EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
ul. Do Studzienki 63
80-227 Gdańsk

tel. 58 524 49 01
fax. 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Synteza odpowiedzi ekspertów w prowadzonym przez Europejski Kongres Finansowy[1] badaniu dotyczącym interpretacji i stosowania regulacji odnośnie do outsourcingu w sektorze bankowym w Polsce.

Badanie przeprowadzono w związku z niepewnością regulacyjną i wątpliwościami interpretacyjnymi dotyczącymi równoczesnego stosowania prawa bankowego oraz Wytycznych EBA w zakresie zasad stosowania outsourcingu w sektorze bankowym.

Metodologia opracowania stanowiska

Opracowanie stanowiska przebiegało w następujących etapach.

Etap 1 (wrzesień 2020)
Przygotowano zestaw pytań konsultacyjnych. Do wzięcia udziału w badaniu zaproszono grupę ekspertów współpracujących z EKF, którym przesłano pytania konsultacyjne. W zaproszeniu eksperci zostali poproszeni o wzięcie pod uwagę trzech reżimów prawnych: obowiązujących ustaw regulujących sektor finansowy, w tym przepisów prawa bankowego, wytycznych KNF (m.in. Rekomendacji D, Komunikatu dotyczącego korzystania przez podmioty nadzorowane z usług chmury obliczeniowej z 23 stycznia 2020 r.) oraz Wytycznych EBA w sprawie outsourcingu wydanych w dniu 25 lutego 2019 r. wraz z praktyką ich interpretowania i stosowania w Unii Europejskiej. Ekspertom zagwarantowana została anonimowość.

Etap 2 (październik 2020)
Na zaproszenie EKF wpłynęło 17 opinii (od indywidualnych ekspertów oraz grup ekspertów i instytucji). Wszystkie odpowiedzi zostały zebrane i przedstawione w formie anonimowej ekspertom, którzy wzięli aktywny udział w konsultacjach. Zwrócono się do nich z prośbą o zaznaczenie w opiniach innych uczestników badania tych sformułowań, które powinny znaleźć się w stanowisku końcowym, jak również tych, z którymi się nie zgadzają. Eksperci mogli także skorygować swoje odpowiedzi pod wpływem argumentów przedstawionych przez innych ekspertów.

Odpowiedzi uzyskano od ekspertów reprezentujących:

- banki,
- firmy IT, fintechy oraz instytucje infrastruktury rynku finansowego
- firmy konsultingowe
- kancelarie prawne

Etap 3 (październik 2020)
Na bazie uzyskanych odpowiedzi i uwag ekspertów opracowane zostało syntetyczne stanowisko Europejskiego Kongresu Finansowego zaprezentowane poniżej. W końcowej części syntezy przedstawiono postulaty zgłoszone przez ekspertów uczestniczących w badaniu, a także podniesione przez nich wątpliwości i pytania, które wymagają odpowiedzi ze strony regulatora.

[1] Celem Europejskiego Kongresu Finansowego (www.efcongress.com) jest debata nt. bezpieczeństwa i stabilności systemu finansowego Unii Europejskiej i Polski.

P1: Czy i jak powinno się badać czy dostawca usługi lub jego podwykonawcy korzystają z rozwiązań chmurowych?

Ciążący na banku obowiązek zbadania, czy dostawca usługi lub jego podwykonawcy korzystają z usługi chmury obliczeniowej wynika z licznych wymagań nałożonych na bank w związku z outsourcingowaniem do chmury danych (Wytyczne EBA, Komunikat UKNF). W razie zaniechania tego badania analiza ryzyka związana z outsourcingiem byłaby niepełna. Dotyczyłoby to w pierwszym rzędzie oceny zgodności z wymaganiami RODO, wytycznymi regulatorów, skali ryzyka utraty dostępu do danych oraz analizy ryzyka geograficznego. Bank, który nie jest pewien, jakie technologie będą miały zastosowanie przy świadczeniu usług, zwłaszcza gdy przedmiotem umowy ma być outsourcowanie przechowywania danych, powinien szczegółowo zbadać, czy dostawca korzysta lub zamierza korzystać z chmury obliczeniowej już na etapie negocjacji przed zawarciem umowy. W razie braku pewności co do zastosowania w procesie chmury obliczeniowej, należy założyć, iż dostawca, świadcząc usługi, będzie korzystał z chmury i w związku z tym stosować wszystkie odnoszące się względem niego obowiązki, w tym analizę ryzyka i modelowanie tak zwanej strategii wyjścia. Gdyby w trakcie weryfikacji okazało się, że usługa świadczona jest z wyłączeniem zastosowania chmury obliczeniowej – bank zaniecha wykonywania dalszych obowiązków związanych z wdrożeniem właściwych regulacji.

