu komputerowego;
- serwis standardowego oprogramowania operacyjnego/systemowego; lub
- czynności dotyczące systemów informatycznych/oprogramowania, które nie są bezpośrednio wykorzystywane w działalności bankowej[30].

28 Np. element aplikacji odnoszący się bezpośrednio do składania wniosku kredytowego w ramach czynności bankowej jaką jest udzielenie kredytu.

29 Tj. usługa, bez której nie jest faktycznie możliwe wykonanie umowy, której dotyczy dana czynności bankowa.

30 Np. systemów kadrowo-płacowych banku, programów wykorzystywanych do prowadzenia gospodarki materiałowej banku.

Obecnie przyjętym przez sektor podejściem jest w praktyce uzależnienie kwestii tego, czy dana usługa chmurowa stanowi outsourcing od przekazywania tajemnicy bankowej oraz kluczowości wprowadzanych rozwiązań dla funkcjonowania banku jako organizacji. Wydaje się, że to podejście nie jest do końca właściwe. Przede wszystkim nie tyle wynika ono z istniejących przepisów, co jest pochodną kwestii możliwości przekazywania danych objętych tajemnicą bankową dostawcom. Gdyby bowiem nie uznawać danej usługi za outsourcing, w praktyce możliwość przekazywania im tajemnicy bankowej jest ograniczona i wymaga znalezienia alternatywnej podstawy prawnej. Powoduje to, iż jako outsourcing często kwalifikowane są usługi i czynności, które nie są wcale bezpośrednio związane z wykonywaniem czynności bankowych.

> ***Nie można nie zauważyć, że w obecnych realiach rynkowych liberalizacja zasad tworzenia łańcucha outsourcingowego wydaje się być koniecznością z uwagi na praktykę panującą na rynku. Coraz więcej usług bazuje bowiem na wystandaryzowanych rozwiązaniach dostarczanych przez wysoce wyspecjalizowane podmioty.***

JAK PRZYGOTOWAĆ BANK DO MIGRACJI CHMUROWEJ?

Pierwszym przystankiem na chmurowej mapie każdego projektu powinna być identyfikacja wymagań, których stosowanie będzie obowiązkowe w przypadku danego wdrożenia. Nie w każdym przypadku stosować bowiem należy komunikat chmurowy. Nie znajdzie on w szczególności zastosowania do usług chmury obliczeniowej prywatnej, a więc takiej, która przeznaczona jest do wyłącznego użytku jednego podmiotu nadzorowanego lub znajduje się w posiadaniu lub jest bezpośrednio zarządzana przez ten podmiot

nadzorowany. Ta zasadniczo nie jest przedmiotem niniejszego opracowania.

Posiadanie chmury obliczeniowej nie oznacza, że bank musi być jej właścicielem. Celem jest zapewnienie bezpiecznego, pod względem prawnym i faktycznym, posiadania chmury obliczeniowej przez okres korzystania. Należy przy tym uwzględnić 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 w szczególności możliwość wprowadzania zmian w infrastrukturze (w tym wymiana sprzętu, aktualizacja oprogramowania), decydowanie o zasadach fizycznego dostępu do infrastruktury oraz decydowanie o zasadach ochrony fizycznej i logicznej infrastruktury.[31].

W praktyce chmura prywatna będzie zdecydowanie rzadziej wykorzystywana niż chmura publiczna, co wynika m.in. z kosztów dla utrzymywania własnych rozwiązań chmurowych. Najczęściej będzie ona występować jako element chmury obliczeniowej hybrydowej. Jeżeli bowiem dostawca oferuje usługę polegającą na dostarczaniu oprogramowania na rzecz wielu podmiotów, a dane podmiotów są separowane tylko w sposób logiczny, to taką usługę uznać należy za oferowaną w modelu chmury publicznej, nawet jeśli z punktu widzenia tego dostawcy chmura znajduje się w jego wyłącznym posiadaniu i jest przez niego bezpośrednio zarządzana.

Poniżej znajdują się elementy wdrożenia w banku usług chmury obliczeniowej publicznej w założeniu, że komunikat chmurowy znajduje zastosowanie.

Określenie strategii chmurowej

Krokiem, który wprawdzie nie znajduje odzwierciedlenia w komunikacie chmurowym, ale bez którego trudno wyobrazić sobie udaną transformację banku do chmury, jest określenie strategii chmurowej. Praktyka pokazuje tymczasem, że wiele banków nadal nie posiada sprecyzowanej idei w zakresie wdrażania i rozwoju rozwiązań chmurowych. Warto wiedzieć, że to identyfikacja potrzeb biznesowych i celu wykorzystania chmury obliczeniowej pozwala określić program i zakres transformacji chmurowej, zdefiniować niezbędne zmiany w organizacji, a także konieczne umiejętności IT i niezbędne wsparcie profesjonalnych dostawców usług. Prawidłowe określenie strategii chmurowej pozwoli natomiast oszacować koszty i sprecyzować oczekiwane efekty transformacji chmurowej. Brak przygotowania takiej strategii oznacza, że efektywne wdrożenie rozwiązań chmurowych nie będzie możliwe, a bank naraża się na ryzyko wystąpienia błędów i problemów regulacyjnych.

Zapewnienie wewnętrznych kompetencji i wsparcie zewnętrzne

Fundamentem udanego projektu - nie tylko wdrożenia chmury obliczeniowej - jest stworzenie zespołu projektowego, posiadającego odpowiednie kompetencje. Bank powinien określić kompetencje niezbędne podczas wdrożenia i przy utrzymaniu konkretnych rozwiązań chmurowych. Kompetencje powinny zapewniać bezpieczeństwo, spójność architektoniczną oraz dostarczać odpowiednie wsparcie rozwiązań, a także rozliczalność wykorzystywanych usług chmury obliczeniowej. Przykładowymi kompetencjami w ramach wdrażania i utrzymania rozwiązań w chmurze obliczeniowej są[32]:

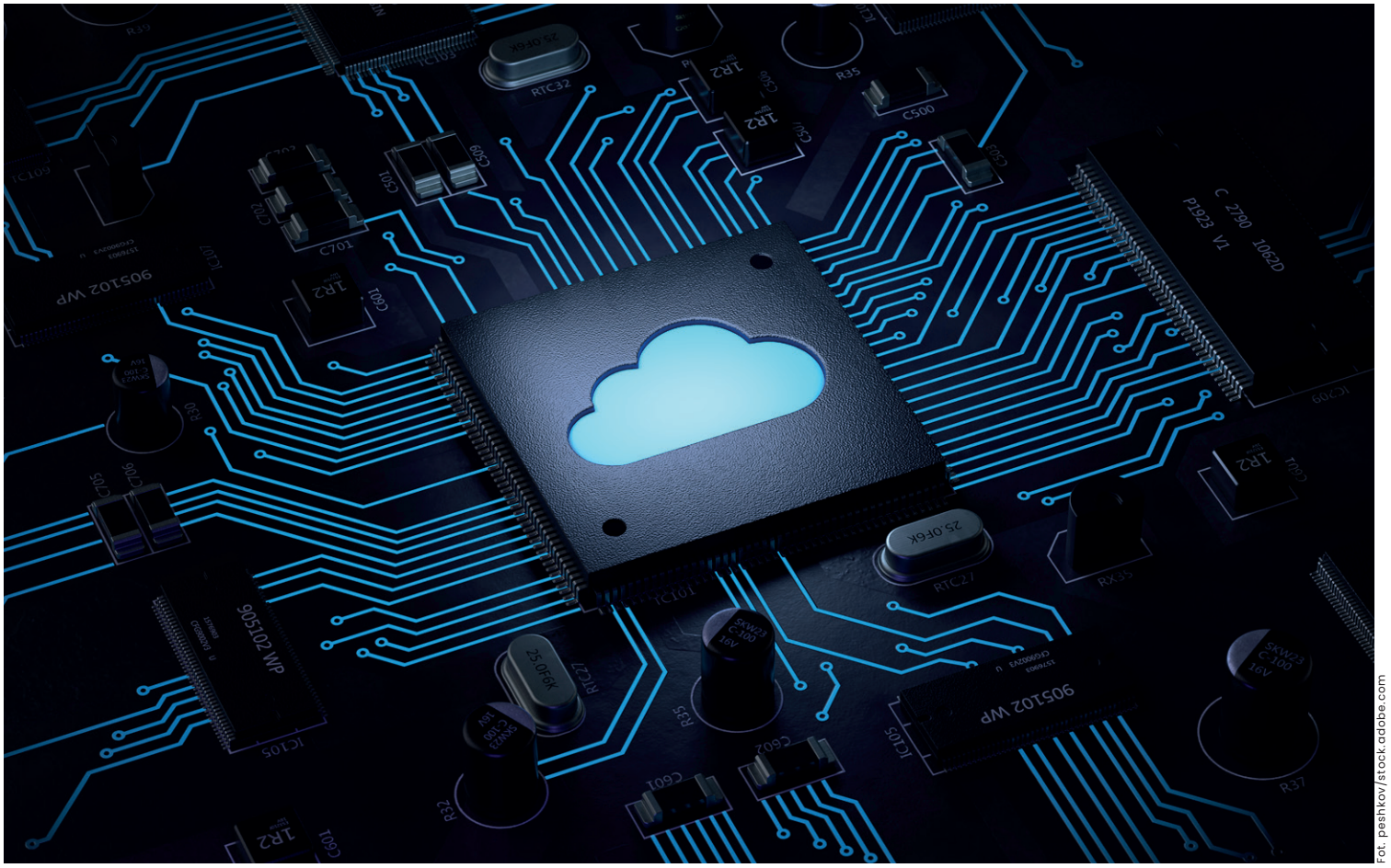
- architektura (rola: architekt infrastruktury);
- bezpieczeństwo (rola: inżynier/specjalista ds. bezpieczeństwa);
- rozwój (role: developer oprogramowania, inżynier DevOps);
- utrzymanie i operacje (role: administrator systemu/sieci, inżynier DevOps);
- biznes (rola: opiekun biznesowy); oraz
- zgodność z wymaganiami prawnymi i umownymi (rola: specjalista ds. compliance, prawnik).

W przypadku identyfikacji luk kompetencyjnych wewnątrz organizacji bank powinien zaadresować je poprzez nabycie takich kompetencji. Może to nastąpić poprzez szkolenia zewnętrzne, wewnętrzne, przenoszenie wiedzy w ramach organizacji itp. Bank może też skorzystać ze wsparcia firm świadczących usługi konsultacyjno-doradcze w zakresie chmury obliczeniowej. Ponadto, w ramach utrzymania produkcyjnych systemów przetwarzających informacje w chmurze obliczeniowej bank powinien posiadać aktywne wsparcie dostawców usług chmury obliczeniowej i zadbać o kontraktowe uregulowanie warunków tego wsparcia.

---

31 Zob. 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 30.11.2021).

32 Por. Standard Wdrożeń Przetwarzania Informacji w chmurze obliczeniowej opracowany przez Polską Izbę Ubezpieczeń, s. 19-20, który w tym zakresie można z powodzeniem zastosować również do sektora bankowego (https://piu.org.pl/wp-content/uploads/2021/06/standard-chmura-obliczeniowa-1.pdf, dostęp 30.11.2021).



Fot. peshkov/stock.adobe.com

Klasyfikacja informacji i data governance

Przed powierzeniem przetwarzania informacji w chmurze obliczeniowej konieczne jest przeprowadzenie klasyfikacji tych informacji. Większość podmiotów nadzorowanych, w tym banków, posiadało mniej lub bardziej rozbudowane polityki klasyfikacji informacji jeszcze przed pojawieniem się komunikatu chmurowego. Zaobserwować można jednak, że przyjęta w wielu organizacjach metodyka klasyfikacji informacji nie odzwierciedla formalnych wymagań dotyczących przetwarzania i bezpieczeństwa informacji.

Często spotyka się podział na cztery klasy informacji[33], gdzie o przypisaniu informacji do danej klasy decyduje najczęściej wysokość potencjalnej szkody wyrządzonej organizacji w przypadku naruszenia bezpieczeństwa informacji. Wiele zależy od dokładnego zdefiniowania poszczególnych klas, ale generalny problem z tak określonymi klasami informacji polega na tym, że klasa jako taka nie informuje o charakterze samej informacji, a stanowi w rzeczywistości wstępne i raczej uproszczone szacowanie ryzyka - często bez znajomości odpowiedniego kontekstu przetwarzania informacji.

Klasyfikacja wymagana przez komunikat chmurowy powinna mieć na celu identyfikację informacji prawnie chronionej celem potwierdzenia konieczności stosowania wymagań komunikatu (co najmniej podział na informacje prawnie chronione i pozostałe informacje), a także identyfikację pozostałych wymagań prawnych, które należy spełnić przed przystąpieniem do przetwarzania informacji w chmurze. Rekomendowane byłoby zatem przynajmniej takie zdefiniowanie klas informacji, aby dane objęte tajemnicą bankową posiadały odrębną klasę, uwzględniającą wymagania prawne i zasady ich przetwarzania.

Warto także rozważyć wyodrębnienie klasy obejmującej informacje krytyczne (szczególnie wrażliwe), które ze swojej natury w ogóle nie powinny być przetwarzane w chmurze obliczeniowej publicznej lub hybrydowej (np. informacje niejawne). Rekomenduje się także rozróżnienie klas w ramach danych osobowych przetwarzanych w organizacji. Informacje dotyczące osób fizycznych mogą mieć bowiem różną wrażliwość, i o ile przetwarzanie danych kontaktowych przedstawiciela partnera nie będzie raczej wymagać dodatkowych nakładów na bezpieczeństwo, o tyle już w przypadku danych biometrycznych (np. używanych do logowania lub przeciwdziałania przestępstwom płatniczym) konieczne będzie zastosowanie wyższego standardu ochrony.

33 Przykładowo: pierwsza (najniższa) obejmuje informacje publiczne, druga informacje wewnętrzne, trzecia informacje chronione, a czwarta informacje wrażliwe.

Dobrą praktyką jest określenie ramowych minimalnych warunków zabezpieczeń obowiązujących w odniesieniu do poszczególnych klas informacji. Przypisanie danej informacji do określonej klasy powinno skutkować zastosowaniem adekwatnych środków bezpieczeństwa (w obszarach poufności, integralności i dostępności) informacji z perspektywy skutków finansowych i regulacyjnych dla organizacji. Na potrzeby wdrożeń chmurowych konieczne jest:

1) opisanie zasad klasyfikacji (polityka klasyfikacji informacji wraz ze stosowną procedurą);
2) udokumentowanie wyników przeprowadzonej klasyfikacji w kontekście danej usługi chmurowej; oraz
3) przeprowadzanie okresowych przeglądów klasyfikacji informacji (nie rzadziej niż raz w roku) wraz z potwierdzeniem aktualności jej wyników.

> ***Kluczowym wymaganiem komunikatu chmurowego jest kompleksowe szacowanie ryzyka przetwarzania informacji w chmurze obliczeniowej przez bank. Szacowanie ryzyka powinno być przeprowadzone w kontekście dokonanej klasyfikacji i oceny informacji i obejmować m.in. identyfikację, analizę oraz ocenę zagrożeń.***

W szerszym ujęciu, niż wynika to z samego komunikatu, klasyfikacja informacji jest tylko częścią systemu zarządzania informacją (data governance) w organizacji. W założeniu system ten powinien mieć na celu identyfikację właścicieli poszczególnych zasobów informacyjnych oraz dokładne mapowanie przepływów danych w organizacji, z uwzględnieniem aplikacji i systemów wykorzystywanych do przetwarzania danych. Oprócz zapewnienia odpowiednich środków bezpieczeństwa dla poszczególnych zasobów informacyjnych należy także pamiętać o rzeczywistym wdrożeniu retencji informacji (nie tylko danych osobowych). Zarządzanie danymi (data governance) zmierzać powinno w kierunku poprawy jakości informacji, poprzez ograniczenie przetwarzania jedynie do danych o istotnym i aktualnym znaczeniu z punktu widzenia biznesu. Może się bowiem okazać, że brak systemowego podejścia do zarządzania informacją w banku stanowić będzie przeszkodę dla większych i bardziej złożonych projektów chmurowych (np. wdrożeń IaaS czy PaaS).

Ocena informacji – dopuszczalność przetwarzania w chmurze

W odróżnieniu od klasyfikacji informacji, celem oceny informacji jest zbadanie dopuszczalności przetwarzania informacji z wykorzystaniem usług chmury obliczeniowej. Ocena informacji powinna odbywać się zawsze w kontekście przeprowadzonej klasyfikacji, uwzględniając także skalę prowadzonej działalności (istotność procesu realizowanego w chmurze), zakres informacji, ich rodzaj i ważność, a także wartość informacji dla banku. Jedynie łączna analiza powyższych czynników pozwoli ocenić, czy dana informacja może być przetwarzana w chmurze.

Wartość informacji stanowić powinny określone dla danego banku konsekwencje materializacji ryzyka polegającego na nieuprawnionym ujawnieniu, zmianie lub zniszczeniu informacji, które mają być przetwarzane w chmurze. Wartość powinna być w miarę możliwości oszacowana kwotowo. Dokonując szacowania wartości informacji można wziąć pod uwagę w szczególności następujące czynniki:

1) potencjalne kary finansowe związane z takim naruszeniem, przy czym szacowanie kary powinno odnosić się do prawdopodobnych wartości, o ile to możliwe z uwzględnieniem danych historycznych (decyzji organów, wyroków sądów, itp.);
2) koszty związane z identyfikacją i usuwaniem naruszenia (np. przywrócenie dostępności systemów, naprawa sprzętu, odtworzenie danych, usługi informatyki śledczej itp.);
3) koszty i utracone przychody wynikające z czasowego lub trwałego braku możliwości prowadzenia sprzedaży, wliczając utratę klientów; oraz
4) koszty reputacyjne oraz wydatki poniesione na obszar PR w przypadku naruszenia bezpieczeństwa informacji.

Ocena informacji powinna również obejmować analizę występowania ograniczeń regulacyjnych, kontraktowych i wewnątrzorganizacyjnych, a także innych okoliczności mogących uniemożliwiać lub ograniczać korzystanie z chmury obliczeniowej (np. ograniczenia terytorialne, ograniczenia w zakresie tworzenia łańcucha outsourcingowego, warunki umowne i regulaminowe odnoszące się do określonych procesów, wewnętrzne procedury ograniczające możliwość przetwarzania określonych informacji z wykorzystaniem usług chmury obliczeniowej, itd.). Wszelkie ograniczenia powinny zostać należycie udokumentowane.

Outsourcing szczególny chmury obliczeniowej

Komunikat chmurowy będzie znajdował zastosowanie nie tylko w przypadku powierzenia przetwarzania informacji objętych ta-

jemnicą bankową z wykorzystaniem usług chmury obliczeniowej publicznej lub hybrydowej, ale także w przypadku wystąpienia outsourcingu szczególnego chmury obliczeniowej. Brak wnikliwej analizy procesu, którego realizacja jest planowana w chmurze, a także odpowiednio przeprowadzonej klasyfikacji i oceny informacji stanowi poważną przeszkodę w ustaleniu, czy w danym przypadku występuje outsourcing szczególny chmury obliczeniowej.

Przez outsourcing szczególny należy rozumieć sytuację, w której bank powierza dostawcy usług chmury obliczeniowej czynności (funkcje), których brak lub przerwa w realizacji spowodowana naruszeniem bezpieczeństwa usługi lub informacji:

1) wpłynęłaby w sposób istotny na ciągłość wypełniania przez bank warunków stanowiących podstawę uprawnienia prowadzenia działalności nadzorowanej (tj. zezwolenia na prowadzenie działalności bankowej); lub
2) zagrażałaby w sposób istotny wynikom finansowym banku; lub
3) zagrażałaby w sposób istotny niezawodności lub ciągłości wykonywania działalności nadzorowanej przez bank.

W zależności od istotności realizowanego procesu, klasy i oszacowanej wartości informacji, a także oceny skutków naruszenia któregoś z atrybutów bezpieczeństwa informacji (dla reputacji, wyników finansowych, ciągłości i niezawodności działania oraz uprawnienia do prowadzenia działalności regulowanej przez bank) bank będzie w stanie stwierdzić, czy w danym przypadku występuje outsourcing szczególny w rozumieniu komunikatu. Kryteria tej oceny każdorazowo zależą od banku i konkretnego procesu realizowanego w chmurze. Ocena powinna jednak zostać udokumentowana i regularnie monitorowana w celu potwierdzenia jej aktualności.

Szacowanie ryzyka przetwarzania w chmurze - metodyka

Kluczowym wymaganiem komunikatu chmurowego jest kompleksowe szacowanie ryzyka przetwarzania informacji w chmurze obliczeniowej przez bank. Szacowanie ryzyka powinno być przeprowadzone w kontekście dokonanej klasyfikacji i oceny informacji i obejmować identyfikację, analizę oraz ocenę zagrożeń, a także możliwość ich wystąpienia i wpływ materializacji poszczególnych ryzyk na bank. Szacowanie ryzyka jest prowadzone w sposób ciągły, z uwzględnieniem praktycznej implementacji zasady PDCA („plan – do – check – act").

Bank powinien przeprowadzić szczegółową identyfikację zagrożeń związanych z korzystaniem z usług chmury obliczeniowej w konkretnym procesie biznesowym wraz ze wskazaniem źródła każdego ryzyka (np. postanowienia umowy z dostawcą, informacje dostępne publicznie, w tym informacje o incydentach bezpieczeństwa, dokumentacja techniczna, itp.). Poszczególne zagrożenia będą oczywiście różnić się w zależności od wykorzystywanych usług, jednakże najczęściej będzie można przyporządkować je do następujących obszarów ryzyka:

- rozproszenie geograficzne (lokalizacje) przetwarzania;
- korzystanie z usług chmury obliczeniowej w sposób inny niż zamierzony;
- ujawnienie i dostęp do informacji objętej tajemnicą bankową;
- własność danych i kontrola przetwarzania;
- zgodność z przepisami dotyczącymi przetwarzania danych osobowych i zabezpieczenie transferów danych;
- podatności interfejsów i błędy konfiguracji;
- zakres szyfrowania i zarządzanie kluczami szyfrującymi;
- kompetencje wewnętrzne, w tym kompetencje techniczne;
- ograniczona kontrola nad przebiegiem współpracy z dostawcą;
- vendor lock-in; oraz
- umowa z dostawcą.