Deklaracje dostawcy usług i – ewentualnie – jego podwykonawców, powinny stanowić załącznik do umowy głównej, lub być częścią samej umowy. Dostawca, który świadczy usługi na podstawie już uprzednio zawartej umowy, powinien złożyć stosowne oświadczenie, w którym stwierdza czy, a jeśli tak, to w jakim zakresie, korzysta z rozwiązań chmurowych. W przypadku odpowiedzi twierdzącej, jeżeli korzystanie z rozwiązań chmurowych uzasadniałoby stosowanie postanowień Komunikatu KNF, w celu kontynuowania dalszej współpracy z dostawcą powinien zostać zawarty aneks do umowy w celu dostosowania jej treści do wymagań Komunikatu KNF.

Proces weryfikacji można podzielić na kilka wątków. Pierwszym jest ankieta skierowana do dostawcy, w której oświadcza on, w jaki sposób zamierza wykonywać czynności powierzone, wskazując jednocześnie wszystkich podwykonawców ze szczególnym uwzględnieniem realizowanego zakresu i wykorzystywanych technologii chmurowych. Rolą zamawiającego jest zweryfikowanie partnera pod względem ryzyka i w zależności od poziomu zaufania lub pozycji rynkowej, potwierdzonej referencjami, albo przystąpić do audytu zakresu powierzanego w umowie, albo odstąpić od niego, świadomie akceptując przedstawione certyfikaty, a w konsekwencji ewentualne ryzyko, które z takiego odstąpienia może wynikać.

Pozyskiwanie oświadczenia dostawcy o korzystaniu lub zamiarze korzystania z rozwiązań chmurowych, jak również kontrole lub audyty dostawcy, mogą być realizowane przez cykliczne wzywanie dostawcy do odpowiedzi na pytania zawarte w szczegółowej ankiecie, dotyczącej sposobu i warunków przetwarzania przez dostawcę powierzonych przez bank danych. W uzasadnionych przypadkach audyty powinny być przeprowadzane osobiście w lokalizacjach przetwarzania powierzonych danych przez dostawcę.

W przypadku umów istotnych sposób ewentualnego korzystania z chmury powinien być jasno opisany w umowie z dostawcą lub dokumentach z nią powiązanych. W przypadku pozostałych umów (tj. nieistotnych) kwestia ewentualnego wykorzystania chmury przed dostawcę powinna być z nim wyraźnie wyjaśniona, jeśli może mieć to wpływ na poziom ryzyka związany z umową np. kwestie ochrony danych, czy bezpieczeństwo danych i systemów.

Nie mniej ważnym obowiązkiem jest też zweryfikowanie planów wyjścia z usług w przypadku zakończenia współpracy i tego co dalej dzieje się z danymi, a także możliwości dalszego zlecania podwykonawstwa przez dostawcę. Równie ważne jest też sprawdzenie, czy powierzane dane są odpowiednio zabezpieczone przed nieautoryzowanym dostępem (np. poprzez szyfrowanie). Tego typu działania powinny być przedmiotem weryfikacji w momencie negocjacji umowy z dostawcą.

Do stałych działań w organizacji klienta powinna należeć cykliczna weryfikacja czy wdrożony w organizacji klienta proces wyłaniania dostawców oraz proces wypracowywania wymagań do zamówień usług i produktów uwzględnia wszystkie oczekiwania organizacji. Szczególnie czy uwzględnia preferencje w zakresie podwykonawstwa pod kątem charakteru świadczenia usług w oparciu o zasoby własne lub obce (w tym chmurowe).

W przypadku decyzji o dopuszczeniu realizacji przedmiotu zamówienia przez wykonawcę/podwykonawcę z wykorzystaniem zasobów obcych (w tym chmurowym) należy przewidzieć analizę czynników ryzyka związanych z realizacją przedmiotu zamówienia – w tym zależności odpowiedzialności za realizację i regresu ewentualnych strat w przypadku problemów z wykonaniem umowy.