Każde spośród zidentyfikowanych zagrożeń powinno zostać ocenione pod kątem wpływu na reputację, wyniki finansowe, ciągłość i niezawodność działania oraz uprawnienia do prowadzenia działalności regulowanej przez bank. Następnie należy również oszacować prawdopodobieństwo wystąpienia poszczególnych zagrożeń. Oceniając prawdopodobieństwo trzeba wziąć pod uwagę co najmniej wiedzę historyczną dotyczącą wystąpienia podobnych zagrożeń, dostępną ekspercką wiedzę w tym zakresie oraz ustaloną wartość informacji przetwarzanych w usługach chmury obliczeniowej. Ponadto, uwzględnieniu podlegać powinny również wzajemne korelacje pomiędzy poszczególnymi zagrożeniami (np. ograniczenia kontroli nad przetwarzaniem informacji wynikające z lokalizacji przetwarzania). Powyższa ocena powinna być regularnie monitorowana i w razie konieczności aktualizowana.

Bank powinien sporządzić szczegółowy plan postępowania z ryzykiem, będącym wypadkową oceny wpływu poszczególnych zagrożeń i prawdopodobieństwa ich materializacji. Plan zarządzania ryzykiem powinien obejmować przynajmniej:

- opis zidentyfikowanych ryzyk;
- strategię postępowania z ryzykiem (redukcja, unikanie, przeniesienie, akceptacja);
- zasady akceptacji poziomu ryzyka;
- zasady monitorowania tych ryzyk; oraz
- uprawnienia, odpowiedzialności i wymagane zasoby związane z monitorowaniem ryzyka i wdrożeniem wybranej strategii postępowania z ryzykiem.

Ustalając plan postępowania z ryzykiem należy ponadto wziąć pod uwagę wymaga-

nia przepisów prawa, regulacji wewnętrznych i postanowień umownych, stopień złożoności organizacyjnej i czynniki występujące w grupie kapitałowej banku, a także efektywność stosowanych mechanizmów kontrolnych. W przypadku podjęcia decyzji o wdrożeniu usług chmury obliczeniowej w zakresie będącym przedmiotem szacowania ryzyka, wyniki przeprowadzonej analizy oraz ustalony plan postępowania z ryzykiem powinny podlegać zatwierdzeniu przez zarząd banku lub inne uprawnione przez zarząd osoby.

Wybrane ryzyka - vendor lock-in i utrata ciągłości działania

Ryzykami szczególnie istotnymi z punktu widzenia wykorzystania chmury obliczeniowej w banku są utrata ciągłości działania oraz tzw. vendor lock-in.

Vendor lock-in jest sytuacją, w której brak zgodności technologicznej pomiędzy usługami różnych dostawców chmury obliczeniowej powoduje przywiązanie banku do jednego dostawcy usług chmury obliczeniowej poprzez ograniczenie albo brak możliwości przenoszenia (korzystania z identycznych) usług lub przetwarzanych informacji[34]. Dlatego przy wyborze dostawcy usługi chmurowej należy brać zawsze ryzyko „nieprzenoszalności" usługi chmurowej. Banki powinny z ostrożnością podchodzić do rozwiązań niezastępowalnych, które choć coraz rzadsze, nadal występują na rynku usług chmurowych.

Bank przenoszący swoje zasoby do chmury obliczeniowej powinien zawsze brać pod uwagę ryzyko niespodziewanej i trwałej utraty dostępu do świadczonej usługi chmurowej. Odpowiedzialna strategia chmurowa będzie zakładała tworzenie rozwiązań hybrydowych, wykorzystujących nie tylko chmurę publiczną, ale także elementy chmury prywatnej lub rozwiązań on-premise. Istotne jest także nieuzależnianie się wyłącznie od jednego dostawcy (choć czasem może się to wydawać korzystne z komercyjnego punktu widzenia), ale wykorzystywanie usług chmurowych dostarczanych przez wielu dostawców (multicloud). Przekłada się to na brzmienie planów ciągłości działania i planów wycofania z chmury.

34 Zob. pkt VI.2.1.e komunikatu chmurowego.

Jednocześnie warto podkreślić, że strategia chmurowa czy polityka outsourcingowa (oraz wynikające z nich plan ciągłości działania czy exit plan) mogą przewidywać, że usługa chmurowa może być także przeniesiona z powrotem do rozwiązania on-premise. Wszystko zależy oczywiście od rodzaju i cech czynności przetwarzanej w chmurze, możliwości finansowych banku oraz w końcu od dostępności danej usługi w tym modelu.

Polityka outsourcingu chmurowego

Większość banków posiada wdrożoną politykę outsourcingową regulującą wewnątrzorganizacyjne zasady powierzenia czynności związanych z działalnością bankową podmiotom zewnętrznym. Wymóg posiadania takiej polityki wynika również z wytycznych EBA w sprawie outsourcingu.

Choć komunikat chmurowy nie wymaga wprost posiadania odrębnego dokumentu określającego politykę banku w zakresie outsourcingu chmury obliczeniowej, to trudno wyobrazić sobie realizację tak złożonego procesu i uwzględnienie wszystkich wymienionych wyżej elementów w oderwaniu od ustalonych procesów korporacyjnych. Rekomendowanym rozwiązaniem jest aktualizacja istniejącej w banku polityki outsourcingowej (np. poprzez dodanie załącznika) lub utworzenie nowej polityki w zakresie outsourcingu chmury obliczeniowej.

Polityka outsourcingu chmurowego powinna obejmować elementy wskazane w niniejszym rozdziale oraz opisywać ogólne reguły regulujące wdrażanie, utrzymywanie i ewentualną rezygnację (w tym przymusową) z usług chmurowych. Rekomendowane jest także uwzględnienie w niej wymagań odnośnie do procesu zakupowego usług chmurowych oraz wymagań, jakie spełniać muszą dostawcy już na etapie zapytań ofertowych.

UMOWA Z DOSTAWCĄ USŁUG CHMUROWYCH

Zagadnienia ogólne

Niezwykle istotnym aspektem każdego wdrożenia chmurowego w banku, obok wielokrotnie wspomnianego w niniejszym raporcie zapewnienia zgodności środowiska prawnego, compliance, finansowego, bezpieczeństwa oraz infrastruktury IT z wymogami regulacji prawnych wiążących banki w zakresie rozwiązań chmurowych jest umowa z dostawcą usług chmurowych.

Umowa o świadczenie usług chmurowych publicznych[35], które wymagają powierzenia tajemnicy bankowej lub stanowią outsourcing szczególny chmury obliczeniowej (zgodnie z objaśnieniami w niniejszym opracowaniu) będzie najczęściej wymagać nie tyl-

35 Zgodnie z komunikatem chmurowym chmura obliczeniowa publiczna to chmura dostępna do użytku publicznego, będąca w posiadaniu lub bezpośrednio zarządzana przez dostawcę usług chmury obliczeniowej;

Fot. jirsak/stock.adobe.com

ko dostosowania do wymagań prawa bankowego i komunikatu chmurowego, ale również zapewnienia zgodności z przepisami dotyczącymi ochrony danych osobowych. Nadmienić przy tym warto, że nawet jeśli zgodnie z matrycą stosowania komunikatu chmurowego, w stosunku do usługi chmurowej dla banku nie stosujemy jego postanowień, a także gdy zastosowania nie znajdą przepisy prawa bankowego (outsourcing nieregulowany), to w przypadku przetwarzania w chmurze danych osobowych nadal należy jednak zapewnić zgodność z RODO[36]oraz regulacjami wewnętrznymi banku[37].

Jeśli zaś chodzi o jej aspekt czysto formalny komunikat chmurowy wymaga, by umowa miała charakter sformalizowany, przy czym dopuszczalne jest (i powszechnie stosowane), że będzie ona w zasadzie kombinacją umów, oświadczeń, regulaminów i warunków korzystania z usług – także w wersji elektronicznej. Jednocześnie lista wymogów w zakresie jej treści nie ma charakteru zamkniętego ani wyłącznego (tzn. nie każdy jej punkt musi zostać pokryty umową na usługę chmurową), a ostateczna jej treść zależy od usługi będącej przedmiotem umowy i zakresu przetwarzanych informacji.

W komunikacie zawarto następujący katalog wymagań, które powinny zostać uwzględnione w umowie z dostawcą usług chmury obliczeniowej[38]:

a) klarowny podział odpowiedzialności w odniesieniu do bezpieczeństwa przetwarzanych informacji, z uwzględnieniem modelu świadczenia usług, ciągłości działania usług (z uwzględnieniem parametrów RTO i RPO tam, gdzie to zasadne) oraz deklarowanego SLA wraz z metodą pomiaru i raportowania;
b) klarowną definicję i wskazanie lokalizacji przetwarzania informacji oraz metod jej weryfikacji i zabezpieczenia zgodności przez co najmniej referencyjne odniesienie do właściwych dokumentów, opisów konfiguracyjnych, metod i narzędzi;
c) prawo właściwe dla umowy (w tym sąd właściwy i zasady rozstrzygania sporów);
d) potwierdzenie zgodności zasad przetwarzania danych osobowych z prawem Unii Europejskiej, o ile ma to zastosowanie;
e) własność przetwarzanych informacji w trakcie trwania umowy oraz po jej zakończeniu (wygaśnięciu, rozwiązaniu), także w sposób nieplanowany;

36 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

37 Rozważania dotyczące charakteru prawego komunikatu chmurowego oraz konieczności jego stosowania względem usługi chmurowej dla banku jak również o stosunku przepisów prawa bankowego w zakresie outsourcingu bankowego do usług chmurowych znajdują się we poprzednich rozdziałach niniejszego opracowania.

38 Zob. pkt VII.4.1. komunikatu chmurowego.

f) gwarancje, rękojmie, ubezpieczenia (polisy ubezpieczeniowe dostawcy usług chmury obliczeniowej), kary umowne, określenie siły wyższej, zdarzeń objętych zakresem siły wyższej oraz zasad postępowania w takich sytuacjach, o ile ma to zastosowanie;
g) określenie zakresu odpowiedzialności za szkody wyrządzone klientom podmiotu nadzorowanego (o ile ma to zastosowanie), zgodnie z wymaganiami prawa obowiązującego podmiot nadzorowany;
h) klarowne wskazanie poddostawców (nazwa, lokalizacja, zakres czynności) dostawcy usług chmury obliczeniowej oraz warunków nadawania praw dostępu do informacji przetwarzanych przez podmiot nadzorowany;
i) klarowne wskazanie zasad, zgodnie z którymi zadania, zakresy uprawnień i odpowiedzialności oraz rozliczalność działań poddostawców dostawcy usług chmury obliczeniowej są transparentne i jasno identyfikowane przez podmiot nadzorowany;
j) źródła autoryzowanych informacji o planowanych zmianach w standardach świadczonych usług chmury obliczeniowej (w tym zmianach o charakterze technicznym);
k) źródła dokumentacji technicznej i deklaracji zgodności (w tym zgodności z obowiązującymi przepisami prawa), wraz z instrukcjami dotyczącymi konfiguracji usług chmury obliczeniowej;
l) zakres dodatkowych informacji i dokumentacji przekazywanych przez dostawcę usług chmury obliczeniowej w związku ze świadczeniem usług chmury obliczeniowej;
m) prawo podmiotu nadzorowanego do przeprowadzenia inspekcji w lokalizacjach przetwarzania informacji, w tym prawo do przeprowadzenia audytu drugiej lub trzeciej strony na zlecenie podmiotu nadzorowanego (o ile taka potrzeba wynika z szacowania ryzyka);
n) prawo dla nadzoru 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;
o) zasady licencjonowania (w tym prawo do aktualizacji bezpieczeństwa używanego oprogramowania lub jego komponentów) oraz prawa własności intelektualnej, w tym – jeżeli dotyczą – prawo do dysponowania przetwarzanymi informacjami;
p) zasady zmiany treści umowy, w tym parametrów technicznych używanych usług chmury obliczeniowej;
q) zasady rozwiązywania umowy, w tym zasady i terminy zwrotu lub usunięcia przetwarzanych informacji;
r) zasady wsparcia, w tym zakres i okna czasowe (z uwzględnieniem stref czasowych), tryb i sposób zgłaszania problemów z usługami chmury obliczeniowej;
s) zasady wymiany informacji, w tym w szczególności w zakresie bezpieczeństwa oraz zarządzania bieżącymi incydentami, obejmujące zarówno pracowników podmiotu nadzorowanego, jak i dostawcę usług chmury obliczeniowej, a w przypadku istotnego narażenia na skutki danego incydentu – również inne strony (np. klientów, poddostawców), w celu zapewnienia adekwatności postępowania do poziomu istotności incydentu.

Na potrzeby niniejszego rozdziału dot. umowy z dostawcą usług chmurowych będziemy odnosić się do sytuacji, w której zastosowanie mają zarówno RODO i prawo bankowe, jak również komunikat chmurowy.

Jak negocjować z większym od siebie?

Dostawcy usług chmurowych dla banków to w zdecydowanej większości znane i renomowane, globalne firmy IT, działające pod wieloma jurysdykcjami i mającym lokalne siedziby niemal w każdym państwie na świecie. Co za tym idzie stosują one zunifikowane i wystandaryzowane wzorce umowne (w tym poprzez odwołania do zbiorów dokumentów dostępnych wyłącznie elektronicznie) dotyczące oferowanych przez siebie usług. Firmy te, mimo że niechętne zmianom swoich standardów, są jednak przy okazji coraz bardziej świadome uwarunkowań lokalnych systemów prawnych i wynikających z nich konsekwencji. Dlatego też udostępniają dla swoich klientów dedykowane procesy, służące dostosowywaniu usług do wymagań lokalnych. Mimo, że procesy te nieco różnią się swoim charakterem i przebiegiem od przyjętych sposobów zmiany umowy, to jednak ich rezultatem jest przyjęcie wiążących dostawcę zmian i zastrzeżeń kontraktowych zapewniających bankowi zgodność obowiązującymi go regulacjami prawnymi.

Warto dlatego już na początku procesu z danym dostawcą chmury zastrzec, że dokumentacja chmurowa dostarczona przez dostawcę podlegać będzie weryfikacji działów bezpieczeństwa, compliance i prawnego, w tym danych osobowych (jak również zewnętrznych doradców banku) tak, aby dostawca poinformował swoje odpowiednie jednostki, często rozproszone po świecie, o możliwym rozpoczęciu w krótkim czasie procedury zmian do dokumentacji.

Poniżej opisaliśmy wybrane zagadnienia dotyczące właśnie wymogów zgodności dokumentacji chmurowej (umowy na usługę chmurową) z regulacjami obowiązującymi banki.

Najlepsze prawo? Prawo państwa członkowskiego UE

Umowy z globalnymi dostawcami usług chmurowych rzadko rządzone są prawem polskim, a próby poddania jej prawu polskiemu zazwyczaj kończą się fiaskiem. Dlatego bardzo ważne jest, że w przypadku, gdy dostawca nie może zgodzić się na poddanie umowy prawu polskiemu umowa podlegała prawu państwa jednego z państw członkowskich UE.

Zgodnie z komunikatem chmurowym, w przypadku poddania umowy prawu państwa trzeciego (rozumianego jako jurysdykcja inna niż państwa członkowskiego UE)bank powinien posiadać pisemną opinię prawną potwierdzającą, że zgodnie z wybranym prawem właściwym umowy wszystkie postanowienia umowy pomiędzy podmiotem nadzorowanym a dostawcą usług chmury obliczeniowej spełniają wymagania prawa obowiązujące podmiot nadzorowany oraz wymagania komunikatu chmurowego; wydanie opinii prawnej będzie zatem procesem raczej kosztownym, wydłużającym i tak niełatwy proces adaptacji chmury w banku.

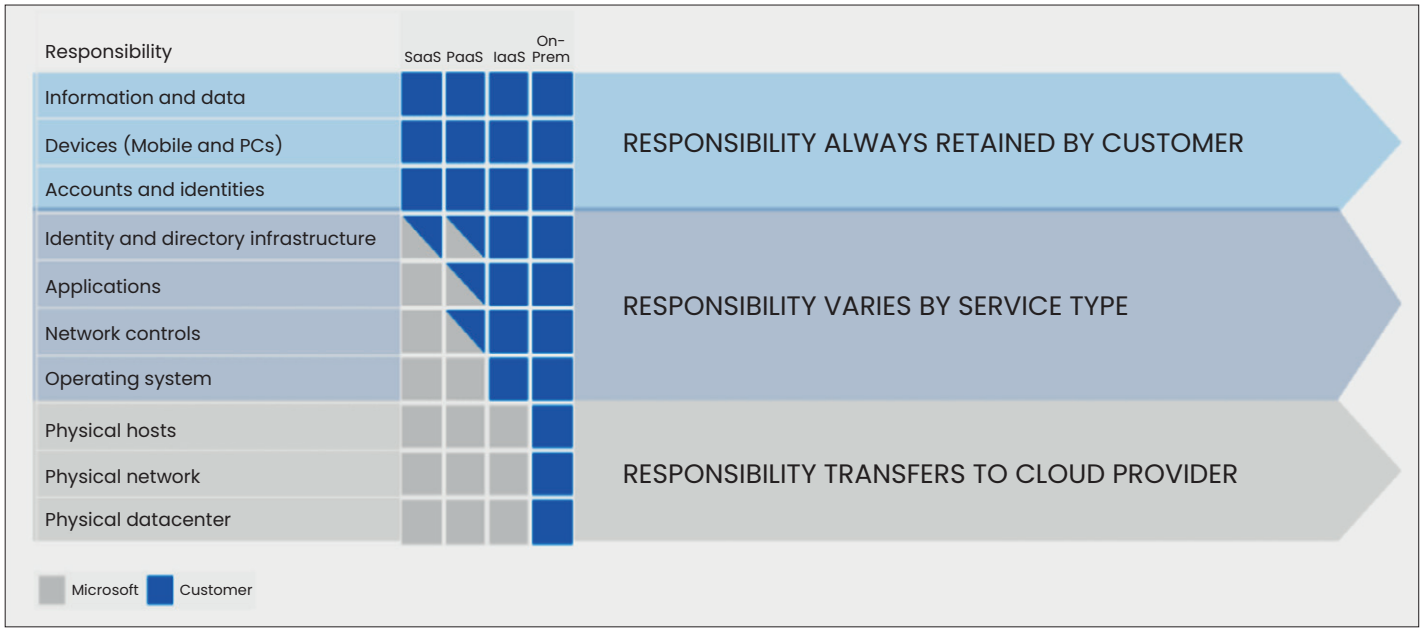
Należy jednak pamiętać, że poddanie umowy z dostawcą usług chmurowych prawu państwa członkowskiego UE (innemu niż prawo polskie)było poprzedzone stosowną analizą w zakresie zgodności formalnoprawnej przez odpowiednie komórki organizacyjne banku oraz ujęte w procesie szacowania ryzyka. Może się bowiem na przykład okazać, że bank nie posiada wystarczających kompetencji wewnętrznych, aby ocenić skutki poddania umowy temu prawu (np. w sytuacji nieprowadzenia działalności w danym kraju). Choć brak jest formalnego obowiązku uzyskania opinii prawnej, iż zawarta umowa spełnia wymagania prawa obowiązujące bank w przypadku wyboru prawa właściwego państwa członkowskiego UE oraz spełnienia przez wszystkie postanowienia umowy wymagań komunikatu[39], to zasięgnięcie takiej opinii z całą pewnością będzie jednym ze sposobów mitygacji zidentyfikowanych w tym zakresie ryzyk.

Podział odpowiedzialności za bezpieczeństwo przetwarzanych danych

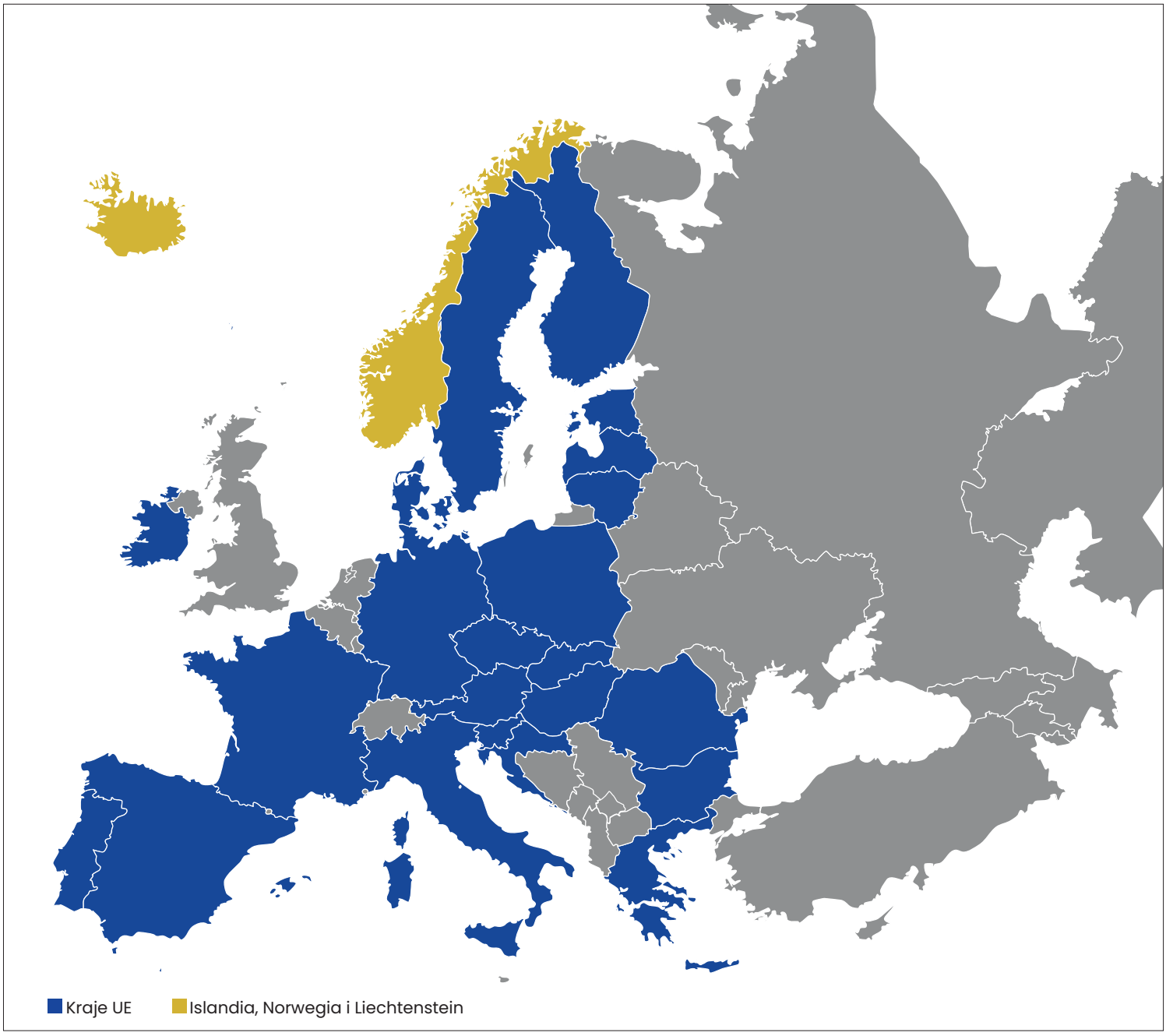
Umowa z dostawcą usług chmurowych powinna w sposób klarowny regulować odpowiedzialność za bezpieczeństwo danych przetwarzanych w chmurze. Model odpowiedzialności współdzielonej (*shared responsibility model*) w usługach chmurowych w każdym przypadku zakładał będzie odpowiedzialność dostawcy za bezpieczeństwo fizycznej infrastruktury (hardware). Jednakże, w zależności od rodzaju świadczonych usług, granica odpowiedzialności za poszczególne warstwy stosu technologicznego będzie kształtowana inaczej.

39 Zob. 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 30.11.2021).

Shared responsibility model



Europejski Obszar Gospodarczy



W przypadku usług świadczonych w modelu SaaS odpowiedzialność dostawcy będzie stosunkowo najszersza. Po stronie banku znajdować się będą bowiem właściwie jedynie takie obszary jak bezpieczeństwo informacji i danych, bezpieczeństwo urządzeń końcowych oraz zarządzanie dostępami i identyfikacja użytkowników. Odpowiedzialność za aplikacje, system operacyjny, sieć, konfigurację firewalli, a także szyfrowanie i zarządzanie kluczami szyfrującymi może spoczywać albo na banku, albo na dostawcy usług chmurowych – w zależności od tego, czy usługa będzie świadczona w modelu PaaS czy IaaS oraz od sposobu konfiguracji usługi w konkretnym przypadku[40].

Przykładowo model odpowiedzialności w usługach chmurowych świadczonych przez Microsoft wygląda następująco[41]:

Komunikat chmurowy nie precyzuje, gdzie dokładnie powinna przebiegać granica odpowiedzialności za bezpieczeństwo prze-

40 Zob. AWS Shared Responsibility Model (https://aws.amazon.com/compliance/shared-responsibility-model/, dostęp 30.11.2021).

41 Shared responsibility in the cloud (https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility, dostęp 30.11.2021).

twarzanych informacji w odniesieniu do poszczególnych usług chmurowych (z pewnymi wyjątkami np. w zakresie zarządzania kluczami szyfrującymi) i jest to podejście słuszne. Ocena w tym zakresie każdorazowo należy bowiem do banku i powinna uwzględniać wyniki szacowania ryzyka w kontekście konkretnej usługi chmury obliczeniowej oraz klasyfikacji i oceny informacji przekazanych do przetwarzania w chmurze. Z punktu widzenia umowy z dostawcą istotne jednak jest klarowne ustalenie obszarów, za których bezpieczeństwo odpowiadać będzie dostawca, a także tych w których odpowiedzialność spoczywać będzie na banku.

Lokalizacja przetwarzania danych

Lokalizacja Centrum Przetwarzania Danych, a zatem miejsca, gdzie dane przekazane w ramach usługi outsourcingowej będą przetwarzane, jest z punktu regulacji prawnych niezwykle istotnym zagadnieniem, wymagającym precyzyjnego uregulowania w umowie dotyczącej usługi chmurowej dla banku. Biorąc pod uwagę całokształt regulacji należy rekomendować co następuje:

1) Centrum Przetwarzania Danych powinno znajdować się na terytorium EOG (w tym zakresie także RODO wymaga podjęcia dodatkowych środków ochrony, gdy lokalizacja przetwarzania znajduje się poza EOG); ważne jest przy tym, że bez uprzedniej pisemnej zgody banku dostawca ani żaden z jego poddostawców nie może mieć prawa do przeniesienia danych banku poza ustalone w umowie CPD (również w sytuacjach awaryjnych);
2) lokalizacja Centrum Przetwarzania Danych powinna być właściwie określona, przy czym nie jest wymagane (a nawet ze względów bezpieczeństwa nie jest to rekomendowane) wskazanie dokładnego adresu CPD; wystarczające jest określenie regionu, czemu zadość czyni np. wskazanie miasta czy samorządowej (lokalnej) jednostki administracyjnej danego państwa[42].

Rekomendowane jest, aby umowa chmurowa w sposób jednoznaczny:

1) zawsze zachowywała zgodność z RODO;
2) wskazywała, że dane będą przetwarzane wyłącznie na obszarze EOG;
3) określała lokalizacje Centrum Przetwarzania Danych (CPD) w którym znajdują się dane przekazane przez bank w ramach usługi chmurowej; oraz
4) zawierała bezwzględny zakaz transferu danych poza EOG bez uprzedniej pisemnej pod zgody banku.

Bank każdorazowo powinien posiadać wiedzę odnośnie do lokalizacji przetwarzanych w chmurze danych, a także możliwość wykazania, że historycznie dane były przetwarzane wyłącznie w określonych lokalizacjach. Zapewnienie powyższego spowoduje, że bank zachowa pełną zgodność z wymogami wiążących go regulacji w zakresie lokalizacji przetwarzania danych.

Podoutsourcing

Poziom złożoności usług chmurowych sprawia, że niemal wszyscy dostawcy usług chmurowych przy świadczeniu takich usług korzystają z poddostawców. Tak długo jak poddostawca nie przetwarza danych objętych tajemnicą bankową od dostawcy usług chmurowych lub nie wykonuje czynności w ramach outsourcingu szczególnego chmury obliczeniowej zagadnienie to pozostaje w zasadzie irrelewantne z punktu widzenia banku. Jednakże, gdy choćby jedna ze wspominanych w poprzednim zdaniu okoliczności wystąpi, wówczas sytuacja znacznie się komplikuje. W stosunku do poddostawców w takim przypadku zaczynają bowiem obowiązywać bezwzględnie obowiązujące przepisy prawa bankowego. W obecnym stanie prawnym (uwzględniając także przyjętą linię interpretacji podzielaną także przez nadzór) zabraniają one stosowania tzw. outsourcingu łańcuchowego, a zatem takiego powierzenia czynności objętych usługą, które w relacji wertykalnej angażowałoby poddostawcę dalszego niż bezpośredni poddostawca dostawcy chmurowego. Innymi słowy poddostawcy, którym dostawca świadczący usługę dla banku zleca realizację określonych czynności w celu świadczenia usług dla banku, nie mogą korzystać w tym celu ze swoich poddostawców (brak prawa dalszego powierzania czynności outsourcingowych). Możliwe jest więc jedynie jednokrotnie powierzenie dalej określonych czynności.

Biorąc pod uwagę powyższe, umowa o świadczenie usług chmurowych powinna przewidywać w szczególności, że:

42 Komunikat chmurowy mówi wprost, że precyzyjne wskazanie lokalizacji centrum przetwarzania danych (CPD) może rodzić zagrożenie dla bezpieczeństwa fizycznego przetwarzanych informacji, jednak 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. W sytuacji, gdy takie określenie nie jest możliwe lub – z uwagi na skalę działania i liczbę miejsc przetwarzania informacji – jest niezasadne, należy podać obszar EOG (dla Europejskiego Obszaru Gospodarczego) lub inne równoważne określenie.

1) dostawca usług chmurowych może dokonać dalszego zlecenia wykonania usługi chmurowej wyłącznie za uprzednią pisemna zgodą banku, a gdyby na takie dalsze zlecenie bank wyraził zgodę już w samej umowie, to zgoda powinna być udzielona względem wyłącznie określonych sprecyzowanych w umowie podmiotów oraz umowa powinna przewidywać klarowne zmiany zasad tych podmiotów oraz prawo do wypowiedzenia umowy; zgoda nigdy nie powinna być całkowicie zgodą „in blanco", gdyż groziłoby to ryzykiem, że usługa może być podzlecana poza wiedzą i kontrolą banku;
2) dostawca zapewni, że poddostawca nie dokona dalszego zlecenia wykonywanej na rzecz dostawcy usługi, a jeśli taki poddostawca poddostawcy dostawcy jest niezbędny do prawidłowego świadczenia usługi chmurowej (bez uszczerbku dla rekomendacji w punkcie 1. powyżej) to dostawca zawrze z nim bezpośrednią umowę tak aby skrócić „łańcuch outsourcingowy"; oraz
3) za złamanie powyższych zobowiązań dostawcy grozić będzie wysoka odpowiedzialność odszkodowawcza względem banku (z uwzględnieniem art. 6b prawa bankowego) oraz uprawnienie banku do natychmiastowego zakończenia współpracy z dostawcą.

W tym miejscu wypada także wspomnieć o jeszcze jednym istotnym zagadaniu poruszonym przez komunikat chmurowy, a mianowicie o sytuacji, w której dostawca banku niebędący dostawcą chmurowym korzysta z usług dostawcy chmurowego, który przetwarza dane banku lub wykonuje procesy, które, jeśli wykonywane byłyby na rzecz banku, spowodowałyby konieczność stosowania komunikatu chmurowego lub prawa bankowego. Tu niestety KNF nie ułatwia życia bankom i stwierdza, że podmiot nadzorowany za każdym razem powinien badać czy taka sytuacja nie zachodzi w jego relacjach z dostawcami.

Dalsze powierzenie czynności outsourcowanych, w przypadkach, w których obejmować będzie również przetwarzanie danych osobowych, powinno też znaleźć odzwierciedlenie w zawieranych przez bank i dostawców umowach powierzenia przetwarzania danych osobowych i zapewniać zgodność z przepisami RODO.

> *W zależności od wyników szacowania ryzyka przeprowadzonego przez bank umowa na usługę chmurową powinna zapewnić także możliwość przeprowadzenia przez bank inspekcji w lokalizacjach przetwarzania informacji (Centrach Przetwarzania Danych), w tym prawo do audytu drugiej lub trzeciej strony na jego zlecenie.*

Uprawnienia kontrolne banku i nadzoru (audyt)

Umowa dotycząca usługi chmurowej dla banku powinna bezwzględnie zapewniać prawo dla KNF do wykonania obowiązków kontrolnych, w tym kontroli pomieszczeń i dokumentacji związanej z przetwarzaniem informacji banku w ramach usługi chmurowej oraz związanych z nią procesów i procedur, organizacji i zarządzania oraz potwierdzeń zgodności.

W zależności od wyników szacowania ryzyka przeprowadzonego przez bank umowa na usługę chmurową powinna zapewnić także możliwość przeprowadzenia przez bank inspekcji w lokalizacjach przetwarzania informacji (Centrach Przetwarzania Danych), w tym prawo do przeprowadzenia audytu drugiej lub trzeciej strony na zlecenie banku.

W praktyce wyniki szacowania ryzyka w większości przypadków nakazują uwzględnienie tzw. prawa audytu banku w CPD dostawcy chmury, a dostawcy chmurowi świadomi tego, zwykle umożliwiają wykonanie takiego uprawnienia. Z uwagi jednak na fakt, że uprawnienie to ma (przynajmniej w teorii) charakter fakultatywny wiąże się ono bardzo często z dodatkowymi kosztami i koniecznością uiszczenia opłat na rzecz dostawcy usługi chmurowej. Mogą one być większe niż praktyczna wartość dodana z dokonania fizycznej inspekcji lokalizacji przetwarzania. Niezależnie od sposobu zakontraktowania takiego uprawnienia bank powinien jednak upewnić się, że jego prawo audytu jest możliwe do wykonania w każdym czasie trwania umowy.

Ciągłość działania, rozwiązanie umowy i exit plan

Plan ciągłości działania (*business continuity plan*, BCP) jest konstytutywnym elementem dokumentacji opracowanej przez bank na potrzeby wdrożenia chmurowego. Odpowiedni plan ciągłości działania powinien być także elementem dokumentacji dostawcy usług chmurowych, którego to posiadanie dostawca powinien zagwarantować w umowie chmurowej. Jego treść wpływa bowiem także na treść planu ciągłości działania samego banku oraz dodatkowo exit planu, tj. dokumentu określającego sposoby wycofania przez bank swojego zaangażowania w przetwarzanie informacji w usługach chmury obliczeniowej danego dostawcy (również w sytuacji awaryjnej), bez uszczerbku dla zachowania zgodności swojego działania z wymaganiami prawa

Fot. Sikov/stock.adobe.com

i innych regulacji, w tym w szczególności związanych z udzielonymi licencjami lub zezwoleniami na prowadzenie określonej działalności.

Z istnieniem exit planu i planu ciągłości działania związane jest zapewnienie w umowie z dostawcą odpowiednio długiego okresu wypowiedzenia (biorąc pod uwagę, że umowy zawierane są zwykle na czas określony), który zagwarantuje bankowi czas na przeniesienie usługi chmurowej ze środowiska dostawcy lub bezpiecznego wycofania się z niej. Dodatkowo zaleca się, aby bank zapewnił sobie w umowie z dostawcą, że w przypadku przeniesienia usługi do nowego dostawcy (bez względu na powód) dostawca zobowiązany będzie współdziałać zarówno z bankiem jak i nowym dostawcą w procesie takiego przeniesienia.

Równie ważne jest także prawo banku do rozwiązania umowy ze skutkiem natychmiastowym. Prawo takie powinno być zastrzeżone dla przypadków naruszenia umowy przez dostawcę we wszystkich zagadnieniach opisanych powyżej. Uwzględnić należy z pewnością również przypadki, gdy KNF swoją decyzją skierowaną do banku nakazuje natychmiastowe rozwiązanie umowy dotyczącej chmury obliczeniowej (z powodów, o których mowa była w poprzednich rozdziałach), czy też wprowadzenia zmian w prawie czyniących wykonywanie usługi sprzecznym z prawem.

Zmiany umowy a zmiany dokumentacji technicznej

Procedura zmiany dokumentacji technicznej stanowiącej część umowy chmurowej powinna pozostawać pod kontrolą i wiedzą banku. Nie oznacza to jednak, że powszechna praktyka (na co zresztą zezwala treść komunikatu chmurowego), polegająca na zmianie (aktualizacji) dokumentacji technicznej bez sporządzania aneksu do umowy jest niedopuszczalna. Tak długo, jak zmiany te nie wpływają na stabilność i bezpieczeństwo usług świadczonych dla banku, taki sposób wykonywania umowy powinien być możliwy do stosowania.

Z punktu widzenia banku, dobrą praktyką jest wskazanie w umowie na obowiązek dostawcy usług informowania o zmianach i określenie terminu realizacji tego obowiązku (z jakim wyprzedzeniem bank powinien być informowany o planowanych zmianach). Odnosi się to w szczególności do zmian o charakterze technologicznym mogących mieć znaczący wpływ na bezpieczeństwo oraz sposób świadczenia usługi. Jeżeli natomiast zmiana dotyczyłaby kluczowych aspektów wykonywanej usługi może okazać się konieczne zawarcie aneksu do umowy lub nawet nowej umowy z dostawcą usług chmurowych – zmiana taka powinna bowiem być uzależniona od zgody banku. Wśród dobrych praktyk wymienić można również wyznaczenie osoby odpowie-

dzialnej za bieżący monitoring oraz współpracę z dostawcą usługi[43].

Gdy w ocenie banku zmiana wiąże się z dodatkowymi ryzykami, które nie będą możliwe do zaakceptowania, bank powinien mieć zagwarantowane prawo wypowiedzenia umowy z odpowiednim okresem wypowiedzenia.

NOTYFIKACJA WYKORZYSTANIA ROZWIĄZAŃ CHMUROWYCH

Po sporządzeniu i zebraniu kompletu dokumentacji projektowej, ostatnim etapem wymaganym przez komunikat w przypadku transformacji banku do chmury jest obowiązek poinformowania UKNF o zamiarze przetwarzania informacji w chmurze obliczeniowej, o ile usługi chmury obliczeniowej stanowią outsourcing szczególny lub w chmurze obliczeniowej przetwarzane są informacje prawnie chronione (objęte tajemnicą bankową).

Również podpisanie umowy w ramach chmury społecznościowej publicznej, np. przez podmiot zrzeszający lub w ramach grupy kapitałowej przez podmiot dominujący, nie zwalnia poszczególnych podmiotów nadzorowanych uczestniczących w zrzeszeniu lub grupie kapitałowej z obowiązku notyfikowania przetwarzania w chmurze. W przypadku współpracy podmiotu nadzorowanego z innym podmiotem nadzorowanym (np. banku z zakładem ubezpieczeń w zakresie bancassurance), podmiot ten nie ma jednak obowiązku dokonywania oddzielnych notyfikacji uwzględniających korzystanie z chmury przez podmiot nadzorowany, któremu powierzono przetwarzanie, jeżeli korzystanie z chmury jest jego autonomiczną decyzją. Jeżeli natomiast, podmiot nadzorowany korzysta z usługi chmurowej dostarczonej przez inny podmiot nadzorowany (np. usługi chmurowe dystrybuowane przez spółkę matkę w ramach grupy kapitałowej), to nawet jeśli wykorzystuje ją do wykonywania czynności na rzecz tego podmiotu, obydwa podmioty dokonują oddzielnych notyfikacji[44]. Ilekroć bank będzie planował wykorzystanie usług chmury obliczeniowej z własnej inicjatywy zobowiązany będzie do dokonania notyfikacji takiego planowanego przetwarzania do organu nadzoru.

Warto przy tym podkreślić, że brak jest obowiązku informowania Nadzoru o zaprzestaniu zgłoszonego wcześniej przetwarzania lub zamiaru przetwarzania informacji w chmurze. Także sama zmiana funkcjonalności usługi chmurowej nie skutkuje powstaniem obowiązku notyfikacyjnego, w szczególności brak jest wymogu informowania o zmianie lokalizacji CPD. KNF wskazuje jednak, że taka informacja byłaby przydatna ze względów nadzorczych[45].

Bank jest zobowiązany do notyfikacji rodzaju i zakresu informacji planowanych do przetwarzania w chmurze obliczeniowej jedynie w przypadkach outsourcingu szczególnego chmury obliczeniowej lub przetwarzania informacji prawnie chronionej. Jeżeli jednak doszłoby do istotnej zmiany rodzaju lub zakresu informacji przetwarzanych w chmurze, a więc do zmiany, która prowadziłaby do rozszerzenia zakresu informacji przetwarzanych w chmurze o nowe kategorie informacji prawnie chronionych lub która powodowałaby kwalifikację outsourcingu jako outsourcingu szczególnego chmury obliczeniowej, to zmiana taka będzie skutkować obowiązkiem dokonania ponownej notyfikacji zgodnie ze wzorem stanowiącym załącznik do komunikatu[46]. W celu zachowania spójności komunikacji z Nadzorem można odwołać się do poprzedniego zgłoszenia, jednakże z formalnego punktu widzenia będą to dwie odrębne notyfikacje.

Zgłoszenia należy dokonać co najmniej 14 dni przed rozpoczęciem przetwarzania informacji używając w tym celu Załącznika 1 do komunikatu chmurowego. Uprawnionym do podpisania informacji, o której mowa w pkt VIII komunikatu jest zarówno zarząd banku (zgodnie z reprezentacją w KRS), jak i osoby właściwie przez zarząd umocowane. Decyzja może mieć formę uchwały zarządu.

43 Zob. 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 30.11.2021).

44 Tamże

45 Tamże

46 Tamże.

Przekonaj się, że warto wiedzieć więcej

„Miesięcznik Finansowy BANK"

Jesteśmy profesjonalnym magazynem środowiska bankowego. Od 30 lat omawiamy zasadnicze problemy rynku finansowego w Polsce. Pomagamy w unowocześnieniu sektora i kształceniu kadr. Współpracujemy z bankami, firmami infrastrukturalnymi i organizacjami środowiskowymi. Organizujemy szereg profesjonalnych konferencji, szkoleń i debat od lat wytyczających rynkowe standardy.

BANK
MIESIĘCZNIK FINANSOWY

www.aleBank.pl/BANK

REDAKCJA	redakcja@miesiecznikBank.pl	DZIAŁ REKLAMY	reklama@wydawnictwocpb.pl
PRENUMERATA	www.alebank.pl/prenumerata	KONFERENCJE I SZKOLENIA	www.alebank.pl/konferencje

Fot. blackboard/stock.adobe.com

Chmura? Tak, ale jaka?

W dzisiejszych czasach coraz częściej mamy do czynienia z pojęciem chmury. Jest to narzędzie, które ma ułatwić życie nie tylko zespołom, które tworzą oprogramowanie, ale również jego docelowym odbiorcom, czyli bankom, faktorom, czy instytucjom finansowym. Jednak przed podjęciem decyzji o przejściu na model chmurowy trzeba zapoznać się z kilkoma związanymi z nim pojęciami oraz zaletami i wadami rozwiązań chmurowych w porównaniu z tradycyjnym modelem on-premises.

Karol Leszczyński
PRODUCT MANAGER
COMARCH SA

Wyróżniamy trzy modele świadczenia usług chmurowych: SaaS (Software-as-a-Service), IaaS (Infrastructure-as-a-Service) oraz PaaS (Platform-as-a-Service). Każdy z wyżej wymienionych modeli pozwala na duże oszczędności w zakresie infrastruktury IT. Jednak, aby zdecydować który model będzie odpowiedni, trzeba dokładnie określić oczekiwania biznesowe. Przed podjęciem decyzji warto przeanalizować kilka czynników:

a) koszty,
b) bezpieczeństwo,
c) czas wdrożenia oprogramowania,
d) utrzymanie infrastruktury,
e) dostęp do oprogramowania.