P2: Jakie rozwiązania na poziomie kontraktowym powinno się stosować w przypadku, w którym dostawca świadczący usługi w ramach outsourcingu bankowego korzysta z podwykonawców i dalszych podwykonawców?

Należy przyjąć że „outsourcing" jest pojęciem szerszym niż powierzenie wykonywania czynności w rozumieniu Prawa bankowego. Istnieje wobec tego możliwość, że dana umowa będzie kwalifikowana jako outsourcing zarówno z punktu widzenia prawa krajowego oraz Wytycznych EBA, jak również że będzie ona outsourcingiem wyłącznie na podstawie Wytycznych EBA.

Zgodnie ze Stanowiskiem KNF co do zasady należy stosować Wytyczne EBA, jako szerzej ujmujące omawiany obszar. Jednak w sytuacji, gdy przepisy krajowe, rekomendacje lub stanowiska interpretacyjne skierowane przez organ nadzoru do wszystkich banków zawierają postanowienia bardziej rygorystyczne, rozumiane jako wymagające zwiększonego wysiłku lub ograniczające swobodę działania banku w stosunku do postanowień Wytycznych EBA, należy stosować w danym przypadku przepisy krajowe, rekomendacje lub stanowiska interpretacyjne skierowane przez organ nadzoru do wszystkich banków. Natomiast, gdy przepisy krajowe, dotychczas wydane rekomendacje lub stanowiska interpretacyjne skierowane przez organ nadzoru do wszystkich banków zawierają postanowienia mniej rygorystyczne niż Wytyczne EBA, należy stosować w danym przypadku Wytyczne EBA.

Dodać także należy, że zgodnie ze Stanowiskiem KNF Wytyczne EBA nie mają zastosowania do usług chmurowych. W tym zakresie należy wziąć pod uwagę treść Komunikatu Chmurowego.

Co do zasady, rozwiązania wynikające z Prawa bankowego w zakresie pod-outsourcingu są dalej idące niż Wytyczne EBA ponieważ ograniczają możliwość korzystania z podwykonawców wyłącznie do wykonywania czynności pomocniczych lub sytuacji awaryjnych, uzależniając tę możliwość od jej wskazania w umowie.

W sytuacji więc gdy, dana umowa stanowi powierzenie wykonywania czynności w rozumieniu Prawa bankowego, a dostawca świadczyć ma usługi z wykorzystaniem podwykonawców, umowa musi wprost przewidywać taką możliwość, a czynności pomocnicze, które miałby wykonywać podwykonawca powinny zostać w umowie wskazane. Ponadto, bank powinien na etapie kontraktowania zapewnić sobie możliwość sprawowania kontroli nad outsourcowanymi czynnościami i nad informacjami stanowiącymi tajemnicę prawnie chronioną. Umowa powinna także zapewniać, że przy powierzeniu wykonywania czynności zostaną spełnione inne wymogi wynikające z Prawa bankowego oraz rekomendacji i wytycznych KNF.

Nadzór wymaga, by w przypadku, gdy umowa outsourcingu dopuszcza pod-outsourcing krytycznych lub istotnych funkcji, zapewniała ona również spełnienie wymogów wynikających z Wytycznych EBA (sekcja 13.1) bardziej rygorystycznych niż te, które wynikają z polskiego prawa oraz rekomendacji i wytycznych KNF.

Ponadto, niezależnie od tego czy dana umowa outsourcingu stanowi powierzenie w rozumieniu przepisów Prawa bankowego, czy też nie, przed zawarciem umowy outsourcingu bank powinien ocenić zgodnie z sekcją 12.2 Wytycznych EBA wszystkie istotne zagrożenia wynikające z korzystania z dostawcy z podwykonawców i dalszych podwykonawców i w razie potrzeby odpowiednio odzwierciedlić je w umowie z dostawcą (np. poprzez postanowienia nakładające na niego pewne obowiązki, ograniczenia lub zakazy).