Modele i ich zalety

Software-as-a-Service zapewnia najbardziej kompleksowy zakres usług. W tym modelu dostawca oprogramowania dostarcza całą niezbędną infrastrukturę IT, która często bywa najbardziej kosztowną częścią inwestycji. Dodatkowo dostarczana jest aplikacja. Cała odpowiedzialność za działanie systemu spoczywa na dostawcy. Klient nie martwi się o działanie aplikacji, sprzęt taki, jak serwery, czy platformy operacyjne. Dodatkowo, w tym rozwiązaniu klient może liczyć na wsparcie dostawcy w zakresie testów aplikacji, nie musi myśleć o wykupie niezbędnych licencji, które także są bardzo kosztowne, czy o monitoringu.

Najważniejsze zalety modelu Software-as-a-Service to:
a) infrastruktura w postaci serwerów,
b) szybkie wdrożenie oprogramowania,
c) bezpieczeństwo po stronie dostawcy oprogramowania,
d) jasno ustalone parametry SLA (Service Level Agreement).

Nieco inny zakres usług zapewnia model **PaaS (Platform-as--a-Service)**, w którym dostawca dostarcza pełną infrastrukturę sprzętowo-systemową do obsługi aplikacji klienta. Dzięki temu rozwiązaniu klient uruchamia aplikację w bardzo krótkim czasie, a także ma realny wpływ na jej rozwój oraz testowanie. Dostawca oprogramowania zapewnia wszystkie niezbędne licencje, a także administrację i zarządzanie warstwą operacyjną (np. system operacyjny, baza danych). Główna różnica pomiędzy modelami PaaS i SaaS polega na tym, że w modelu PaaS twórca aplikacji zajmuje się jej właściwym przygotowaniem do pracy i dostosowaniem do potrzeb użytkowników. Ten model usługowy eliminuje wysokie koszty początkowe, co jest szczególnie istotne na wczesnym etapie projektu.

Zalety modelu Platform-as-a-Service:
a) ograniczenie nakładów na uruchomienie infrastruktury IT,
b) jasno ustalone parametry SLA (Service Level Agreement),
c) monitoring po stronie dostawcy,
d) zaawansowana infrastruktura IT dostępna nawet dla małych projektów.

Infrastructure-as-a-Service to model, który polega na wynajęciu infrastruktury informatycznej. Dostawca udostępnia swojemu klientowi wymaganą liczbę serwerów, ilość mocy obliczeniowej, czy niezbędną przestrzeń dyskową. Wybór modelu IaaS zapewnia możliwość elastycznego i skalowalnego doboru elementów infrastruktury IT. Model ten cechuje elastyczność w przypadku nagłych zmian potrzeb biznesowych. Główna jego zaleta to brak konieczności inwestycji środków na wymagania związane z budową lub adaptacją serwerowni do nowych potrzeb firmy. Jednak całe zarządzanie infrastrukturą leży już po stronie zespołu IT klienta. Dostawca musi zapewnić niezawodność infrastruktury.

Zalety Infrastructure-as-a-Service:
a) ograniczenie nakładów na uruchomienie infrastruktury IT,
b) elastyczność w zakresie dostosowania potrzebnych zasobów,
c) jasno ustalone parametry SLA,
d) możliwość dowolnego wykorzystania udostępnianych zasobów.

Do niedawna najbardziej popularnym rozwiązaniem był tradycyjny model on-premises. Tu oprogramowanie jest instalowane na infrastrukturze klienta, która jest jego wyłączną własnością. Klient musi także zadbać o utrzymanie całego niezbędnego sprzętu. Licencje są zazwyczaj rozliczane poprzez jednorazową opłatę, która jednak stanowi znaczny koszt oprogramowania. Co więcej, model on-premises wymaga także dużego wydatku na początku, ale ze względu na jednorazową opłatę licencyjną całkowity koszt rozwiązania może być niższy niż w przypadku SaaS. Należy przy tym pamiętać o kwestii utrzymania systemu, a co za tym idzie zatrudnienia i opłacenia odpowiednich specjalistów. Dodatkowo, dla niektórych instytucji warunkiem koniecznym jest pełna kontrola nad danymi oraz bezpieczeństwem – co dyskwalifikuje rozwiązania Software-as-a-Service. Jeśli chcemy porównać czas implementacji, to tu dużą przewagę wykazuje model SaaS. Ale już przy dostosowywaniu oprogramowania do potrzeb klienta, SaaS zostaje w tyle za on-premises. Ten ostatni model można w dużym stopniu dopasowywać do konkretnych wymagań, choć ta opcja pociąga za sobą dodatkowe koszty.

Zalety i wady mikroserwisów

Ważną częścią architektury chmurowej są mikroserwisy. Ich największą zaletą jest to, że obejmują tylko jeden obszar biznesu, czyli dzielą monolityczną aplikację na mniejsze usługi, które ze sobą współpracują. Można powiedzieć, że każdy mikroserwis jest „osobną" mini-aplikacją, na którą składa się architektura czy logika biznesowa. W porównaniu z podejściem monolitycznym, mikrousługi cechuje wiele zalet:
a) pozwalają na szybsze i częstsze wdrożenia nowych wersji,
b) poprawiają stabilność systemu,
c) zmniejszają ryzyko wstrzymania pracy systemu z powodu błędu w innym obszarze,
d) ułatwiają zarządzanie zespołem odpowiedzialnym za dany mikroserwis.

Zaletami mikroserwisów jest również to, że:
a) rozwiązują problem złożoności systemu, aplikacja podzielona jest na wiele elementów, łatwiejszych w zarządzaniu, szybszych w opracowaniu i łatwiejszych w utrzymaniu,
b) umożliwiają rozwój wybranej usługi przez osobny zespół, który dzięki temu może koncentrować się tylko na tej usłudze,

> ”
>
> ***Software-as-a-Service zapewnia najbardziej kompleksowy zakres usług. Dostawca oprogramowania dostarcza całą niezbędną infrastrukturę IT, która często bywa najbardziej kosztowną częścią inwestycji. Dodatkowo dostarczana jest aplikacja. Cała odpowiedzialność za działanie systemu spoczywa na dostawcy.***

c) pozwalają na swobodne dopasowanie technologii,
d) ułatwiają skalowanie każdej usługi.

Jednak architektura ta nie jest wolna od wad. Przede wszystkim jest to architektura bardziej złożona, bo obejmuje systemy rozproszone. Dodatkowo należy zwrócić uwagę na kilka kwestii:

a) Architektura partycjonowanej bazy danych – w aplikacjach opartych na mikroserwisach transakcje biznesowe niekiedy aktualizują wiele zbiorów danych, należących do różnych usług i znajdujących się w wielu różnych bazach danych. Korzystanie z transakcji rozproszonych zwykle nie wchodzi w rachubę i ostatecznie musimy zapewnić spójność programowo, co jest oczywiście trudniejsze dla programistów.

> ***Pay-as-you-grow – model, który bardzo często jest stosowany w przypadku rozwiązań chmurowych, wydaje się ciekawym rozwiązaniem. Jego główną zaletą jest to, że pozwala na początku działalności zaoszczędzić duże nakłady środków na infrastrukturę. W tym modelu klient płaci za faktycznie zużyte zasoby.***

b) Testowanie aplikacji opartych na mikroserwisach jest dużo bardziej złożone niż testy monolitycznej aplikacji webowej.
c) Trudniej jest wprowadzić zmiany obejmujące wiele usług. W monolitycznej aplikacji możemy po prostu zmienić odpowiednie moduły, zintegrować zmiany i wdrożyć je za jednym razem. W architekturze mikrousługowej dokładnie planujemy i koordynujemy wdrażanie zmian w każdej z usług.
d) Wdrażanie aplikacji jest bardziej złożone. Monolityczna aplikacja jest po prostu wdrażana z wykorzystaniem zestawu maszyn wirtualnych. Natomiast aplikacja oparta na mikrousługach zazwyczaj składa się z wielu usług, a każda ma wiele instancji środowiska wykonawczego. Z kolei każda instancja musi być skonfigurowana, wdrożona, skalowana i monitorowana. Musimy także zapewnić mechanizm wykrywania usług. Ten poziom złożoności wymaga już dużej automatyzacji.

Migracja systemu monolitycznego do mikroserwisów

Przejście na mikrousługi z systemu, który jest monolitem, może zająć od kilkunastu miesięcy do kilku lat. Dobrym rozwiązaniem wydaje się droga pośrednia, gdzie migrujemy i ograniczamy monolit przez wydzielanie z niego kolejnych mikroserwisów. Na kilka rzeczy powinniśmy zwrócić uwagę na samym początku:

a) Właściciel mikroserwisu – na początku powinniśmy zadbać, aby każdy mikroserwis miał zdefiniowanego właściciela. Takie podejście po pierwsze przypisuje odpowiedzialność za wybraną usługę, ale także nadaje mu pewien obszar swobody. Dzięki takim ustaleniom jesteśmy w stanie znacznie skrócić czas zgłaszania nowych funkcji lub awarii.
b) Monitoring i dokumentacja – ważnym aspektem jest monitorowanie jakości pracy mikroserwisów. Dzięki niemu zapobiegniemy awariom. Dodatkowo warto zadbać o dziennik zmian. Takie podejście ułatwi śledzenie nowych funkcji oraz poprawianie błędów.
c) Niezależność mikroserwisów – przy projektowaniu zmiany przejścia z monolitu na mikroserwisy powinniśmy z wyprzedzeniem identyfikować zależności, aby jak najlepiej zaplanować ciągły rozwój systemu. Poszczególne mikroserwisy powinny być jak najbardziej niezależne. Dzięki temu zyskamy wysoką dostępność naszego rozwiązania.
d) Standaryzacja – warto wykorzystać standardowe sposoby, by ujednolicić komunikację w systemie i poza nim. To ułatwi rozwój całego systemu.
e) Gotowe frameworki – stosowanie gotowych frameworków do tworzenia mikroserwisów pozwala na skrócenie czasu dostosowania się do standardów. Można także opracować własne szkielety, jednak to rozwiązanie wymaga większego nakładu czasu i pracy.

Skalowalność

Skalowalność może być zdefiniowana jako „łatwość" z jaką system lub komponent można zmodyfikować, aby rozwiązać problem wydajności w danym obszarze.

Skalowalny system ma trzy proste cechy:

a) jest gotowy do obsługi dynamicznie zwiększającej się liczby użytkowników,
b) może pomieścić zwiększony zestaw danych,
c) jest wydajny i dostosowuje moce obliczeniowe do aktualnego obciążenia.

Innymi słowy, skalowalność odnosi się do zdolności systemu do pracy w warunkach rosnących potrzeb (rosnący ruch lub zwiększona ilość danych). Skalowalność przekłada się także na zyski biznesowe, takie jak zmniejszenie strat finansowych spowodowanych przestojami systemu czy wzrost zaufania klientów. Skalowalność jest jednym z najcenniejszych atrybutów jakości systemu.

Fot. peshkov/stock.adobe.com

Kolejne ważne pytanie, które pojawia się w kontekście pracy systemu to: „Jak skalować?". Rozróżniamy dwa rodzaje skalowania:

SKALOWANIE WERTYKALNE (SKALOWANIE W PIONIE LUB SKALOWANIE W GÓRĘ)

Ten rodzaj skalowania odnosi się do maksymalizacji zasobów pojedynczej jednostki w celu rozwinięcia jego zdolności do obsługi rosnącego obciążenia. Pod względem sprzętowym obejmuje to np. zwiększenie pamięci na komputerze fizycznym z uruchomionym serwerem. Pod względem oprogramowania skalowanie w górę może obejmować optymalizację algorytmów i kodu aplikacji. Jednak ten rodzaj skalowania w pewnym momencie może zacząć stwarzać problemy. Zwiększanie pojemności infrastruktury przez dodawanie kolejnych elementów powoduje znaczny wzrost kosztów oraz pojawienie się problemów z odnalezieniem potrzebnych danych. Problemem mogą być także kwestie ustalenia dostępu i ochrony przechowywanych danych, zwłaszcza wtedy, gdy używamy wielu produktów z oddzielną bazą danych w każdym z nich. Nowoczesne podejście do ochrony danych i zarządzania nimi prowadzi nas do drugiego rodzaju skalowania.

SKALOWANIE HORYZONTALNE (SKALOWANIE W POZIOMIE)

Ten rodzaj skalowania odnosi się do przyrostu zasobów przez dodanie jednostek do systemu. Oznacza to dodanie większej liczby jednostek o mniejszej pojemności, zamiast jednej jednostki o większej pojemności. Żądania dotyczące zasobów są następnie rozłożone na wiele jednostek, zmniejszając w ten sposób nadmierne obciążenie jednej maszyny. Posiadanie wielu jednostek pozwala nam na łatwiejsze utrzymanie systemu, nawet jeśli jedna z jednostek ulegnie awarii, to zostanie zastąpiona poprzez inne. Całkowity koszt poniesiony przez wiele mniejszych jednostek jest mniejszy niż koszt pojedynczej większej jednostki.

Transparentność kosztowa

Pay-as-you-grow – model, który bardzo często jest stosowany w przypadku rozwiązań chmurowych, wydaje się ciekawym rozwiązaniem. Jego główną zaletą jest to, że pozwala na początku działalności zaoszczędzić duże nakłady środków na infrastrukturę. W tym modelu klient płaci za faktycznie zużyte zasoby (wykorzystanie chmury obliczeniowej). Co ciekawe, jeśli biznes będzie się rozwijał, klient zapłaci adekwatnie więcej. Jednak w przypadku słabszego okresu w rozwoju firmy koszty te także zostaną dostosowane.

Rodzaje chmur obliczeniowych

Chmura publiczna, chmura prywatna czy może chmura hybrydowa? Czym różnią się poszczególne rodzaje chmur obliczeniowych, na jaki typ się zdecydować, co wyróżnia poszczególne rozwiązania? Chmury obliczeniowe różnią się przede wszystkim fizyczną lokalizacją zasobów i tym, kto jest ich właścicielem. Nie należy mylić rodzajów chmury z rodzajami usług chmurowych.

CHMURA PUBLICZNA

Chmura publiczna jest rozwiązaniem, w którym usługodawca udostępnia klientom zasoby w zamian za odpowiednią opłatę. Jest ona „publiczna", ponieważ zasoby i usługi ze wspólnej puli mogą być wynajęte przez każdego chętnego i zastosowane zgodnie z własnymi wymaganiami.

Zalety:

a) Chmury publiczne wykorzystują model znany jako pay-as-you-grow. Oznacza to, że klient płaci za wykorzystane zasoby w danym miesiącu. Nie ma konieczności uiszczania opłat abonamentowych. Rozwiązanie to może się sprawdzić w przypadku dużych wahań koniunkturalnych, gdzie zapotrzebowanie na daną usługę może w niektórych miesiącach wzrastać, a w innych spadać.
b) Chmurę publiczną cechuje to, że wszyscy mają dostęp do takiego samego sprzętu i takich samych usług, nie ma tu znaczenia czy jest to osoba fizyczna, mała czy średnia firma, czy wielka korporacja.
c) Zaletą chmury publicznej jest także to, że jej zasoby mogą być dowolnie skalowane, rosnąc i zmniejszając się w miarę zapotrzebowania.
d) Najwięksi dostawcy chmury publicznej oferują bardzo szeroką ofertę różnych usług, od wirtualnych serwerów, systemów storage i sieci, aż po całe gotowe platformy programistyczne. Ułatwia to rozpoczęcie pracy w danym środowisku, nie trzeba poświęcać czasu na jego przygotowanie i dostosowanie.

Wady:

a) Zasoby wynajmowane przez poszczególnych użytkowników chmury publicznej są zazwyczaj odseparowane jedynie wirtualnie. Dlatego w niektórych przypadkach może to powodować obawy o bezpieczeństwo, stabilność i dostępność.
b) Chmura publiczna pozwala na duży zakres konfigurowalności, ale niektóre wymagania mogą okazać się trudne lub bardzo kosztowne do zrealizowania.

CHMURA PRYWATNA

Chmura prywatna to taka, której rozwiązania są dostarczane do wyłącznego użytku pojedynczej organizacji. Poza tym chmura prywatna tak samo, jak chmura publiczna, zapewnia skalowalność, automatyzację działań, czy dostarczanie zasobów na żądanie przez sieć.

Zalety:

a) Chmura prywatna zapewnia korzystającej z niej organizacji pełną kontrolę nad zasobami i usługami, dodatkowo dostosowana jest wyłącznie do wymogów pojedynczej firmy.
b) Bezpieczeństwo danych, stabilność i dostępność usług.

Wady:

a) Budowa chmury prywatnej jest procesem bardzo skomplikowanym a przez to niezwykle kosztownym.
b) Zwiększanie zasobów chmury prywatnej w miarę rosnących potrzeb jest trudniejsze niż w przypadku chmury publicznej – nie mamy tu efektu skali.

Chmura prywatna przede wszystkim sprawdzi się w dużych organizacjach, które będą mogły sobie pozwolić na kosztowniejszą inwestycję w sprzęt oraz zasoby ludzkie niż w przypadku chmury publicznej. Cenę kreuje tu bowiem kadra niezbędna do zapewnienia właściwej obsługi oraz konfiguracji wymagań.

CHMURA HYBRYDOWA

Ciekawym rozwiązaniem wydaje się tzw. hybryda, czyli rozwiązanie, które łączy cechy chmury prywatnej i publicznej. Dla przykładu: chmura prywatna zapewnia szerokie możliwości konfiguracji oraz wysoki poziom bezpieczeństwa, jest jednak kosztowna oraz nie zapewnia skalowalności, a także szerokiego zakresu usług, jakie możemy otrzymać w przypadku chmury publicznej. Okazuje się, że można połączyć zalety obu wcześniejszych rozwiązań.

Zalety:

a) Bezpieczeństwo oraz możliwości praktycznie dowolnej konfiguracji znane z chmury prywatnej idące w parze ze skalowalnością i usługami chmury publicznej.
b) Koszt zbudowania i obsługi chmury hybrydowej może być niższy, niż chmury prywatnej – wpływa na to brak konieczności uwzględnienia najwyższego możliwego obciążenia systemu w krótkim czasie, które musiałaby obsłużyć chmura prywatna.

Wady:

a) Chmura hybrydowa, a szczególnie jej prywatna część, wymaga dużych nakładów finansowych zarówno na sprzęt, jak i administratorów oraz architektów będących w stanie zarówno zbudować, jak i obsłużyć takie rozwiązanie.

Podsumowując – chmura hybrydowa znajdzie zastosowanie, gdy kwestie dla nas istotne, takie jak wrażliwe dane, chcemy utrzymywać po swojej stronie, a jednocześnie zależy nam na zachowaniu zalet płynących z zastosowania chmury publicznej.

Oczywiście na końcu pojawi się pytanie: „które rozwiązanie wybrać?". Niestety nie ma na nie jednej właściwej odpowiedzi. To, który rodzaj chmury obliczeniowej sprawdzi się najlepiej, zależy od jej zastosowania i środowiska, w którym będzie działała. Przy wyborze usług chmurowych należy kierować się tym, co dla nas i naszych klientów jest najlepsze funkcjonalnie i kosztowo. •

aleBank.pl

■ Bezgotówkowo ■ Blogi ■ ESG ■ Firma i gospodarka ■ Komentarze ekspertów
Nieruchomości ■ Powiedzieli ■ Prawo i regulacje ■ Rynek pracy ■ Wydarzenia
Bankowość spółdzielcza ■ Bez krawata ■ Edukacja - Banki dla Gospodarki
Finanse osobiste ■ Mój plan emerytalny ■ Kadry ■ Multimedia ■ Polecamy
■ Raporty ■ Technologie i innowacje ■ Z rynku ■ Praca zdalna

Portal ekonomiczny ■ ■ #NajbliżejFinansów

Fot. ipopba/stock.adobe.com

Chmura jako cel strategiczny

Po pierwszym kroku, w którym banki koncentrowały się na migracji określonych obciążeń w celu obniżenia kosztów i wykorzystania skalowalności chmury, pora na następne. Cloud może stać się dla banku potężną platformą do zmian w prowadzonym biznesie i wykorzystania narzędzi dostępnych wyłącznie w chmurze.

W przeszłości organizacje z sektora bankowego miały duże opory przed migracją do chmury, głównie ze względu na obawy związane z bezpieczeństwem danych i zgodnością z regulacjami. Jednak zmieniające się oczekiwania konsumentów, przyspieszona przez pandemię cyfryzacja, a także zielone światło od regulatorów skłaniają firmy świadczące usługi finansowe do fundamentalnej rewizji swoich modeli biznesowych. Obecnie wśród instytucji finansowych, które wcześniej nie chciały korzystać z chmury, nie brakuje liderów transformacji. Banki zdały sobie sprawę z możliwości, jakie oferuje przetwarzanie w chmurze w zakresie skalowalności, ograniczania kosztów, bezpieczeństwa i zgodności. Doceniają też innowacyjność, jaką można osiągnąć dzięki dostępowi do najnowszych technologii, takich jak analityka big data czy uczenie maszynowe.

Aby sprostać zmieniającym się wymaganiom i przygotować się na niestabilną przyszłość banki będą przyspieszać swoją transformację cyfrową i zwiększać wydatki na IT. Ich struktura wyraźnie się zmienia – analitycy z IDC oceniają, że w latach 2018–2021 ta cześć budżetów IT, która jest przeznaczana w bankach na chmurę publiczną, zwiększyła się dwukrotnie. Rosnący trend sprawi, że cloud będzie coraz częściej traktowany jako podstawowy zasób informatyczny.

Zanim to jednak nastąpi, w swojej transformacji do chmury banki przechodzą przez kolejne fazy. W pierwszej skupiają się przede wszystkim na redukcji kosztów operacyjnych poprzez

przeniesienie wybranych obszarów funkcjonalnych do chmury publicznej. Optymalizacja infrastruktury poprzez taktyczne migracje wybranych funkcji i obciążeń jest ważną częścią procesu wdrażania chmury. Do zarządów trafia argument ograniczenia dużych wydatków płaconych z góry i przejścia na elastyczny system płatności w modelu subskrypcyjnymi i zgodnie z rzeczywistym wykorzystaniem zasobów. Oczywiście pod warunkiem, że zapewni im się pewną przewidywalność kosztów w ujęciu miesięcznym lub rocznym. Dotyczy to wszystkich banków, także tych, które do tej pory skupiały się na gromadzeniu infrastruktury i budowie własnych data center.