Szczególnie istotnym elementem umowy jest zobowiązanie dostawcy do zawarcia określonych postanowień umownych w umowie pomiędzy nim a poddostawcą, przy pomocy którego realizować będzie on usługę chmury bankowej. Bank powinien zobowiązać podmiot świadczący usługę do zawarcia odpowiedniego postanowienia umownego w umowie z poddostawcą, która czyniłaby tę umowę umową o świadczenie na rzecz osoby trzeciej (w rozumieniu art. 393 KC) i – w przypadku właściwości prawa polskiego – uprawniałaby bank do żądania bezpośredniej realizacji usługi przez poddostawcę. Ważnym zagadnieniem w kontekście zobowiązania do włączenia odpowiednich postanowień umownych jest także zagadnienie odpowiedniości i stosownych kwalifikacji zespołu, który będzie realizował usługę – w tym wskazanie osób, które będą miały dostęp do informacji wrażliwych, objętych tajemnicą bankową. Zabezpieczając swoje interesy (jak zostało wskazane powyżej – na banku w tym względzie spoczywa obowiązek nadzorowania nad prawidłowością przetwarzania danych w chmurze) bank powinien zobowiązać dostawcę, aby ten uzyskał od poddostawcy listę osób, które w ramach dalszego outsourcingu, otrzymają dostęp do informacji niejawnych, objętych tajemnicą bankową (lub klucza szyfrowania), jak i zobowiązanie do przedłożenia bankowi udokumentowanej procedury ochrony

przetwarzanych danych przed nieautoryzowanym dostępem zgodnie z wymogami zawartymi m. in. w komunikacie chmurowym. Bank powinien wymagać, aby dostawca i poddostawcy, w razie potrzeby, na bieżąco aktualizowali te dane.

W przypadku nowych umów z dostawcami usługi, kluczowe jest zobowiązanie umowne (lub w formie aneksu w przypadku istniejących umów) do zapewnienia odpowiedniej jakości oferowanych usług w „chmurze" zarówno realizowanych przez nich samych jak też podmioty z nimi współpracujące czyli podwykonawców (za których dostawca usługi bierze całkowitą odpowiedzialność) oraz ich pełną zgodność z wytycznymi UKNF.

Umowa powinna określać odpowiedzialności dostawcy jak również jego zobowiązanie do zapewnienia zgodności podwykonawcy oraz zapewnienie prawa do audytu dostawcy oraz poddostawców (w umowie z dostawcą, zadaniem dostawcy jest zapewnić odpowiednie zapisy w umowie z poddostawcą), łącznie z zapewnieniem prawa wniesienia sprzeciwu wobec dalszego pod-outsourcingu lub rozwiązania umowy.

Umowa z dostawcą powinna zawierać wszystkie informacje (w tym zasady bezpieczeństwa dostawcy i ewentualnych podwykonawców), oraz parametry pozwalające określić stopień ryzyka związany ze świadczeniem usługi i miejscem jej wykonania. Te same wymagania powinny dotyczyć umów zawartych z podwykonawcami. Dostawca zobowiązany jest zweryfikować wymagania banku w zakresie bezpieczeństwa informacji i zagwarantować ich spełnienie przez swoich podwykonawców bądź zasygnalizować konieczność wyspecyfikowania odrębnych wymagań bezpieczeństwa. Umowy z podwykonawcami powinny uwzględniać klauzule dotyczące pełnej odpowiedzialności Dostawcy za działania podwykonawców i zobowiązania podwykonawców w takim samym zakresie w jakim zobowiązany jest sam dostawca.

W kontrakcie z zasady powinien być zapis o możliwości lub wręcz konieczności przeprowadzania przez zamawiającego okresowych (nie rzadziej niż raz na rok) audytów celowych w zakresie czynności powierzonych. Ważne jest, aby dostawca zapewnił możliwość przeprowadzania audytów i kontroli u poddostawców na poziomie nie niższym, niż dotyczy to samego dostawcy, choć zamawiający, oceniając ryzyko, może odstąpić od sprawdzenia podwykonawców opierając się na dostarczonych przez wykonawcę dokumentach potwierdzających odpowiedni poziom zabezpieczeń i wykonane sprawdzenia, w tym wypadku można zaakceptować certyfikaty na zgodność z właściwymi normami ISO. Audyty prowadzone u wykonawcy mogą być zastąpione uznanym i dostarczonym przez wykonawcę certyfikatem w zakresie objętym umową. Zamawiający powinien też mieć prawo, w uzasadnionych przypadkach, żądania regularnych informacji o kondycji finansowej podwykonawców.

W zakresie outsourcingu bankowego istotne jest upewnienie się, że dostawcy i ich produkty czy usługi spełniają wymagania i regulacje narzucane przez organy nadzoru sektorowego Warto na poziomie kontraktu zabezpieczyć konieczność poddania się dostawcy tym obowiązkom poprzez odwołania się do klauzul związanych z obowiązkami instytucji zamawiających, które podlegają regulacjom.

Przechodząc do kwestii bardziej technicznych koniecznie należy zwrócić uwagę na sposób zabezpieczenia i odzyskania danych w przypadku zmiany dostawcy lub

zakończenia umowy. Należy zabezpieczyć kontraktowo odpowiednie obowiązki związane ze współpracą przy zakończeniu umowy (np. plan wyjścia, migracja danych, dokumentacja).

Dostawca powinien być zobowiązany do informowania zamawiającego o zmianie poddostawcy, umożliwiając sprawdzenie, czy w nowych warunkach usługa generuje dodatkowe czynniki ryzyka. Dostawca powinien potwierdzić zgodność usługi z regulacjami oraz pilnować czy nie pojawiają się zmiany regulacyjne, które wymuszają zmiany ram funkcjonowania usługi (oraz stosownie do tego adaptować usługę). Warto także zapewnić możliwość inspekcji w Data Center dostawcy.

Bank powinien zagwarantować sobie dostęp do informacji na temat posiadanych przez podwykonawcę zasad bezpieczeństwa, a także możliwość weryfikacji tych dokumentów.

Poniżej zebrane są rozwiązania kontraktowe, dotyczące podwykonawcy, które powinny się znaleźć w umowie o charakterze outsourcingu kwalifikowanego:

- skorzystanie ze świadczeń podwykonawcy (innego niż wskazany w umowie w chwili jej zawierania), jest dopuszczalne wyłącznie po uzyskaniu uprzedniej zgody Banku w formie aneksu do umowy;
- w wypadku korzystania z podwykonawców, niezależnie od wyrażenia na to zgody przez Bank, dostawca na zasadzie ryzyka ponosi pełną odpowiedzialność za wykonywanie zobowiązań oraz szkody wyrządzone przez podwykonawców podczas i przy okazji realizacji umowy, jak za własne działania lub zaniechania;
- dostawca nałoży na podwykonawców obowiązek przestrzegania wszelkich zasad, reguł i zobowiązań określonych w umowie – w zakresie w jakim odnosić się one będą do zakresu prac podwykonawcy powierzonego do wykonania przez dostawcę.
- dostawca zapewnia, że zarówno on jak i podwykonawca posiadają regularnie testowane plany ciągłości działania i procedury awaryjne zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową. plany stanowią załącznik do umowy
- dostawca zapewnia, że zarówno jego pracownicy jak i podwykonawcy uczestniczący w realizacji przedmiotu umowy podlegają takiemu samemu zobowiązaniu do zachowania poufności jak dostawca
- umowa musi wyraźnie określać zarówno samego podwykonawcę zaangażowanego do realizacji usług, jak i opis czynności mu powierzonych (zakres obowiązków podwykonawcy może stanowić wyłącznie czynności pomocnicze w stosunku do świadczenia głównego realizowanego przez dostawcę)
- wykonywanie czynności przez podwykonawcę odbywa się w oparciu o art. 6a ust. 7 pkt 1 Prawa bankowego po spełnieniu łącznie poniższych warunków:
  - wyłącznie w zakresie wskazanych w umowie czynności służących realizacji głównego świadczenia (tzw. czynności pomocnicze);
  - dostawca zobowiąże podwykonawcę w łączącej go z nim umowie do przestrzegania obowiązków dostawcy wynikających z umowy w zakresie w jakim obowiązki te dotyczą czynności wykonywanych przez podwykonawcę;
  - dostawca zobowiąże podwykonawcę w łączącej go z nim umowie do zapewnienia takiego samego poziomu jakości usług oraz poufności jaki wynika z umowy;

- dostawca zobowiąże podwykonawcę w łączącej go z nim umowie do wprowadzenia zakazu korzystania z dalszych podwykonawców;
- dostawca zobowiązuje się zapewnić w łączącej go z nim umowie, że podwykonawca będzie ponosił odpowiedzialność za szkody powstałe w wyniku niewykonania bądź nienależytego wykonania zobowiązań wynikających z umowy zawartej pomiędzy dostawcą a podwykonawcą zgodnie z obowiązującymi przepisami prawa;
- dostawca zobowiązuje się zapewnić, że pracownicy podwykonawcy będą posiadali odpowiednie doświadczenie i kwalifikacje umożliwiające należyte wykonywanie czynności wynikających z umowy;
- dostawca zobowiązuje się zapewnić, że podwykonawca będzie w pełni poinformowany o wymaganiach prawnych i regulacyjnych związanych z wykonywanymi czynnościami wynikającymi z Umowy, w szczególności związanych z zachowaniem tajemnicy bankowej.