Opcja chmurowa jest już w bankach rozważana obowiązkowo w przypadku nowych projektów i inicjatyw. Skalowalność we wprowadzaniu nowych rzeczy, które zawsze są mniejszym lub większym eksperymentem, staje się kluczowa. Nie trzeba kupować sprzętu, można wyjść od małego zasobu i dynamicznie go zwiększać.

Ale to wciąż podejście taktyczne, a punktem wyjścia do myślenia strategicznego stają się posiadane dane. Internet, zalew treści, demokratyzacja danych oraz możliwości ich analizowania, a także mnogość urządzeń i czujników podłączonych do sieci – wszystko to sprawiło, że bardzo zmienił się dostęp do informacji i jej dostarczanie. Banki zbierają bez porównania więcej danych niż kiedyś, zarówno własnych, jak i zewnętrznych. Dlatego tak ważne staje się znalezienie sposobu na ich wykorzystanie i utrzymanie przewagi konkurencyjnej poprzez użycie nowych technologii, takich jak interfejsy API, uczenie maszynowe (ML) i sztuczna inteligencja (AI).

Jeśli chmura ma stać się platformą dla innowacji, warto zwrócić uwagę na obszar analityki danych. Będzie to dla banku tym łatwiejsze, że platformy analityczne i hurtownie danych funkcjonują niejako z boku głównego systemu transakcyjnego i można je modernizować bez większego ryzyka dla funkcjonowania całego biznesu.

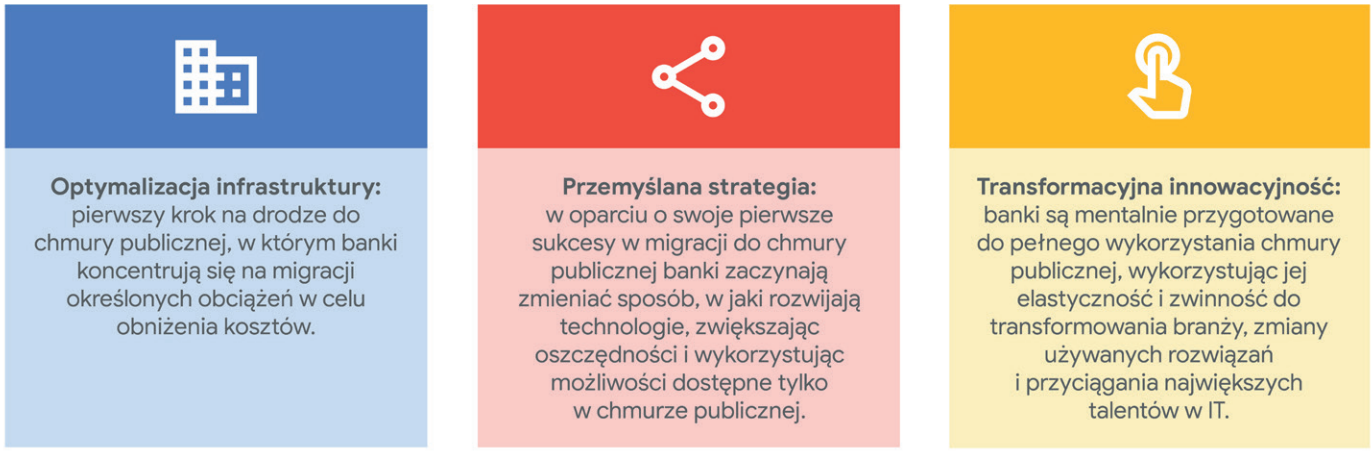
Innowacyjność, której źródłem są dane

Organizacje świadczące usługi finansowe mają do czynienia z ogromną ilością danych, w tym ustrukturyzowanymi danymi klientów i innymi informacjami zebranymi „z pierwszej ręki", a także nieustrukturyzowanymi danymi pozyskiwanymi z internetu i innych źródeł. Posiadanie tylu danych teoretycznie zapewnia lepszy wgląd w prowadzony biznes i rynek, ale w praktyce większość z informacji pozostaje niewykorzystana ze względu na złożoność zarządzania tradycyjnymi hurtowniami danych.

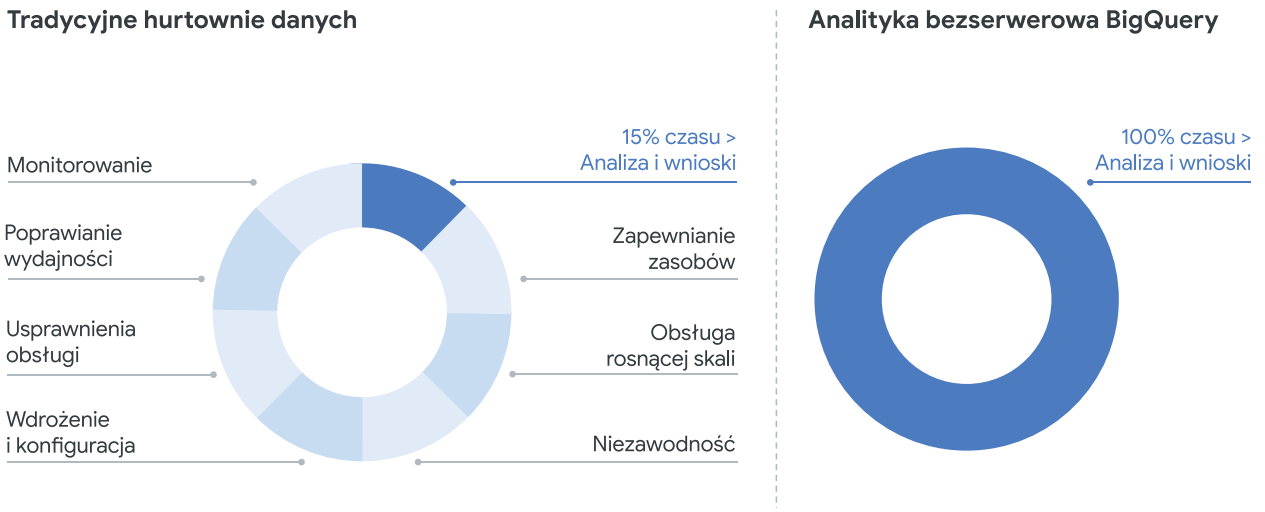
Z dyskusji, jakie firma Google prowadzi ze swoimi klientami, wynika się, że gros czasu zajmuje im inżynieria systemów i prace utrzymaniowe, a niewiele godzin zostaje im na analizowanie danych (zob. grafika). Ponieważ tradycyjna infrastruktura jest złożona, firmy wciąż inwestują w personel mający zarządzać przestarzałymi systemami, nawet jeśli nie są w stanie realizować ich strategii związanych z danymi, ani zapewniać elastyczności.

Osiąganie granicy pojemności tradycyjnej hurtowni danych nie jest czymś niezwykłym

Kolejne etapy transformacji banków do chmury



Utrzymanie tradycyjnej hurtowni danych



w sektorze bankowym. Posiadanie takiego systemu sprowadza się do ciągłego balansowania w obszarach mocy obliczeniowej, pamięci masowej i operacyjnej. W sytuacji gwałtownego wzrostu zapotrzebowania na któryś z tych elementów, niewiele daje się zrobić. Co więcej, tradycyjne rozwiązania nie skalują się dobrze.

Cloud eliminuje tego typu problemy, oferując praktycznie nieograniczoną pojemność. Rozwiązanie, takie jak Google BigQuery, oferuje działającą w modelu serverless, wysoce skalowalną i efektywną kosztowo hurtownię danych w chmurze. Automatyzuje ona zadania inżynierii systemów i zapewnia uproszczony interfejs użytkownika, uwalniając organizacje od czasochłonnych zadań utrzymaniowych i dając im więcej czasu na pracę z danymi. Ponieważ jest całkowicie oparta na oprogramowaniu, więc nie trzeba wdrażać i konfigurować sprzętu. Automatycznie się skaluje, by zmaksymalizować wydajność zapytań. Administratorzy IT nie muszą udostępniać zasobów obliczeniowych, a analitycy danych obawiać się o możliwości infrastruktury przy uruchamianiu swoich analiz.

Chmurowa hurtowania danych oferuje też znacznie większą elastyczność kosztową. Oczywiście, ktoś może wpaść na pomysł przeniesienia jeden do jednego nieefektywnej starszej architektury do chmury publicznej. Powinien jednak wcześniej pomyśleć o całkowitym koszcie posiadania hurtowni danych. TCO wykaże, jak starsze technologie i sprawność biznesowa nie pasują do siebie. Migracja do BigQuery to nie tylko transformacja do chmury, ale także przejście do nowego modelu kosztów, w którym eliminuje się infrastrukturę i inżynierię systemów. Wyliczenia Enterprise Strategy Group pokazują, że organizacje, które migrują do BigQuery, mogą obniżyć TCO nawet o blisko połowę.

Dzięki hurtowni danych w chmurze, takiej jak BigQuery, i technologiom big data banki mogą wdrażać zaawansowane systemy szacowania ryzyka. Mają one kluczowe znaczenie dla ich biznesu, zwłaszcza że po światowym kryzysie finansowym w 2008 roku zarządzanie ryzykiem znalazło się w centrum uwagi regulatorów. Z jednej strony systemy te powinny dostarczać wszelkich danych mających uzasadnić podjęcie ryzyka kredytowego. Z drugiej – dawać bankowi dbającemu o właściwe relacje z klientami argumenty przy ewentualnej odmowie.

Chmura nadaje się doskonale do stworzenia niezawodnego systemu pozyskiwania informacji z najróżniejszych źródeł, w tym danych finansowych, które – bez obaw o możliwości infrastruktury – będą wykorzystane w procesie modelowanie ryzyka. Warto zauważyć, że w obszarze szacowania ryzyka zachodzą znaczące zmiany – takie języki programowania, jak Python i R, bardzo zyskały w ostatnich

latach na popularności, stając się poważną konkurencją dla tradycyjnych rozwiązań. Banki mogą obecnie stworzyć kompletny proces modelowania ryzyka kredytowego przy użyciu wspomnianych języków open source, zapewniając sobie tym samym o wiele większy dostęp do programistów i optymalizację kosztów.

Wysoce skalowalne rozwiązania dostępne w chmurze nie tylko przynoszą oszczędność czasu i kosztów, ale także pozwalają bankom odkrywać nowe możliwości rozwoju. Sztuczna inteligencja i uczenie maszynowe zmieniają już oblicze innych branż. Takich na przykład, jak handel detaliczny, gdzie analityka predykcyjna pomaga retailerom podejmować lepsze decyzje. Banki także będą podążać tą drogą, choćby wykorzystując BigQuery jako działający w czasie rzeczywistym system do wykrywania nadużyć kart kredytowych.

AI i ML – potężne, ale łatwe w użyciu narzędzia

Brak pełnego wglądu w klienta, a tym samym niemożność zbudowania z nim jak najlepszej relacji, to tracony dochód. Rozwiązaniem staje się uczenie maszynowe, które może sprawić, że „inteligencja banku" będzie wzrastać wykładniczo. „Inteligencja" w tym przypadku oznacza pozyskiwanie bardziej wartościowych informacji o klientach, które mogą przekładać się na jak najlepszą ich obsługę, czyli na to, co branża uznaje za klucz do wyróżnienia się na tle konkurencji, wzrostu biznesu i zwiększenia zysków. Sztuczna inteligencja i uczenie maszynowe mogą usprawnić bankowość w kilku obszarach, w tym personalizacji obsługi klienta, identyfikacji wzorców i powiązań (których człowiek nie jest w stanie sam wykryć), oraz udzielaniu odpowiedzi i rozwiązywaniu problemów w czasie rzeczywistym. Od jakiegoś czasu banki wykorzystują elementy uczenia maszynowego, przetwarzania kognitywnego i języka naturalnego w kilku typowych zastosowaniach (zob. ramka).

> *Wdrożenie uczenia maszynowego nie jest tak proste, jak naciśnięcie guzika, ale dzięki chmurze nie potrzeba dużego zespołu specjalistów, by w pełni wykorzystać swoje dane. Można od razu skorzystać ze sprawdzonych, intensywnie wytrenowanych modeli, takich jak Cloud Vision, Natural Language czy Translate.*

Banki mogą korzystać z szerokiej gamy narzędzi sztucznej inteligencji i systemów uczących się, przeznaczonych zarówno dla programistów i analityków, jak i tych użytkowników, którzy nie mają doświadczenia w data science. Przykładowo BigQuery ML umożliwia analitykom danych tworzenie i wdrażanie zaawansowanych, niestandardowych modeli uczących się przy użyciu wyłącznie podstawowych komend SQL. Modele te można dalej udoskonalać – dodawać lokalizację lub dowolną inną, potrzebną analitykowi zmienną, wykorzystując przy tym obszerną bibliotekę publicznych zbiorów danych Google.

Innym przykładem jest rozwiązanie Document AI, które analizuje i wydobywa informacje z dokumentów biznesowych. W oparciu na nim powstało narzędzie LendingDoc AI, stworzone do obsługi kredytów hipotecznych. LendingDoc AI automatyzuje rutynowe przeglądy dokumentów hipotecznych, skraca czas przetwarzania i usprawnia przechwytywania danych przy jednoczesnym zapewnieniu zgodności z regulacjami. W efekcie pożyczkodawcy tracą mniej czasu na zadania administracyjne, a pożyczkobiorcy korzystają z szybszej i płynniejszej obsługi swoich wniosków.

Oczywiście, wdrożenie uczenia maszynowego nie jest tak proste, jak naciśnięcie guzika, ale dzięki chmurze nie potrzeba dużego zespołu specjalistów, by w pełni wykorzystać swoje dane. Można od razu skorzystać ze sprawdzonych, intensywnie wytrenowanych modeli, takich jak Cloud Vision, Natural Language czy Translate. Można też szybko tworzyć własne modele przy użyciu Cloud Machine Learning Engine czy TensorFlow, powszechnie wykorzystywanych platform do uczenia maszynowego.

Dużym ułatwieniem mogą być także produkty AutoML, umożliwiające programistom z niewielkim doświadczeniem w zakresie uczenia maszynowego wytrenowanie wysokiej jakości modeli dostosowanych do konkretnych potrzeb biznesowych ich firm. Pozwalają one budować własny, niestandardowy model ML w bardzo krótkim czasie.

Otwarta platforma i aplikacje, które można uruchamiać w każdej chmurze

W działających od lat bankach plany związane z migracją do chmury muszą uwzględniać duże nakłady, które do tej pory włożono w infrastrukturę on-prem, w tym starsze aplikacje o znaczeniu krytycznym, których często nie da się napisać od nowa. Ale nawet wtedy, gdy organizacja jest gotowa zrezygnować z tych inwestycji, mogą jej na to nie pozwolić istniejące przepisy. Bez względu na to, czy regulacje dopuszczają przeniesienie się w całości do chmury, czy też nie, i tak najczęstszym scenariuszem migracji będzie budowa środowiska hybrydowego, złożonego z chmury prywatnej i publicznej.

Preferowaną strategią stanie się też multicloud, czyli korzystanie z więcej niż jednego

Typowe zastosowania AI i ML w bankowości

Wykrywanie oszustw w czasie rzeczywistym: sztuczna inteligencja i uczenie maszynowe mogą identyfikować nieuczciwe działania w trakcie ich trwania, a także przewidywać, w jakim kierunku mogą się one rozwinąć. W tym procesie pomocą są dane lokalizacyjne.

Zapewnianie zgodności z regulacjami: nowe technologie mogą być wykorzystane do spełniania ustalonych standardów i prowadzonego w czasie rzeczywistym monitoringu przechowywanych danych. Dzięki temu ewentualne problemy mogą być zgłaszane znacznie wcześniej.

Zarządzanie ryzykiem: jest wiele sposobów na wykorzystanie AI i ML w tym obszarze. Przykładowo systemy oparte na sztucznej inteligencji mogą przewidywać ryzyko inwestycyjne i ubezpieczeniowe, analizować rzeczywiste zamiary klienta, któremu ma być udzielony kredyt, a także oceniać ryzyko zaangażowania w pranie pieniędzy lub finansowanie terroryzmu.

Obniżenie kosztów i zwiększenie przychodów: największy potencjał ma tutaj automatyzacja pierwszej linii. Korzyści płynące z bardziej zautomatyzowanej i inteligentnej komunikacji z klientami wynikają z ograniczenia kosztów, przy ryzyku rozłożonym na miliony interakcji z klientami. Wirtualni asystenci i robotyka back office staja się już powszechne.

Podnoszenie poziomu obsługi klienta: uczenie maszynowe zapewnia możliwość lepszego i szybszego podejmowania decyzji poprzez uzyskanie głębokich i praktycznych obserwacji (np. wzorców zachowań klientów). Niektóre z aplikacji wykorzystują nową technologię interakcji głosowej albo chatboty, podczas gdy inne mogą działać w tle, wspierając komunikację marketingową.

Zwiększanie zaangażowania klientów: sztuczna inteligencja pomaga w tworzeniu spersonalizowanych i inteligentnych produktów oraz usług z nowymi funkcjami, bardziej intuicyjnymi interakcjami (np. opartymi na mowie) i zdolnościami doradczymi (np. w zarządzaniu finansami osobistymi).

dostawcy chmury publicznej. Daje to możliwość użycia najlepszych funkcji z dostępnych na rynku platform i uruchamiania wybranych obciążeń w wybranej chmurze. Kolejnymi zaletami podejścia opartego na wielu chmurach jest większa nadmiarowość i unikanie uzależnienia od dostawcy (vendor lock-in). Problem w tym, że środowiska multicloud są bardzo złożone i trudne w zarządzaniu. Działy IT i cyberbezpieczeństwa muszą korzystać z różnych konsol i narzędzi przy każdym wdrożeniu chmury, co jest żmudne, czasochłonne i zwiększa ryzyko błędów. Przy wielu chmurach trudnym do pokonania wyzwaniem staje się też uzyskanie pełnego obrazu tego, co dzieje się w całym zarządzanym środowisku danych.

Dlatego potrzebne jest centralnie obsługiwane i wysoce dostępne rozwiązanie do wdrażania, zabezpieczania i zarządzania w spójny oraz efektywny kosztowo sposób wszystkimi obciążeniami środowisku hybrydowym i multicloud. Platforma, która zapewnia migrację i modernizację przeprowadzaną w wybranym tempie, umożliwiając jednocześnie korzystanie ze spójnego środowiska programistycznego i operacyjnego, zarówno w chmurze, jak i on-prem. I która staje się centralnym punktem dla zunifikowanej analityki, działań operacyjnych i opartej na politykach automatyzacji.

W docelowym środowisku wielochmurowym kluczowe staje się zapewnienie neutralności i przenaszalności obciążeń, ponieważ pozwala to uniknąć marnowania czasu na debugowanie, diagnozowanie problemów i wdrażanie aplikacji w różnych chmurach. Najprostszym i najskuteczniejszym rozwiązaniem tego problemu okazały się być kontenery. Mogą być uruchamiane w dowolnym miejscu, zapewniają spójne, przewidywalne środowisko wykonawcze i zużywają znacznie mniej zasobów niż maszyny wirtualne. Kubernetes – stworzony przez Google i rozwijany obecnie na zasadach open source system orkiestracji kontenerów – stał się de facto standardem w zarządzaniu środowiskami kontenerowymi. Można go wdrożyć w dowolnym środowisku chmury, zarówno prywatnej, publicznej, jak i hybrydowej.

Decydując się na migrację, organizacje miały wcześniej dwie możliwości przenoszenia obciążeń lokalnych do chmury. Mogły najpierw migrować aplikacje, a potem je skonteneryzować, albo najpierw skonteneryzować, a migrować później. Żadna z tych opcji nie była szczególnie atrakcyjna. Duże firmy, ta-

Bank Polski

Studium przypadku

PKO Bank Polski: misja wprowadzenia Polski do chmury i tworzenie bankowych usług przyszłości PKO Bank Polski korzysta z Google Cloud, aby przyspieszyć dostarczanie nowoczesnych usług bankowych swoim klientom. Zachęca przy tym inne firm do korzystania z technologii chmury, wspomagając rozwój polskiej gospodarki.

Korzyści z migracji do chmury:

- szybsze docieranie z usługami aplikacyjnymi do klientów poprzez skrócenia czasu wprowadzania ich na rynek,
- użycie zaawansowanej analizy danych do rozwijania innowacyjnych funkcji odpowiadających na zachowania klientów,
- lepsza komunikacja doradców z klientami, w tym zdalne spotkania „twarzą w twarz" przy użyciu Google Meet z pakietu Google Workspace,
- stworzenie punktu odniesienia dla innych firm w Polsce i zachęcanie ich do korzystania z rozwiązań chmurowych i hybrydowych.

Źródło: https://cloud.google.com/customers/pko-bank-polski

Podstawową korzyścią od początku migracji infrastruktury aplikacji do Google Cloud był skrócony czas wprowadzania nowych usług na rynek. Po zakończeniu migracji do chmury w 2023 r. będziemy mogli również zamknąć jedno z naszych dwóch centrów danych, co pomoże zoptymalizować koszty i uelastycznić naszą infrastrukturę.

Adam Marciniak,
CTO, PKO Bank Polski

COMMERZBANK

Studium przypadku

Commerzbank: cel - przeniesie wielu aplikacji bankowych do chmuryGoogle Cloud będzie wspierać Commerzbank w jego realizowanej od 2017 r. strategii transformacji cyfrowej, której celem jest stworzenie organizacji opartej na chmurze i wprowadzanie innowacyjnych rozwiązań dla klientów banku. Klienci Commerzbanku już korzystają z „Digitale Kontoanalyse", pierwszej aplikacji stworzonej na Google Cloud Platform.

Korzyści z tej aplikacji dla klientów i pracowników Commerzbanku:

- cyfrowa analiza konta, skutkująca lepszą współpracą banku i klientów, m.in. szybszym przetwarzaniem wniosków kredytowych,
- tworzenie dokładnych bilansów przychodów i wydatków dla każdego konta klienta,
- usprawnione śledzenie historycznych danych finansowych, dzięki czemu klienci mogą optymalizować swoje dochody i wydatki.

Źródło: https://cloud.google.com/press-releases/2021/0329/commerzbank-google-cloud

W naszej nowej „Strategii 2024" podejście wielochmurowe odgrywa ważną rolę. Będziemy korzystać z dużych możliwości Google Cloud w zakresie modernizacji infrastruktury, a także z know-how w zakresie analizy danych i uczenia maszynowego tej firmy, jednego z pionierów w tym obszarze. W naszej migracji do chmury Google Cloud jest ważnym partnerem strategicznym.

Richard Bates,
Global Head of HSBC's Intelligence Hub, Wealth and Personal Banking, HSBC

kie jak banki, mają zazwyczaj setki, jeśli nie tysiące starszych aplikacji, z których wszystkie musiałyby zostać ręcznie zrefaktoryzowane, aby mogły zostać skonteneryzowane. Obecnie, wykorzystując odpowiednie narzędzia z chmury, można jednocześnie migrować i konteneryzować aplikacje maszyn wirtualnych. Potem je uruchamiać i zarządzać nimi za pośrednictwem Kubernetesa, bez konieczności ręcznej refaktoryzacji.

Bezpieczeństwo w chmurze to argument za migracją

Początkowo, ze względu na regulacje, sektor bankowy bardzo powoli migrował do chmury publicznej. Za największe bariery dla transformacji uznawano kwestie związane z bezpieczeństwem danych, zachowaniem zgodności

W docelowym środowisku wielochmurowym kluczowe staje się zapewnienie neutralności i przenaszalności obciążeń, ponieważ pozwala to uniknąć marnowania czasu na debugowanie, diagnozowanie problemów i wdrażanie aplikacji w różnych chmurach. Najprostszym i najskuteczniejszym rozwiązaniem tego problemu okazały się być kontenery.

i ochroną prywatności. Jednakże w ciągu ostatnich kilku lat wykorzystanie usług w chmurze wyraźnie wzrosło, gdy banki zdały sobie sprawę z korzyści biznesowych i większego bezpieczeństwa wynikającego z migracji. Branża zwraca się do dostawców chmury, by ograniczać ryzyko poprzez zapewnienie wysokiej dostępności oraz integralności, przenośności i poufności danych.

Jeśli chodzi o poufność informacji, to operator chmury publicznej nie tylko szyfruje wszystkie dane przesyłane (in transit) pomiędzy platformami, klientami i centrami danych, ale także domyślnie szyfruje wszystkie dane przechowy-

wane (at rest) w ramach swoich usług. Co więcej, dane mogą być zaszyfrowane także podczas przetwarzania (in use) przy użyciu zabezpieczeń oferowanych przez procesory nowej generacji. Dane pozostaną wtedy zaszyfrowane również podczas ich używania, indeksowania, odpytywania czy trenowania.

Zapewnia to usługa Confidential Computing, której użycie jest bardzo proste. Wystarczy zaznaczyć pole wyboru, by zwykła maszyna wirtualna została automatycznie przekonwertowana na poufną. Nikt nie będzie dotykał kodu ani w inny sposób zmieniał obciążenia. Banki i inne instytucje finansowe mogą migrować swoje aplikacje do wysoce bezpiecznego środowiska bez wysiłku i utraty wydajności. Dodatkowo, operator chmury umożliwia programistom implementowanie szyfrowania w warstwie aplikacji, zapewniając najwyższy możliwy poziom ochrony danych.

> *Operator chmury publicznej nie tylko szyfruje wszystkie dane przesyłane (in transit) pomiędzy platformami, klientami i centrami danych, ale także domyślnie szyfruje wszystkie dane przechowywane (at rest) w ramach swoich usług. Co więcej, dane mogą być zaszyfrowane także podczas przetwarzania (in use).*

Operator nie korzysta z dostępu do danych klientów poza sytuacjami, gdy jest to absolutnie konieczne do wypełnienia zobowiązań umowy – na przykład rozwiązywania problemów technicznych lub dotyczących bezpieczeństwa. Wewnętrzne mechanizmy kontroli operatora wymagają od wszystkich pracowników, którzy uzyskują dostęp do danych klientów, przedstawienia ważnego uzasadnienia biznesowego. Przeprowadza on także regularne audyty, by zagwarantować, że mechanizmy kontroli dostępu są przestrzegane. •

PayPal

Studium przypadku

PayPal: wykorzystanie Google Cloud do bezproblemowego zarządzania nagłymi przyrostami transakcji finansowych Firma PayPal przeprowadziła migrację do Google Cloud skalowalnych poziomo aplikacji swojej platformy płatniczej. To znaczący zwrot strategii w kierunku transakcji w chmurze w celu zapewnienia klientom łatwych w użyciu i niezawodnych usług.

Korzyści z migracji do chmury:

- przeniesienie skalowalnych poziomo aplikacji platformy płatniczej i obciążeń transakcyjnych do chmury,
- zakończenie w chmurze w ciągu kilku minut prac, które w środowisku on-prem zabrałyby miesiąc ,
- znaczne ograniczenie kosztów w porównaniu z tym, jakie trzeba by ponieść na zasoby on-prem w celu obsłużenia szczytowych wolumenów,
- bezproblemowa obsługa gwałtownych przyrostów transakcji związanych z pandemią i sezonem świątecznym 2020.

Źródło: https://cloud.google.com/customers/paypal/

Inżynierowie PayPal zarządzający obciążeniami początkowo wyrażali pewne obawy związane ze zmianą. Gdy następnie przekonali się, jak łatwo jest zwiększyć pojemność w najbardziej gorącym okresie świątecznym, jak dotąd przeżyliśmy, a potem zmniejszyć pojemność, gdy nie jest już potrzebna, stali się entuzjastami przejścia do chmury.

Wes Hummel,
Vice President, Site Reliability and Cloud Engineering, PayPal

HSBC

Studium przypadku

HSBC: wykorzystanie chmury do podniesienia poziomu obsługi klienta w call center. Współpracując z Google Cloud, HSBC automatyzuje system oceny jakości rozmów sprzedażowych w contact center, skracając znacznie czas tego procesu i usprawniając obsługę klienta. Bank pracuje również nad zapewnieniem szybszego dostępu do zasobów w chmurze, wspieraniem opartych na niej innowacji i rozwojem produktów.

Korzyści z migracji do chmury:

- znaczące przyspieszenie procesu oceny wartości rozmów sprzedażowych, co przekłada się na dużo większe możliwości podnoszenia ich jakości, zgodnie z potrzebami klientów,
- zwiększenie ogólnego poziomu obsługi klienta przez call center poprzez szybkie uzyskiwanie informacji zwrotnych na poziomie agenta i centrum,
- skrócenie czasu potrzebnego na uruchomienie modeli uczenia maszynowego z tygodnia do godziny.

Źródło: https://cloud.google.com/customers/hsbc

Google jest jednym z naszych strategicznych partnerów. Wraz z nimi inwestujemy w uczenie maszynowe i możliwości przetwarzania danych, ponieważ ich rozwiązanie w chmurze zapewnia bezpieczne i niezawodne przetwarzanie danych osobowych.

Richard Bates,
Global Head of HSBC's Intelligence Hub, Wealth and Personal Banking, HSBC

Jesteśmy z Wami od ponad 10 lat!

www.nzb.pl

NOWOCZESNE ZARZĄDZANIE BIZNESEM

Program współpracy szkół wyższych i sektora finansowego

Ponad **120** szkół wyższych

Blisko **320 000** studentów

Ponad **2 450** wykładów

Ponad **360** konferencji

Ponad **500** stref edukacyjnych

Partnerzy programu edukacyjnego Nowoczesne Zarządzanie Biznesem:

Związek Banków Polskich

BIG InfoMonitor

BIK Biuro Informacji Kredytowej

KIR

ZUS Zakład Ubezpieczeń Społecznych

Grupa BPS Banki Spółdzielcze i Bank BPS

SGB Spółdzielcza Grupa Bankowa Liczysz się dla nas

Fot. peshkov/stock.adobe.com

IBM ułatwia transformację banków do chmury – rady ekspertów

Adopcja chmury stale wzrasta w wielu branżach i choć instytucje finansowe, ze względu na dużą liczbę poufnych informacji o klientach, są ściśle regulowane, to przyjęcie przez nie chmury wcale nie musi być spowolnione.

W raporcie przygotowanym przez Celent, wiodącą firmę badawczą i doradczą skoncentrowaną na technologiach dla instytucji finansowych działających na całym świecie wyróżniono siedem kluczowych zagadnień związanych z wykorzystaniem chmury publicznej przez branżę finansową.

Są to:

- bezpieczeństwo i zaufanie;
- zarządzanie ryzykiem i zgodność;
- zarządzanie partnerami ekosystemu klienta;
- poprawa satysfakcji klienta;
- elastyczność zarządzania kosztami (zamiana CAPEX na OPEX);
- zwinność, aby szybciej wprowadzać nowe produkty na rynek;
- efektywność operacyjna.

Jak spełnić te warunki? Usługa IBM Cloud™ for Financial Services ułatwia zarządzanie ryzykiem podczas wdrażania chmury, bo zaprojektowano ją z zapewnieniem dedykowanych funkcji dla potrzeb bezpieczeństwa, zachowania zgodności i dostępności wymaganej przez instytucje finansowe. Dzięki temu można bez obaw udostępniać w takiej chmurze newralgiczne aplikacje oraz szybko i efektywnie obsługiwać transakcje. Jednocześnie banki mogą skorzystać z ekosystemu rozwiązań ponad 100 partnerów technologicznych, zweryfikowanych przez IBM, udostępniających swoje rozwiązania w IBM Cloud.

Dodatkowo wstępnie już skonfigurowane mechanizmy kontroli pozwalają zapewnić ciągłą zgodność infrastruktury z wymogami lokalnego regulatora oraz przyspieszyć wdrożenie chmury. Natomiast poufne przetwarzanie danych zapewnia usprawnienie mechanizmów zabezpieczeń, a także pełną kontrolę.

Droga do chmury z IBM

Przejście do chmury powinno być procesem poprzedzonym analizą, czyli przede wszystkim oszacowaniem potencjalnych korzyści dla klienta kontra ryzyka, a na końcu oczywiście wdro-

żeniem i utrzymaniem projektu, który na przestrzeni lat będzie ewoluował. Warto zadać sobie pytanie, po co chcemy przenieść swoje aplikacje do chmury, jakie osiągniemy cele krótko i długoterminowe, oraz jakie ryzyka przy tym ponosimy. Przy czym chmura nie powinna być postrzegana tylko jako kolejna platforma dla aplikacji, ale zapewniać znacznie więcej, jeśli chcemy, żeby nasz projekt migracji, przyniósł nam większe efekty. Zamiana kosztów inwestycyjnych na operacyjne albo szybsze uruchamianie projektów, to tylko cześć korzyści, które możemy osiągnąć przy tej operacji. Warto rozważyć wsparcie najnowszych zdobyczy technologicznych, takich jak sztuczna inteligencja albo blockchain, żeby ulepszyć obsługę swoich klientów oraz przewidywać zachowania i trendy na rynku, które dopiero będą miały miejsce, zamiast tradycyjnej analizy danych z zeszłych lat.

IBM ma w tym zakresie duże doświadczenie, realizując takie projekty z bankami od wielu lat. Dawniej były to projekty outsourcingowe, które teraz transformują się w projekty oparte na platformie chmurowej oraz są związane z modernizacją aplikacji, aby dostarczały więcej wartości.

Fot. IBM

Marcin Klabinski: Komunikat chmurowy stawia wyzwania, które bez wnikliwej analizy prowadzą niekiedy do zbyt szybkiej tezy, „że się nie da". I rzeczywiście adopcja usług chmurowych może być trudna bez zbudowania właściwych kompetencji i świadomości tego, jak się korzysta z usług przetwarzania danych w chmurze. Należy pamiętać, że chmura nie zdejmie całej odpowiedzialności z użytkownika. Jej wykorzystanie jest tylko innym sposobem podejścia do utrzymania i rozwoju systemów informatycznych. Jest innym, dlatego też wymaga nowych kompetencji oraz zmiany świadomości dotyczącej zachowania bezpieczeństwa. Finalnie jednak to nadal klient albo integrator odpowiedzialny jest za to, żeby dane były przetwarzane w sposób zgodny z regulacjami, ale przede wszystkim w sposób bezpieczny, oraz za chronienie danych swoich klientów i informacji biznesowych. A składa się na to wiele komponentów, takich jak właściwa konfiguracja nadawania uprawnień, szyfrowanie danych w ruchu i spoczynku, zapewnienie architektury wysokiej dostępności, tworzenie kopii zapasowych i wiele innych, wynikających z najlepszych praktyk projektowania systemów oraz wymagań UKNF.

Stąd też wynikła potrzeba zbudowania IBM Cloud™ for Financial Services, który wykorzystujemy w projektach prowadzonych z bankami i który jest predefiniowanym środowiskiem implementującym określone regulacje, standardy i dobre praktyki wynikające zarówno bezpośrednio z regulacji, jakim podlegają banki, jak i z innych standardów obecnych na rynku. IBM Cloud™ for Financial Services jako gotowy zestaw narzędzi na Chmurze IBM pozwala szybciej wdrożyć elementy pomagające bankom monitorować i konfigurować oraz zabezpieczać we właściwy sposób swoje środowiska, żeby działały one w najwyższych dostępnych standardach.

Fot. IBM

Piotr Beńke: Technologia i dostępność narzędzi, które oferuje IBM, ułatwia procesy migracji systemów na platformę chmurową, a tym samym ułatwia podejmowanie decyzji o migracji do środowisk chmurowych. Przykładem jest IBM CloudTM for Financial Services. Chmura zaprojektowana z myślą o budowaniu zaufania i przejrzystego ekosystemu chmury publicznej. Zapewniająca dedykowane funkcje na potrzeby bezpieczeństwa, zachowania zgodności i odporności, wymagane przez instytucje finansowe. Dzięki temu rozwiązaniu banki mogą bez obaw realizować transakcje w chmurze, korzystając jednocześnie z ekosystemu ponad 90 partnerów, udostępniających oprogramowanie jako usługę. Kolejnym przykładem są serwisy chmurowe IBM Hyper Protect, które udostępniają, aktualizują i monitorują między innymi bazy danych takich jak MongoDB, czy PostgreSQL. Tutaj pełna kontrola danych, zarządzanie kluczami szyfrującymi jest po stronie klienta. Zapewnia to ochronę przed naruszeniem zabezpieczeń danych i ich niepożądanym modyfikowaniem przez nieuprzywilejowanych użytkowników. W tym przypadku dostęp do przechowywanych danych jest niemożliwy także dla operatora chmury.

Przygotowanie przejścia do chmury

Marcin Klabiński: W transformacji chmurowej na samym początku najważniejsze jest zawsze zdefiniowanie, co bank chce osiągnąć? Czy najważniejszym oczekiwaniem jest optymalizacja kosztowa, czy może zmiana procesów biznesowych np. zmiana podejścia do obsługi klienta, tak aby była bardziej klientocentryczna, bardziej zwinna, i szybciej dostosowywała się do zmieniających się warunków, chociażby takich, jakie spowodowała pandemia. Dopiero w kolejnym kroku właściwie przeprowadzona analiza powinna doprowadzić nas do koniecznych zmian technologicznych, w tym również wniosków dotyczących korzyści z wykorzystania chmury. IBM ma bardzo dobrze zdefiniowaną metodykę i takie projekty transformacyjne realizowaliśmy wspólnie z naszymi klientami. Rozpoczynały się one od prac prowadzonych przez dział konsultingowy IBM, który przygotowywał analizę stanu obecne-

go i oczekiwanego oraz to, co należy zrobić, żeby uzyskać pożądane efekty, uwzględniając czynniki technologiczne, procesowe i organizacyjne.

Piotr Beńke: Decyzja o migracji na platformę chmurową powinna mieć uzasadnienie biznesowe np. zgodność z regulacjami, koszty vs. korzyści, elastyczność rozwiązania, szybkość uruchomienie nowych modeli lub funkcji biznesowych, rozbudowywalność itp. Pozwoli to określić, jakie systemy i aplikacje powinniśmy mieć w takim modelu. Wcale nie chodzi tu o decyzję o migracji do chmury publicznej lub prywatnej, ale o zbudowanie rozwiązania pozwalające na zapewnienie elastyczności dla funkcji i modeli biznesowych w środowisku wielochmurowym, hybrydowym. Traktujmy

> *Technologia, którą oferuje IBM, ułatwia podjęcie decyzji o migrowaniu systemów do chmury i przeprowadzenie tego procesu. Przykładem jest IBM CloudTM for Financial Services lub serwisy Hyper Protect w IBM CloudTM. Rozwiązania te zapewniają przetwarzanie poufnych danych, wykonując obliczenia w sprzętowym zaufanym środowisku wykonawczym, chroniąc dane w całymich cyklu życia obliczeniowego w spoczynku, podczas przesyłania i użytkowania.*

chmurę jako platformę o pewnych cechach, a nie jako konkretne miejsce uruchomienia aplikacji. Dobrze zaprojektowane rozwiązanie pozwala na jego uruchomienie na dowolnej chmurze (prywatnej, publicznej, hybrydowej, czy też rozproszonej). Rozwiązanie takie jak IBM Cloud Satellite, pozwala np. uruchomić część procesu na fragmencie chmury publicznej IBM Cloud wykorzystującej infrastrukturę klienta (własne DC, chmura innych dostawców). Warto zadać sobie pytanie, czy migrować i modernizować aplikację, czy budować nowe systemy bazując na modelach chmurowych i architekturze mikroserwisowej.

Lepiej od razu zrobić większy projekt

Marcin Klabiński: Niekiedy klienci stosują podejście, żeby zacząć swoją przygodę z chmurą od czegoś małego i na bazie zdobytych doświadczeń realizować kolejne pomysły. Z moich wieloletnich doświadczeń wynika, że na ogół takie podejście się nie sprawdzało. W szczególności w sektorze bankowym, gdzie oprócz konieczności wdrożenia nowych procesów operacyjnych wynikających ze specyfiki chmury, zmian w architekturze bezpieczeństwa systemów informatycznych, banki muszą zapewnić zgodność rozwiązania z obowiązującymi je regulacjami i wykazać regulatorowi, że realizujemy projekt zgodnie z najwyższymi standardami. Podsumowanie niezbędnych inwestycji z korzyściami biznesowymi na ogół prowadziło do wniosku, że to się zwyczajnie nie opłacało.

Dlatego budowa systemu „małymi krokami" jest moim zdaniem nieefektywna. W dużych projektach, które prowadziliśmy z bankami takimi jak: Bank of America, BNP Paribas we Francji, czy Santander Bankiem myślenie o transformacji chmurowej miało charakter strategiczny. Tylko wtedy bank może odnieść istotne korzyści wynikające nie tylko z optymalizacji kosztowej, ale również z innego sposobu podejścia do procesów i obsługi klienta.

Piotr Benke: IBM ma doświadczenie nabyte podczas współpracy z wieloma bankami na całym świecie. Posiada rozwiązania chmurowe, które już przez wiele z nich jest wykorzystywane. Także w Polsce coraz więcej podmiotów nadzorowanych przez Urząd Komisji Nadzoru Finansowego (KNF) rozważa lub wdraża rozwiązania wykorzystujące chmurę publiczną, a na pewno każdy z podmiotów pracuje nad projektami w modelu chmury hybrydowej. IBM ze swoim szerokim portfolio rozwiązań dla chmury hybrydowej jest gotowy pomóc każdemu z nich.

Marcin Klabiński: Dzisiaj coraz rzadziej spotykamy się z oczekiwaniem klienta, że dane muszą być składowane i przetwarzane w Polsce, bo na ogół adekwatnym jest Europejski Obszar Gospodarczy. Wciąż jednak wymagana jest weryfikacja i potwierdzenie, że rzeczywiście dane nie są „wyprowadzane" poza EOG. IBM może tu udzielić jednoznacznych odpowiedzi. W przypadku chmury IBM dane pozostają tam, gdzie inicjalnie została powołana usługa do ich przechowywania i zarządzania nimi. Zasada ta dotyczy nie tylko danych biznesowych składowanych w dedykowanych do ich składowania i przetwarzania usługach, ale również danych zawartych w logach i metadanych, z których część też może stanowić tajemnicę biznesową.

Piotr Beńke: Jest też obszar danych, takich jak kopie zapasowe (backup), dane replikowane na potrzeby procesów odtwarzania po awarii (disaster recovery). Tutaj z praktycznego punktu widzenia może pojawić się pokusa, by takie dane umieścić w innej strefie czasowej. To spowoduje, że dane banków mogą trafić poza rejon Unii Europejskiej. Dlatego ważne są usługi, które pozwalają na pełną autonomię zarządzania danymi przez klienta, a nie przez operatora. Takie też oferuje IBM. Operator udostępnia tylko miejsce i przestrzeń do gromadzenia i procesowania danych. Natomiast nie ma do nich wglądu.

Marcin Klabiński: Często skupiamy się na lokalizacji danych, ale należy brać pod uwagę wszystkie możliwe elementy, które je zabezpieczają. Miejsce przechowywania może mieć plusy, ale nie jest warunkiem wystarczającym do właściwego zabezpieczenia informacji. Dopiero zastosowanie wszystkich możliwych opcji, czyli na przykład silnego szyfrowania (potwierdzonego choćby certyfikatem FIPS 140–2 Level 4), właściwej granulacji nadawania uprawnień, jasnego po-

działu odpowiedzialności pomiędzy dostawcą chmury i jego użytkownikiem, gwarancja pozostawania danych w inicjalnej lokalizacji powołania usługi, konfiguracja sieci umożliwiająca właściwy poziom izolacji zasobów itp. pozwalają na odpowiednie zabezpieczenie danych. Trzeba na to zagadnienie patrzeć kompleksowo. Jeżeli mówimy o chmurze i o dostępie z każdego miejsca na świecie, to w tym przypadku lokalizacja na przykład w Polsce, nie wnosi jakiś istotnych elementów do zabezpieczenia przechowywanych informacji.