P3: Jak powinno się badać architekturę rozważanego rozwiązania w celu ustalenia poziomów poddostawców / podwykonawców w kontekście zakazu dalszego pod-outsourcingu (art. 6a ust. 7 Prawa bankowego)?

W ramach analizy ryzyka i opcji wyjścia należy pobocznie zweryfikować te kwestie, chociażby w ramach potrzeby bieżącego monitorowania zgodności przetwarzania przez podmiot świadczący usługę chmury danych w chmurze z nałożonymi na bank obowiązkami w tym zakresie, w szczególności wynikającymi z Komunikatu Urzędu Komisji Nadzoru Finansowego z dnia 23 stycznia 2020 r. dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej. Ponadto zgodnie z rekomendacją 2 rekomendacji D w banku powinien funkcjonować sformalizowany system informacji, dostosowany jednak do poziomu zidentyfikowanego ryzyka. Wydaje się, że element ten powinien zostać uwzględniony w ramach ustalania relacji pomiędzy bankiem a podmiotem świadczącym usługi chmury. Zasadnym zdaje się, aby bank w umowie o świadczenie usługi chmury obliczeniowej jednoznacznie zobowiązał podmiot świadczący do każdorazowego informowania o włączeniu w świadczoną usługę poddostawców. Ponieważ na banku ciąży obowiązek bieżącego monitorowania ryzyka, wydaje się, że w tym względzie bank może przy użyciu wszelkich dostępnych sposobów, w ramach prowadzonej analizy, weryfikować w jakim zakresie dostawca realizuje usługę poprzez poddostawców.

Aby zapewnić odpowiedni poziom kontroli, każdorazowe powierzenie czynności do podwykonawcy powinno być poprzedzone adekwatnym oświadczeniem z min. 30 dniowym wyprzedzeniem aby przedsiębiorstwo mogło podjąć odpowiednie działania weryfikujące lub zgłosić swój sprzeciw.

Opis architektury rozważanego rozwiązania powinien obejmować wszystkie usługi użyte w danym rozwiązaniu. Każda usługa powinna być zbadana pod kątem miejsca i parametrów świadczenia usług jak i dostawcy wykonania usługi. Może zdarzyć się rozwiązanie zbudowane z wykorzystaniem usług od różnych dostawców lub od jednego dostawcy zamawiającego usługi od poddostawców. Określenie usług opisanych w architekturze rozwiązania a także wykonawcy usług pozwoli określić ryzyko rozwiązania.

Badanie architektury musi odbyć się przez wykwalifikowanego pracownika zlecającego lub wskazany podmiot posiadający właściwe kompetencje i realizującego w imieniu zamawiającego sprawdzenie zgodności architektury z zadeklarowanym schematem. Wykonawca musi zgodzić się na takie sprawdzenie i informować zamawiającego w przypadku istotnych wpływających na bezpieczeństwo i architekturę rozwiązania zmian.

Należy zwrócić uwagę na lokalizację fizyczną i logiczną poszczególnych elementów architektury/infrastruktury projektowanego rozwiązania ze szczególnym rozpoznaniem warunków prawnych oraz pod kątem zależności regresowym w zakresie SLM/SLA ze względu na potencjalne sprzeczne uwarunkowania w lokalizacjach infrastruktury występujących poza krajem zamawiającego/wykonawcy z którym zamawiający zawiązuje umowę.

Podstawowa metoda takiego badania może być powiązana z analizą **przepływu i dostępu do danych**. W przypadku jej zastosowania sprawdzamy jak nasze (czyli banku) dane są obsługiwane przez dostawcę. Czy są kopiowane i dokąd? Kto ma do nich dostęp i w jakim zakresie? Metoda jest relatywnie prosta w użyciu, gdyż dostawcy trudno jest nie udzielić odpowiedzi na tak zadane pytania. W wielu wypadkach kwestia dostępu do danych będzie dodatkowo regulowana innymi przepisami (np. RODO) i w badaniach warto korzystać z tego, co jest/powinno być efektem stosowania tych przepisów. Choć wyrażenie terminu „dostęp do danych" językiem prawniczym stanowi pewne wyzwanie, na poziomie technicznym jest to relatywnie proste.

Poza przepływem danych istotne i znacznie trudniejsze może być podejście do **przepływu informacji.** Na ile usługodawca dzieli się z innym podmiotem danymi już w formie przetworzonej (np. agregaty danych niezbędne do analizy portfelowej). Tutaj ograniczenie na poziomie architektury może być niewystarczające. Dlatego warto przejść do pytania o **zewnętrzne źródła wiedzy/informacji** z jakich poddostawca korzysta przy wykonywaniu usługi. Z punktu widzenia architektury rozwiązania pytanie dotyczy zewnętrznego **zasilenia danymi** systemów podwykonawcy.

Warto też zapoznać się z wynikami globalnego badania przeprowadzonego na przełomie 2019 i 2020 roku w zakresie praktyk zarządzania ryzykiem stron trzecich (TPRM – third party risk management). Pokazało ono, że aż 57% badanych instytucji finansowych polega na ustaleniach umownych z trzecią stroną lub wykonywaniu oceny / monitorowania podwykonawców (stron czwartych) przez strony trzecie. Warto zwrócić uwagę, że w badaniu wzięło udział 246 organizacji, w tym 123 globalnych instytucji finansowych – zróżnicowanych co do skali działalności i złożoności, jak również dojrzałości procesu zarządzania ryzykiem outsourcingu. Wyniki badania ankietowego wskazują, jak najczęściej organizacje podchodzą do badania ryzyka związanego z działalnością podwykonawców swoich dostawców (stron czwartych).

1/3 ankietowanych organizacji świadczących usługi finansowe polega na warunkach umownych ze swoimi stronami trzecimi w zakresie monitorowania stron czwartych. Często stosowaną praktyką (25% badanych podmiotów) jest poleganie przez instytucje na ocenie ryzyka podwykonawców przeprowadzonej przez stronę trzecią. W 17% przypadkach instytucje przy ocenie ryzyka stron trzecich bazują na umowie zawartej

pomiędzy stroną trzecią a stroną czwartą, co wymaga dużej transparentności modelu świadczenia usługi na rzecz banku w zakresie angażowania stron czwartych.

Niewielu ankietowanych (9%) przeprowadza własne, niezależne przeglądy stron czwartych, chociaż liczba ta wzrosła w porównaniu do badania z przełomu 2018/2019 roku. Tylko 6% respondentów wskazała, że strony czwarte nie są monitorowane.

Angażowanie przez strony trzecie dalszych podwykonawców jest dziś w skali światowej zjawiskiem powszechnym, biorąc pod uwagę złożoność rozwiązań technologicznych, łańcuchów powiązań i możliwości optymalizacji kosztowej. Dopuszczenie możliwości świadczenia usług przez strony czwarte w ramach podstawowej umowy outsourcingowej jest dla banków i ich podwykonawców kuszące i z pewnością ten trend będzie się nasilał w przyszłości. Wymaga to jednak sprawnego systemu zarządzania ryzykiem takich relacji, wyraźnych zgód w umowie outsourcingowej ze strony banku oraz zapewnienia kontroli stron czwartych przez strony trzecie, a w uzasadnionych przypadkach (w zależności od oceny ryzyka/istotności/krytyczności relacji outsourcingowej) również kontroli stron czwartych przez bank.

Podsumowując, wachlarz dostępnych rozwiązań w zakresie monitorowania stron czwartych jest szeroki i obejmuje następujące rozwiązania:

- poleganie na umowie ze stroną trzecią,
- poleganie na ocenie ryzyka przeprowadzonej przez stronę trzecią,
- poleganie na umowie pomiędzy stroną trzecią a stroną czwartą,
- przeprowadzenie niezależnego przeglądu stron czwartych.

P4: W jaki sposób powinno się definiować w umowach outsourcingu bankowego zakres odpowiedzialności podwykonawcy insourcera?