JUŻ PRZESZLI DO CHMURY RAZEM Z IBM!

Luminor Bank wdrożył IBM Cloud™ for Financial Services

Luminor Bank i IBM w grudniu 2020 r. podpisały nową, pięcioletnią umowę, na mocy której IBM Services wspiera Luminor w przyspieszeniu cyfrowej transformacji, przy stałym wzmacnianiu procesów bezpieczeństwa i zgodności z przepisami poprzez migrację infrastruktury IT do IBM Cloud™ for Financial Services. Luminor dąży do przyspieszenia wdrażania technologii nowej generacji i rozwiązań wykorzystujących technologię cyfrową w środowisku chmury hybrydowej. Pomoże to w osiąganiu lepszych wyników w procesach biznesowych i umożliwi szybsze wdrażanie aplikacji oraz zapewni elastyczność przy zwiększonym bezpieczeństwie oraz odporności.

Luminor to trzeci co do wielkości bank w regionie bałtyckim i Estonii, powstały w 2017 roku w wyniku połączenia operacji Nordea i DNB w krajach bałtyckich. Bank wszedł w kolejny etap transformacji po udanej migracji klientów do nowej wspólnej platformy bankowej, niezależnej od dawnych banków macierzystych.

Nowa platforma cyfrowa obejmuje IBM Cloud Framework for Financial Services. Zawiera również te same uznane możliwości przetwarzania poufnego, takie jak w IBM Z, a także funkcje szyfrowania „Keep Your Own Key", dostarczane za pośrednictwem usług IBM Hyper Protect. W ramach umowy IBM Global Business Services zapewnia bankowi Luminor wiedzę branżową i dostęp do innowacji technologicznych w chmurze, sztucznej inteligencji i bezpieczeństwie. Jak powiedział **Ilja Sovetov**, CTO Luminor: „*IBM dysponuje najnowocześniejszymi możliwościami zarówno w zakresie operacji technologicznych, jak i zrozumienia konkretnych potrzeb branży bankowej w zakresie zgodności z przepisami, bezpieczeństwa i odporności. Ten program może również pomóc w przyspieszeniu wdrażania zaawansowanych rozwiązań w zakresie cyberbezpieczeństwa, zgodności i przepisów*".

BNP Paribas wykorzystuje IBM Cloud™ for Financial Services

Bank BNP Paribas zdecydował się przyłączyć się do IBM Cloud™ for Financial Services jako główny klient w Europie, aby wesprzeć swoją pierwszą na Starym Kontynencie dedykowaną chmurę, by była zgodna z RODO. To potwierdza, że chmura publiczna korzysta z głębokiej wiedzy IBM o branży finansowej, w ramach kontroli i najlepszej możliwości ochrony danych oraz spełnia rygorystyczne standardy. BNP Paribas korzysta z dedykowanej chmury, opracowanej i zarządzanej przez IBM. Wykorzystuje ona technologie chmury publicznej IBM, w tym funkcje szyfrowania Keep Your Own Key (KYOK). BNP Paribas może w przyszłości planować włączenie dodatkowych partnerów bankowych do ekosystemu w całej Europie.

Bank of America korzysta z IBM Cloud™ for Financial Services

David Reilly, dyrektor ds. Global Banking & Markets w Bank of America powiedział: „*Odnieśliśmy wielki sukces dzięki naszej zastrzeżonej, prywatnej chmurze, w której obecnie mieści się większość naszych obciążeń technologicznych. Jednocześnie staraliśmy się znaleźć rozwiązanie gotowe do obsługi usług finansowych, które oferuje ten sam poziom bezpieczeństwa i ekonomii, co nasza chmura prywatna ze zwiększoną skalowalnością. Dlatego współpracujemy z IBM, aby stworzyć pierwsze w branży rozwiązanie, chmury zewnętrznej, które stawia wymagania dotyczące odporności danych, prywatności i bezpieczeństwa informacji o klientach na czele procesu decyzyjnego*".

Centrum rozwoju IBM Cloud™ for Financial Services współpracowało z Bank of America i konsultingową Promontory Financial Group, należącą do IBM jednostką biznesową IBM Services i światowym liderem w doradztwie dotyczącym zgodności z przepisami związanymi z usługami finansowymi. IBM Cloud Policy Framework dla usług finansowych jest już dostępny i zapewnia oparty na wiedzy branżowej mechanizm kontroli chmury publicznej IBM, wymagany do bezpiecznego działania z danymi wrażliwymi banków w chmurze publicznej.

Współpraca IBM z CaixaBank

Niedawno, bo 15 września 2021 r. IBM ogłosił swój pierwszy region IBM Cloud Multizone Region (MZR) w Hiszpanii oraz poinformował o nowej umowęie z CaixaBank, główną hiszpańską grupą finansową. IBM jest partnerem technologicznym CaixaBank od ponad 50 lat, a w ramach nowej umowy CaixaBank uruchomi projekt CloudNow. Hybrydowa chmura IBM i rozwiązania sztucznej inteligencji pomogą bankowi wzmocnić jego model biznesowy i poprawić jakość obsługi klienta. W ramach umowy Kyndryl, nowa, niezależna spółka publiczna, która zostanie utworzona po rozdzieleniu działalności IBM Managed Infrastructure Services, pomoże CaixaBank w integracji nowego modelu chmury hybrydowej, a bank wykorzysta doświadczenie branżowe IBM Global Business Services.

MUFG Bank prowadzi wdrożenie rozwiązania IBM Cloud™ for Financial Services w Japonii, a kataloński Banco Sabadell w Hiszpanii. To nie koniec przyłączania się kolejnych instytucji do stale rozwijanych i udoskonalanych rozwiązań chmurowych IBM.

Na swoim blogu, **Howard Boville** z IBM zauważył, że dzięki podejściu przez firmę do wykorzystania chmury hybrydowej, modernizacja nie odbywa się kosztem dotychczasowych inwestycji w IT ani bezpieczeństwa danych, a wysuwa je na pierwszy plan. Podobnie jak nowe budynki w Rzymie, możemy budować w istniejącym środowisku na starożytnych fundamentach z dodatkowymi strukturami i wzmocnieniami. To pozwala nam bezpiecznie kontynuować podróż w ramach cyfrowej transformacji teraz i w przyszłości. •

Fot. blackboard/stock.adobe.com

Chmura z efektem biznesowym

Organizacje działające w obszarze rynków i usług finansowych, a zwłaszcza banki, poddawane są ciągłej presji różnego rodzaju transformacji. To efekt zmian na rynku, nowych regulacji, nowego spojrzenia na rynek pracy przez pracowników banków a przede wszystkim nowych zachowań konsumentów. Nowe oczekiwania klientów to klucz do zrozumienia tych zjawisk, które dotykają banki, a które implikują konieczność modyfikacji usług finalnie dostarczanych właśnie klientom oraz bardzo często modelu ich oferowania czy zupełnie innych ich parametrów.

Fot. PwC

Przemysław Galiński
DYREKTOR, PWC POLSKA

Nowe pokolenia klientów chcą w dużej mierze inaczej podchodzić do banków jako instytucji, niż pokolenia ich rodziców, które korzystały z tych usług jeszcze dziesięć czy dwadzieścia lat temu. Jedną z podstawowych zmian jest oczekiwanie tzw. podejścia 360 stopni, a więc uwzględnienia indywidualnej, unikalnej charakterystyki każdego klienta, jego wymagań i oczekiwań, specyfiki sytuacji materialnej, miejsca w którym żyje - łącznie ze statusem społecznym i otoczeniem (środowiskiem), w którym funkcjonuje. To wszystko sprawia, że przed organizacjami finansowymi stoi szereg wyzwań, których wcześniej nie musiały uwzględniać aż w takim stopniu. A przynajmniej nie w takim stopniu z uwagi na nie tak mocno nasycony i konkurencyjny rynek jak ma to miejsce teraz.

Nie bez znaczenia jest, że pojawiają się również obszary wpływu i konieczność zmian, które historycznie nigdy wcześniej nie miały miejsca – jak pandemia, która zmieniła postrzeganie i oczekiwania stawiane instytucjom finansowym, w tym choćby prawdziwej omnikanałowości, czyli w pełni cyfrowej bankowości świadczonej niezależnie od miejsca i czasu.

Ponadto zwiększył się poziom wymagań klientów. Wynika on z aktywnego działania konkurencyjnego klasycznych instytucji finansowych, a więc m.in. innych banków, ale również fintechów, które bardzo szybko potrafią zaadresować oczekiwania klientów. Wychodząc na rynek z komunikatem, że potrafią z większą lub mniejszą skutecznością przewidywać trendy oraz obszary, które wkrótce pojawią się na rynku, a już dziś są w domenie zainteresowań konsumentów a więc klientów.

Polski rynek finansowy jest na poziomie technologii jednym z dynamicznie się rozwijających. Powoduje to, że mamy do czynienia z dość dobrze działającą, rozpędzoną maszyną, której zmiana lub modyfikacja nie jest łatwa, a jest potencjalnie kosztowna. Na szczęście menedżerowie banków obserwując bardziej dojrzałe rynki mają świadomość konieczności zmiany. Przed nami jeden z większych historycznie przełomów, który porównałbym do choćby przejścia z systemów papierowych na elektroniczne.

Technologia

Technologia staje się imperatywem każdej organizacji, a cloud imperatywem strategii technologicznej. Idąc tym tropem można przyjąć założenie, które łatwo potwierdzić analizując i obserwując dojrzalsze rynki, że adaptacja technologiczna i chmurowa stanowią jeden z głównych czynników wspierających i umożliwiających głęboką transformację organizacji. Tak dzieje się już w instytucjach finansowych na naszym rynku. Każdy kto działa z instytucjami finansowymi może potwierdzić, że właściwie nie pozostał żaden bank, który obecnie nie testuje, wdraża i w mniejszym lub większym zakresie nie używa chmury obliczeniowej lub nie korzysta z rozwiązań klasy software as a service. Pracując na rynku nowych technologii przez kilkanaście lat, nigdy wcześniej nie zaobserwowałem takiej liczby ambitnych, a przy tym bardzo ciekawych projektów digitalizacyjnych jak ma to miejsce teraz. Jako eksperta od chmury i równocześnie klienta banków napawa mnie to uzasadnionym optymizmem.

Adaptacja chmury

Oczywiście jeden projekt adaptacji chmury nie jest równy drugiemu. Zanim banki globalnie zaczną masowo przenosić swoje systemy centralne do chmury (choć zaczyna się to powoli dziać) albo zastąpią je rozwiązaniami, które bazując technologicznie na chmurze będą miały inną logikę działania (choć podobną funkcję biznesową) to minie jeszcze trochę czasu. Jednakże już teraz takie prace trwają, także na naszym polskim rynku.

Z punktu widzenia PwC, można zaobserwować kilka rodzajów aktywności. Są to m.in. testowanie rozwiązań opartych na chmurze (w obszarze usług dostępnych na platformach PaaS i SaaS dostawców cloud), implementacja rozwiązań chmurowych stanowiących systemy istotne, ale nie kluczowe dla banków – np. implementacja narzędzi typu modern workplace (narzędzi do pracy biurowej, komunikacji IM itp.) oraz podejście do „ciężkich" systemów bankowych w celu ich ewentualnej modernizacji, lub zmiany w kierunku migracji do chmury lub szerokiej w zakresie transformacji. To tylko przykłady stanowiące wycinek tego, co można obserwować w bankowości w zakresie chmury, jednak oddające charakterystykę trwających aktywności. W większym lub mniejszym stopniu takie działania są prowadzone we wszystkich polskich bankach, bez wyjątku, na coraz większą skalę.

Dlaczego banki chcą wykorzystywać chmurę i dlaczego muszą?

Jednym z kluczowych, wspomnianych już czynników jest uzasadnienie biznesowe. Upraszczając, zmieniają się oczekiwania klientów (wewnętrznych i zewnętrznych) i organizacja powinna być w takim stopniu gotowa i elastyczna, aby sprostać im w możliwie szybkim czasie. Żeby się to stało, w banku powinien zostać określony obszar kompetencyjny oraz gotowość technologiczna do szybkiego, elastycznego, bezpiecznego i efektywnego kosztowo tworzenia, testowania, uruchamiania, a później utrzymywania rozwiązań (systemów, aplikacji, workloadów), które będą zaspokajały potrzeby klientów, oferując im określone produkty. To właśnie chmura (w obszarze technologii) może zaadresować te wszystkie wymagania. Oczywiście nie jest to jedyny czynnik – tutaj mówimy tylko o technologii – bo równie ważny jest czynnik ludzki, czyli gotowość zespołów i obszarów odpowiadających za kompetencje IT banku do wykorzystania tej technologii, adaptacja zmiany czy też świadomość ograniczeń kompetencyjnych, z którymi będziemy się mierzyć.

Podsumowując, tylko chmura (jako ogromny, elastyczny i niemal nieskończenie skalowalny zasób informatyczny) może efektywnie zaoferować fundamenty tego wszystkiego, co jest niezbędne do dostarczenia klientom tego, czego finalnie oczekują. Nigdy wcześniej takiej możliwości nie było, a jeśli się pojawiała to była nieporównywalnie bardziej kosztowna w adaptacji.

Czy sama platforma chmurowa to wszystko, co jest niezbędne do implementacji cloud?

Na tak zadane pytanie można odpowiedzieć jednoznacznie – nie. Chmura (jako sama technologia) jest składnikiem koniecznym, ale tylko jednym z wielu w procesie transformacji. Często też jest katalizatorem większych zmian następujących

w obszarze biznesu. Jako PwC dostrzegliśmy wiele wyzwań w projektach chmurowych, a ich część wynika z czynników innych niż stricte IT – choć te są dominujące. Dlatego też jako jedna z nielicznych firm na świecie potrafimy dostrzec, a także zaadresować, proces adaptacji uwzględniający wszystkie takie elementy, bez wyjątku. W naszej unikalnej metodyce adaptacji chmury uwzględniamy WSZYSTKIE czynniki wpływające na projekt.

Mieszczą się one w zakresie trzech obszarów:

- **Technologia** – tutaj nie ma wątpliwości, powinna być wystarczająco wydajna, bezpieczna, optymalna kosztowo i najlepiej dopasowana do SPECYFICZNYCH wymagań danej organizacji. Zarówno zespoły wewnętrzne, jak i dostawcy, partnerzy wdrożeniowi powinni cechować się możliwie najwyższymi interdyscyplinarnymi (w obszarze technologii IT i cloud) umiejętnościami, tak aby móc wykorzystać cały potencjał chmury. W tej (oraz poniższej, biznesowej) części mamy do czynienia także z ewentualnym opracowaniem lub dostosowaniem istniejącego modelu operacyjnego, który musi być przystosowany do funkcjonowania z zupełnie innym modelem korzystania z usług charakteryzowanych jako „as a service" (usług, których odbiorcami jest biznes banku a potem klienci końcowi). Bez zaadresowania tego elementu potencjalne wdrożenie będzie mieć o wiele niższy wpływ na naszą organizację, ergo przyniesie o wiele mniejsze korzyści i uzysk.
- **Regulacje/prawo** – to krytyczny obszar w projektach implementacji chmury. Z uwagi na wysokie wymagania regulacyjne, charakterystyczne nie tylko dla Polski, specyfikę branży oraz obowiązki spoczywające na organizacji wdrażającej tę technologię, jest to miejsce, które powinno być uwzględnione w kontekście wsparcia już od samego początku projektu i/lub programu chmurowego. Rozszerzeniem tego obszaru jest cloud security – a więc obszar odpowiadający za technologiczne bezpieczeństwo, ale również to wynikające z wymagań właśnie regulacyjnych.
- **Biznes** – stanowi kolejny krytyczny czynnik w implementacji cloud. Chmura sama w sobie nie stanowi wystarczającej wartości, a nabywa ją dopiero wtedy, gdy przynosi wartość biznesową samej organizacji (a dalej klientom). To tu następuje uwzględnienie wszystkich wymagań biznesowych i to tutaj możemy przewidzieć i określić, czy i w jaki sposób chmura wpłynie na naszą organizację w przyszłości i to, w jaki sposób może wzmocnić np. naszą przewagę konkurencyjną, wpłynąć na zyski czy np. wycenę giełdową. Tu widzimy przyszłość albo przynajmniej staramy się dostrzec przyszłość naszej organizacji i jej miejsce względem choćby konkurencji.

Te wszystkie trzy obszary są przez nasz zespół ekspertów PwC określane jako „DNA projektu chmurowego" i w tym zakresie każdy projekt wdrożeniowo-implementacyjny powinien być sparametryzowany, a potem wsparty, żeby na końcu móc ocenić jego efektywność.

Bazując na projektach, które realizowaliśmy, to właśnie zaadresowanie czy uwzględnienie tych trzech elementów wyraźnie zwiększa prawdopodobieństwo sukcesu projektu, implementacji, modernizacji lub migracji do chmury. Naszym doświadczeniem rekomendujemy wprost takie budowanie projektów chmurowych, aby objąć każdy z nich, choć oczywiście zarówno nakład pracy, jak i koszty nie są proporcjonalnie rozłożone. Często charakteryzuje się to tym, że np. technologia z punktu widzenia wielkości projektu, jego skali i kosztów angażuje 60% zasobów (i kosztów), regulacje i bezpieczeństwo 30%, a część biznesowa kolejne 10%. Wszystko zależy od wymagań stawianych projektowi i sytuacji w samej organizacji.

Jak zacząć? Co jest jeszcze ważne?

Z punktu widzenia rozpoczęcia projektu chmurowego jednym z pierwszych kroków jest opracowanie i przedstawienie strategii technologicznej organizacji (często strategii cloud) będącej rozwinięciem lub kontynuacją strategii biznesowej organizacji. Powinny one mieć zbliżone, a często tożsame fundamenty i na pewno nie być przeciwstawne. Nadrzędne i wspólne cele to klucz do powodzenia. Następnie konieczne jest przeanalizowanie organizacji w za-

Tab. 1. Model dojrzałości na obszar

Focus area	Level 1	Level 2	Level 3	Level 4	Level 5
Active Knowledge	No skilled resources	Skilled resources	Skilled resources + 1 additional	Skilled resources + 2 additional 4	Skilled resources + 3 additional 4
Application Life Cycle Management	Waterfall	Iterative	Agile	DevOps	SecDevOps
Application Design	Monolith	Decoupled	Loosely Coupled	Containers	Microservices
Technology Configuration	Closed System	Open System	Infrastructure as a Service	Platform as a Service	Serverless / Software as a Service

Źródło: https://www.pwc.nl/nl/financial-services/assets/pdf/pwc-whitepaper-legacy%20modernization-2020.pdf

Fot. kras99/stock.adobe.com

kresie posiadanych kompetencji i ewentualnie dojrzałości organizacyjnej w kontekście adaptacji chmury. Ciekawym podejściem jest analiza dojrzałości organizacyjnej uwzględniająca kilka obszarów.

Istotne z punktu widzenia technologii chmurowej jest także zbudowanie tzw. Cloud Competency Center, czyli centrum kompetencji chmurowych. Jest to obszar w organizacji (wykraczający poza silosy kompetencyjne IT), który zbierze posiadane kompetencje cloud, zinwentaryzuje je, a następnie będzie gotowy do opracowania i pozyskiwania nowej, specyficznej wiedzy, która umożliwi IT (przede wszystkim) operowanie w nowym modelu usługowym. Jest to także istotne z punktu widzenia zaadresowania szeroko pojętego HR, czyli pozyskania talentów (co w obecnej sytuacji na rynku pracy nie jest zadaniem prostym) utrzymania posiadanych i modernizacji istniejących już kompetencji ludzi i zespołów. Tutaj także powinno nastąpić zaadresowanie obaw ludzi związanych z nadchodzącą niewątpliwie dużą zmianą organizacyjną.

Najlepsze praktyki, czyli dlaczego zewnętrzne wsparcie jest często niezbędne?

Z punktu widzenia banku i jego celów jako organizacji finansowej mamy do czynienia ze świadczeniem usług finansowych (i nie tylko) dla klientów. Jest to nadrzędny cel organizacji (stawiany wprost przez właścicieli np. giełdę) – oczywiście nie bez znaczenia pozostają wymagania takie jak wzmacnianie stabilności systemu finansowego danego kraju i/lub krytyczna rola organizacji zaufania publicznego. Jednakże upraszczając, biznesowo organizacja ma świadczyć usługi finansowe w sposób bezpieczny i pewny, a w zamian za to otrzymuje stosowne wynagrodzenie (od swoich klientów czy rynku) generując zysk dla właścicieli. Do funkcjonowania tak złożonego przedsiębiorstwa potrzeba różnego rodzaju kompetencji i zasobów, także informatycznych. Bez wątpienia wiedza i kompetencje dotyczące chmury są niezbędne do wykonywania w obecnych czasach usług, które świadczą nowoczesne działy IT, ale każda organizacja powinna odpowiedzieć sobie na pytania: czy lepiej pozyskać, nabywać i budować kompetencje, które będą potrzebne w danym momencie? Może też warto utrwalić te, które pomogą organizacji funkcjonować w nowym, chmurowym modelu, a dla ograniczenia czasu, w którym następuje transformacja (migracja do chmury), posiłkować się zasobami zewnętrznymi, które w przyszłości nie będą już wykorzystywane w takim zakresie?

W PwC z uwagi na specyficzną rolę niezależnego, agnostycznego z punktu widzenia technologii i vendorów, dostawcy rozwiązań i usług profesjonalnych, koncentrujemy się przede wszystkim na celu biznesowym organizacji. Dlatego uzasadnione pozostaje stwierdzenie, że migracja banku jako dużej, złożonej organizacji do chmury, która dzieje się prawdopodobnie

jeden raz na wiele lat powinna być realizowana przede wszystkim najlepszymi zasobami, jakie są możliwe do pozyskania i wykorzystując najlepszych specjalistów. Tutaj konieczne jest ograniczenie do minimum ryzyk takich, jak np. niedostępności systemów dla klientów czy utrata danych. Idąc dalej, zasoby (specjaliści, eksperci) posiadające specyficzną, często też unikalną wiedzę i co najważniejsze doświadczenie niezbędne np. do przystosowania aplikacji do migracji (niezależnie czy mówimy o migracji typu lift & shift czy o głębokiej zmianie w samej strukturze aplikacji lub architekturze, czyli o re-engineeringu) i są wykorzystywane tylko raz w danym momencie albo projekcie.

> *Sama chmura bez kontekstu i uzasadnienia biznesowego nie niesie większej wartości. Natomiast chmura z efektem biznesowym może podnieść naszą organizację do poziomu, którego konkurencja nie będzie mogła osiągnąć, a na pewno nie tak szybko.*

Pozyskanie ich z rynku jest obecnie wyjątkowo kosztowne i trudne. Następnie taki zasób potencjalnie nie będzie już wykorzystywany w pełnym zakresie swoich, jak wspomniałem, specyficznych kompetencji. Dlatego też najrozsądniejszym kosztowo, ale także technologicznie, pozostaje korzystanie z zewnętrznych zasobów, firm specjalizujących się w takich pracach, a następnie uzyskanie niezbędnej wiedzy przez zespoły banku. Równie istotne jest wykorzystanie specyficznych, gotowych i unikalnych metodyk stosowanych choćby przez PwC, które zostały wypracowane przez lata doświadczeń oraz często setki zrealizowanych z sukcesem projektów – to kolejny element, który przynosi wymierne korzyści – czas i bezpieczeństwo.

Model ten jest z jednej strony optymalny kosztowo (w dłuższej perspektywie), a z drugiej potencjalnie najszybszy w implementacji. To stanowi ogromną zaletę zwłaszcza w czasie niewątpliwego wyścigu technologicznego, jaki trwa na rynku i konkurencji, która realizuje podobne działania prawdopodobnie w tym samym czasie, pozyskując ekspertów z tego samego rynku co my. Nie bez znaczenia jest fakt posiadania choćby takich zespołów, jak zespół ekspertów i praktyków PwC z pełnym spektrum kompetencji począwszy od budowania strategii, poprzez technologie, a skończywszy na obszarach bezpieczeństwa i regulacji prawnych.

Na co można liczyć wdrażając cloud?

Bazując na bogatym doświadczeniu realizowanych projektów implementacji chmury przez PwC dostrzegamy kilka głównych elementów. Nie wyczerpują one wszystkich benefitów, które pojawią się po i dzięki implementacji chmury w banku, ale mogą stanowić swojego rodzaju „must have" do osiągnięcia. Są to m.in.:

- **Elastyczność w wykorzystaniu zasobów informatycznych.** Zarówno w górę, jak i w dół, tzn. optymalizacja pod względem precyzyjnego dostarczenia tylu zasobów informatycznych (np. mocy obliczeniowej, pamięci itp.) ile jest w danej chwili niezbędnych. Mówimy tutaj praktycznie o niemal nieograniczonych możliwościach skalowania się.
- **Efektywność kosztowa**. Zgodnie z modelem pay as you go (lub innym wybranym dla chmury) płacimy za zasoby wykorzystane, niezaalokowane (oczywiście są od tej zasady pewne odstępstwa, ale dla potrzeb niniejszego opracowania pozwoliłem sobie je pominąć). Co implikuje oszczędności wynikające z tytułu niealokowania środków finansowych w zasób niebędący w danym momencie potrzebny (ograniczenie wynikające choćby z kosztów pieniądza w czasie). Warto dodać także zmianę modelu kosztowego z CAPEX na OPEX.
- **Prędkość i szybkość przede wszystkim uruchamiania rozwiązań a także m.in. testowania.** Dzięki dostępnemu bardzo szerokiemu portfolio nowego rodzaju rozwiązań i funkcji, dostępnych na platformach chmurowych (rozwiązania IoT, zaawansowana analityka, sztuczna inteligencja, blockchain, podejście API lub też dedykowane rozwiązania dla klientów sektora finansowego) zespoły IT mogą wdrażać szybko i potencjalnie tanio rozwiązania, które w chwili, w której odniosą określony sukces, mogą być łatwo skalowalne. Bazowanie na chmurze umożliwia także bardzo łatwe „zamykanie" zasobów i rezygnację z tychże (tutaj zgodnie z zasadą „fail fast").
- **Zarządzanie talentami w organizacji**. Wdrażanie chmury to często bardzo atrakcyjny, z punktu widzenia pozyskania i rozwoju kompetencji poszczególnych osób, obszar technologiczny. Co ma swój efekt w postaci potencjalnie łatwiejszego pozyskania ludzkich zasobów do naszej organizacji, a potem utrzymania ich w niej i wykorzystania wiedzy oraz kompetencji tych osób.

Unikalne obszary

Samo wdrażanie technologii cloud, niezależnie od tego, czy mówimy o przeniesieniu systemów SAP do chmury publicznej, uruchomieniu narzędzi komunikacyjnych (Modern Workplace) w chmurze

lub też wykorzystaniu różnego rodzaju chmur do zróżnicowanych celów biznesowych (podejście hybrid-cloud czy multicloud) jest bardzo często klasycznym projektem IT, ale nie realizowanym w sposób standardowy. Przede wszystkim charakterystyczna dla tego rodzaju projektów jest większa dynamika działań, a potencjalnie również ryzyko – choć zarządzalne. Ale są także elementy, których wcześniej nie było, a jeśli występowały to w nie tak dużym zakresie. Nigdy wcześniej determinacja wszystkich dostawców technologii (tu dostawców chmury) we wsparciu klientów nie była tak zauważalna, co może nieść określone wymierne korzyści dla samych banków. Odpowiednie zarządzanie dostawcami może wesprzeć projekt wdrożenia chmury w wielu aspektach jego realizacji.

Warto także uwzględnić gotowe metodyki i unikalne podejścia organizacji, które takie realizacje w dużej skali i dla wielu klientów mają już za sobą, a często doświadczenie budowały od wielu lat. Tutaj dobrym przykładem jest obszar PwC dotyczący kompetencji Cloud & Digital Transformation, z sukcesem realizujący kilkuetapowe podejście do modernizacji, migracji aplikacji lub też podejście przejścia organizacji do chmury w obszarze choćby samej infrastruktury informatycznej. A te elementy stanowić mogą pewnego rodzaju podwaliny do roadmapy migracji. Należy jednak pamiętać, że jest to tylko wycinek, choć bardzo istotny, całego obrazu cyfrowej transformacji.

Na takie metodyki składają się następujące kroki:

- **Zrozumienie zależności, złożoności i specyfiki oczekiwań biznesowych i technologicznych**, czyli sprawdzenie (analiza) środowisk IT (on-premises) oraz potencjalnie modelu operacyjnego, a także opracowanie wysokopoziomowego business case'u wraz z wymaganiami biznesowymi.
- **Identyfikacja wzorców rozwiązań i działań oraz opracowanie wysokopoziomowej roadmapy dalszych kroków** (np. projektu implementacji, migracji czy adaptacji chmury). Tutaj następuje także dopracowanie business case'u.
- **Potwierdzenie założeń oraz pryncypiów ŁĄCZNIE biznesowych i technologicznych**. W tym miejscu następuje synchronizacja ze wszystkimi strategicznymi inicjatywami w organizacji. Projekt chmurowy powinien wpisywać się (co nie znaczy, że nie może dominować) w inne inicjatywy technologiczne i biznesowe.
- **Działania w obszarze określenia i osiągnięcia tzw. quick-wins**. Mogą to być zauważalne, mierzalne elementy dotyczące szybkiego zabezpieczenia systemów banku (wynikające choćby z dużej skalowalności, która to z kolei zabezpieczy zasoby na wypadek bardzo dużych potrzeb w danym okresie), uruchomienie Disaster Recovery lub implementacja punktowych rozwiązań biznesowych (np. chatbota do obsługi klientów). Ograniczeniem jest tylko kreatywność zespołów banku lub partnera wdrożeniowego.
- **Realizacja działań zgodnie z planem oraz uruchomienie tzw. Digital PMO w celu zabezpieczenia odpowiedniej dynamiki projektu** oraz stałej kontroli wymagań biznesowych, technologicznych i/lub ekonomicznych dla projektu.

Powyższe jest tylko dużym uproszczeniem realizacji strategii implementacji chmury, ale w sposób wystarczający oddaje główne elementy składające się na taki program. Warto uwzględnić elementy, które pozwolą nam zabezpieczyć się i znacząco obniżyć ryzyko zawsze pojawiające się wszędzie tam, gdzie organizacja realizuje duże zmiany, zwłaszcza w obszarze technologii i wtedy, gdy ta dotyka wszystkich obszarów organizacji.

Podsumowując, chmura stała się krytycznym filarem projektów informatycznych każdego banku. Zarówno rozwiązania chmury prywatnej (uruchomionej w Data Center banku lub dedykowanych, wydzielonych galwanicznie lub logicznie zasobów u dostawcy chmurowego), a zwłaszcza chmury publicznej (realizowanej także coraz częściej w modelu multicloud, w którym wykorzystywani są określeni dostawcy do określonych zastosowań) stały się odpowiedzią na większość wymagań technicznych stawianych zespołom IT przez biznes.

Zdezaktualizowały się dyskusje dotyczące tego, czy chmura jest mniej bezpieczna niż rozwiązania on-premises. Uprawniona i nadal w mocy pozostaje polemika dotycząca zarządzania bezpieczeństwem w chmurze i zabezpieczania zgodności regulacyjnej dla implementacji chmury. Równie ważne są dyskusje dotyczące tzw. cloud economy. U podstaw stoi przede wszystkim wymaganie biznesowe, które determinuje działania i bardzo często alokuje zasoby finansowe w dany projekt. Dlatego tak ważne pozostają pryncypia, które powinny wskazywać chmurę nie jako projekt, a PROGRAM. To coś znacznie szerszego i większego, dotyczące i wpływające na każdy bez wyjątku obszar firmy. Dlatego tym bardziej warto go realizować z najlepszymi specjalistami, cechującymi się przede wszystkim agnostycznością, doświadczeniem, praktyką i gotowymi metodykami. Tylko taki zespół elementów może zagwarantować, że wdrożenie będzie szybkie, efektywne kosztowo i technologicznie, a przede wszystkim zapewni oczekiwany efekt biznesowy. Sama chmura bez kontekstu i uzasadnienia biznesowego nie niesie większej wartości. Natomiast **chmura z efektem biznesowym** może podnieść naszą organizację do poziomu, którego konkurencja nie będzie mogła osiągnąć, a na pewno nie tak szybko. •

Salesforce rozszerza swoją ofertę usług finansowych dla bankowości korporacyjnej i inwestycyjnej

Firma Salesforce (NYSE: CRM), globalny lider w dziedzinie CRM, ogłosiła wprowadzenie Corporate and Investment Banking for Financial Services Cloud – nowej technologii, która pomaga bankowcom i zespołom doradztwa transakcyjnego pogłębiać i zarządzać relacjami z klientem na jednej platformie oraz realizować transakcje z poszanowaniem prawa i prywatności konsumentów.

Jak pokazała pandemia, branże muszą szybko wprowadzać innowacje, aby utrzymać się na rynku. Usługi finansowe nie są tu wyjątkiem – bankowcy inwestycyjni potrzebują technologii cyfrowej, aby zwiększyć wydajność, budować i pogłębiać relacje z klientami oraz realizować więcej rentownych transakcji. Potrzebują również narzędzi, które usprawnią dostęp do danych o klientach, zintegrowanych w ramach jednej platformy.

Ponadto, ważna jest też kwestia bezpieczeństwa danych. Pracownicy zatrudnieni na stanowisku compliance officers, podczas wykonywania swoich codziennych obowiązków mają styczność z zawiłymi regulacjami i zasadami bezpieczeństwa, które mają za zadanie chronić wrażliwe dane, którymi operują. W przypadku wycieku lub niewłaściwego zarządzania takimi informacjami, reputacja banku mogłaby zostać mocno nadszarpnięta, co skutkowałoby utratą znacznej części klientów.

„Bankowcy potrzebują nowych sposobów na budowanie trwałych i prawdziwych relacji z klientami, które są możliwe dzięki rozwiązaniom opartym na danych" – powiedział **Jujhar Singh**, EVP i GM Salesforce Industries. „Corporate and Investment Banking for Financial Services Cloud dostarcza pracownikom instytucji finansowych narzędzi opartych na sztucznej inteligencji, które pozwalają wypełnić luki w obsłudze klienta. Dzięki tym innowacjom od Salesforce bankowcy mogą w pełni poświęcić się roli oddanych i zaufanych doradców dla swoich klientów, przyspieszając proces realizacji transakcji i zwiększając bezpieczeństwo poufnych danych, aby zapewnić zgodność z przepisami, na każdym etapie transakcji".

> *Dzięki specjalnie opracowanym funkcjom oraz możliwościom chmur Sales Cloud i Service Cloud, instytucje świadczące usługi finansowe mogą zwiększyć produktywność swoich pracowników, zdecydowanie przyspieszyć czas uzyskania przychodu i znacząco pogłębić zaufanie klientów przy każdej interakcji z nimi.*

„Pracujemy w wysoce konkurencyjnej i dynamicznej branży, która wymaga, aby nasi bankowcy mieli istotne informacje na wyciągnięcie ręki" – stwierdził **Tim LaLonde**, dyrektor operacyjny Bankowości Inwestycyjnej w Evercore. „Projektujemy i wdrażamy nasz Salesforce CRM, aby funkcjonował jako główny system bazy informacji o klientach dla naszych doradców, umożliwiając tym samym dostarczanie kluczowych porad dla naszych klientów, zawsze wtedy, gdy tego potrzebują".

Usługa Corporate and Investment Banking for Financial Services Cloud

Bankowość korporacyjna i inwestycyjna w chmurze Financial Services Cloud została zaprojektowana tak, aby dostarczać kompletne doświadczenie w całym procesie obsługi klienta. Usługa jest zintegrowana z Tableau CRM i Einstein Relationship Insights (ERI), aby zapewnić pracownikom banku usługę skrojoną na miarę ich potrzeb. Dzięki tym rozwiązaniom zapewniana jest:

- **Maksymalizacja efektywności i produktywności bankowców**. Bankowcy inwestycyjni mogą zarządzać całym cyklem „życia" transakcji, śledząc działania podejmowane

w jej ramach na jednej platformie. Wykorzystanie narzędzi Salesforce Low Code pomaga zautomatyzować procesy realizacji transakcji związanych z fuzjami i przejęciami, pozyskiwaniem kapitału i restrukturyzacją przedsiębiorstw. Dzięki możliwościom Tableau CRM for Financial Services bankowcy mogą wykorzystywać analitykę transakcji do optymalizacji jej przebiegu i zaangażowania klientów, mając bowiem dostęp do danych o klientach z poprzednich wizyt, ofert i notatek ze spotkań – wszystko w jednym miejscu i z dostępem z dowolnego urządzenia.

- **Odkrywanie relacji za pomocą narzędzia badawczego opartego na sztucznej inteligencji**. ERI to nowe narzędzie do budowania relacji zintegrowane z Financial Services Cloud. Narzędzie to automatycznie wyszukuje osoby lub firmy wspomniane w źródłach takich, jak informacje prasowe, artykuły lub wiadomości e-mail, aby szybciej filtrować informacje i odkrywać możliwości nawiązania nowych kontaktów. Przykładem może być sytuacja, w której pracownik banku chce przedstawić się nowemu klientowi, wtedy system ERI przeszukuje dane i informacje w sieci, takie jak na przykład ogłoszenia o nowym członku zarządu lub przynależność do danej organizacji. Będąc w posiadaniu takich informacji pracownik może lepiej poznać swojego klienta i jego potrzeby.
- **Zapewnienie funkcji compliance**. Banki inwestycyjne mogą zachować zgodność z przepisami prawa, umowami i aktami wewnętrznymi poprzez zapewnienie, że wrażliwe dane dotyczące klientów lub transakcji są udostępniane wyłącznie odpowiednim interesariuszom. Na przykład, jeśli pracownik zajmuje się transakcją dotyczącą fuzji lub przejęcia przedsiębiorstwa, to dane dotyczące tego przedsięwzięcia nie zostaną udostępnione stronom trzecim i nie trafią w niepowołane ręce. Bankowiec może również zainicjować proces onboardingu klienta z poziomu platformy Salesforce i śledzić jego przebieg za pomocą dostępnych rozwiązań partnerskich.
- **Wykorzystanie danych jako przewaga konkurencyjna.** Bankowcy często muszą logować się do siedmiu lub ośmiu systemów, aby uzyskać dostęp do informacji istotnych dla ich sprawy. Obecnie, dzięki nowoczesnemu rozwiązaniu mogą integrować wewnętrzne dane z zewnętrznymi, pochodzącymi od partnerów – takich jak S&P Global, w celu uzyskania pełnego profilu swoich klientów. System Salesforce umożliwia wgląd w takie informacje, jak wycena działalności handlowej od S&P Global, przychody, wynagrodzenie pracowników i inne, bez konieczności przełączania się z systemu do systemu.

„Bankierzy inwestycyjni spędzają dziś nadmierną ilość czasu, próbując zebrać informacje potrzebne do przygotowania pitch decków, raportów, zarządzania transakcją i śledzenia procesów compliance" – zauważył **Spencer Mindlin**, analityk branży rynków kapitałowych, Aite Group. „Aby rozwiązać ten problem, banki muszą zastosować automatyzację i sztuczną inteligencję w celu usprawnienia procesów związanych z planowaniem, zbieraniem informacji, zarządzaniem transakcjami i operacjami prawnymi. Te innowacje są kluczem do utrzymania konkurencyjności, ponieważ uwalniają pracowników od rutynowych działań, dzięki czemu mogą oni poświęcać więcej czasu klientom".

Największe instytucje bankowe już wykorzystują Salesforce do pogłębiania kontaktów ze swoimi klientami:

- **Evercore**, wiodąca na świecie niezależna firma doradcza z zakresu bankowości inwestycyjnej, dostrzegła wartość, jaką platforma technologiczna może wnieść do jej działalności. Wybrała ona platformę Salesforce, aby stworzyć bezpieczne, scentralizowane rozwiązanie, które zapewni dostęp do istotnych informacji o klientach. Jako klient, Evercore będzie korzystać z innowacji dostarczanych przez Corporate and Investment Banking for Financial Services Cloud, skupiających się na mapowaniu relacji z klientami, współpracy wewnętrznej i innych funkcjach zaprojektowanych specjalnie w celu zapewnienia bardziej spersonalizowanego doświadczenia.

Fot. Salesforce Poland

Piotr Mroziński
FINANCIAL SERVICES INDUSTRY LEADER
SALESFORCE POLAND

Transformacja cyfrowa w polskich bankach ma charakter ciągły. Wielu naszym klientom nie chodzi już tylko o to, aby nadążyć za swymi potrzebami, ale je w znacznym stopniu wyprzedzić. Salesforce Financial Services Cloud jest rozwiązaniem dedykowanym dla sektora finansowego, które pozwala zaadresować bezpośrednio kluczowe obszary w bankowości czy ubezpieczeniach. Dla wielu naszych klientów stworzenie spójnego, bezpiecznego i rozwojowego ekosystemu stało się priorytetem – zaczynając od analityki i hyperpersonalizacji w bankowości detalicznej, poprzez relacyjność w segmencie MŚP czy korporacyjnym, a kończąc na demokratyzacji danych organizacji. Salesforce staje się zaufanym partnerem, który kompleksowo wspiera całościowy proces przejścia do chmury, dostarczając kluczową platformę łączącą instytucje finansowe z ich klientami.

- **TD** jest jednym z największych banków w Ameryce Północnej. W ramach swojej strategii technologicznej, buduje ujednolicone doświadczenie bankowe, wykorzystując platformę Salesforce we wszystkich swoich placówkach. W TD Securities wdrażane jest kompleksowe rozwiązanie CRM oparte na platformie Salesforce, które ma pomóc w dostarczaniu klientom wiodących produktów i zaufanych porad.
- **Moelis & Co.** To niezależny bank inwestycyjny o zasięgu globalnym, który świadczy usługi doradztwa finansowego dla korporacji, rządów i sponsorów finansowych. Dzięki Salesforce Moelis & Co. jest w stanie lepiej usprawnić procesy bankowe. Dzięki aplikacji typu mobile-first pracownicy są na bieżąco informowani o ostatnich działaniach klientów, ale także mają dostęp do danych gromadzonych pasywnie. Dzięki tej technologii bankierzy mają lepszy wgląd w relacje z klientami w całej firmie, co pozwala im lepiej współpracować i być na bieżąco w kontaktach z klientami.

Rozszerzenie bankowości korporacyjnej i inwestycyjnej poprzez Salesforce Partner Ecosystem

Salesforce posiada rozbudowany ekosystem partnerski, który zapewnia unikalną wiedzę i rozwiązania dla instytucji finansowych na całym świecie. Partnerzy ISV, tacy jak S&P Global Market Intelligence i Fenergo, rozszerzają i stanowią wartość dodaną dla chmury Financial Services Cloud. Dodatkowo, partnerzy konsultingowi KPMG, Silverline i VASS są ekspertami w dziedzinie bankowości korporacyjnej i inwestycyjnej oraz są przygotowani do wdrażania rozwiązań z zakresu usług finansowych dostosowanych do indywidualnych potrzeb klientów.

Informacje o Financial Services Cloud

Usługa Financial Services Cloud, zbudowana na platformie CRM nr 1 na świecie, umożliwia instytucjom finansowym budowanie zaufania poprzez ujednolicenie obsługi klienta we wszystkich kanałach, regionach geograficznych i biznesach. Dzięki specjalnie opracowanym funkcjom oraz możliwościom chmur Sales Cloud i Service Cloud, firmy świadczące usługi finansowe mogą zwiększyć produktywność pracowników, przyspieszyć czas uzyskania przychodu i pogłębić zaufanie klientów przy każdej interakcji. Więcej informacji o Salesforce Financial Services Cloud – https://www.salesforce.com/products/financial-services-cloud/overview/. •

We BRING FINANCIAL SERVICES *and* LOYAL CUSTOMERS TOGETHER

Hi, we're Salesforce. We help companies unify marketing, sales, service, commerce, and IT on the #1 CRM platform, so you can give every customer the personal experiences they love. Visit https://www.salesforce.com/FINS

salesforce