Zgodnie z Prawem bankowym odpowiedzialności dostawcy, wobec banku za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy outsourcingowej, nie można wyłączyć ani ograniczyć. Przepis jest bezwzględnie obowiązujący a zatem żadne postanowienia kontraktowe między stronami nie mogą go zmienić lub zastąpić. Zarówno jednak banki jak i przede wszystkim dostawcy są świadomi nie tylko istnienia ale również charakteru tego postanowienia.

Pomimo to nie ma jednej dobrej odpowiedzi na to pytanie. Zależy ona od rodzaju przedmiotu outsourcingu i jego charakterystyki. Ale niezależnie od przedmiotu outsourcingu w umowie outsourcingu bankowego dostawca ponosi pełną odpowiedzialność za wykonywanie zobowiązań oraz szkody wyrządzone przez podwykonawców podczas i przy okazji realizacji umowy, tak jak za własne działania lub zaniechania i ten fakt powinien znaleźć swoje odzwierciedlenie w umowie banku z dostawcą. Jest to istotne, ponieważ bank, jako podmiot zlecający, nie powinien wchodzić w relacje z podwykonawcą. Na poziomie kontaktowym wykonawca powinien brać pełną odpowiedzialność za swojego podwykonawcę.

Jak się wydaje, najkorzystniejsze z perspektywy banku byłoby ustanowienie odpowiedzialności po stronie dostawcy na wzór odpowiedzialności zbliżonej konstrukcyjnie do odpowiedzialności solidarnej, jednak z uwagi na brak bezpośredniego

stosunku kontraktowego pomiędzy bankiem i poddostawcą, odpowiedzialność umowna odnosić będzie się jedynie wobec dostawcy. Wobec poddostawcy przysługiwałoby bankowi roszczenie na gruncie deliktowym. Wydaje się przy tym istotne, aby w umowie rozszerzyć odpowiedzialność dostawcy także o niewykonanie zobowiązania dokonane przez poddostawcę. Teoretycznie – w przypadku zastosowania prawa polskiego – kwestie taką reguluje artykuł 474 KC lub 429 KC. Wydaje się rzeczą istotną, zwłaszcza w przypadku ustanowienia dla umowy prawa właściwego innego niż polskie, inkorporowanie do umowy odpowiednich postanowień odzwierciedlających treść powyższych artykułów. W razie nienależytego wykonania umowy świadczenia usługi z przyczyn leżących po stronie podwykonawcy umożliwiłoby to bankowi roszczenie bezpośrednio względem dostawcy, który natomiast miałby prawo regresu wobec poddostawcy.

P5: Jakie trudności organizacyjne i prawne mogą wystąpić w związku z zawieraniem umów outsourcingu bankowego?

W wielu przypadkach wyzwaniem może być ustalenie, czy dana usługa zalicza się do „outsourcingu bankowego". Dobrym przykładem jest dyskusja czy obsługa poczty elektronicznej w banku, to już jest outsourcing bankowy. Konsekwencje takiego rozstrzygnięcia mogą być daleko idące, ponieważ interpretacja, zgodnie z którą korzystanie z poczty z serwerami umieszczonymi w chmurze obliczeniowej zalicza się do outsourcingu bankowego, zawiesiła na długi czas wprowadzanie technologii chmurowych w bankach. Warto zwrócić uwagę, że nadal pozostaje wiele funkcji wsparcia, które nie są zaliczane do outsourcingu bankowego (np. obsługa HR), co powoduje, że określenie granicy wymaga oceny w każdym konkretnym przypadku. Problemem są także niejasne wymogi KNF związane z kryteriami, jakie musi spełniać poddostawca, aby zostać zaliczony do łańcucha outsourcingowego

Wymogi formalno-prawne postrzegane są jako istotne przeszkody. Duże trudności, zwłaszcza mniejszym podmiotom, sprawia konieczność uzyskiwania zgód regulatora na transfer danych poza EU. W przypadku korzystania z usług centrów wspólnych zlokalizowanych w krajach o niskich kosztach prowadzenia działalności np. w Azji, uzyskanie dla danego podmiotu dokumentów według listy KNF oraz ich przetłumaczenie jest bardzo czasochłonne i kosztowne – tym bardziej że polski reżim outsourcingowy jest w tym zakresie unikalny i nie jest oparty na zasadzie ryzyka tj. każdy outsourcing jest traktowany tak samo.

Co więcej często się zdarza, że konieczne jest zebranie dokumentów od razu dla dwóch podmiotów, tj dla głównego dostawcy usług oraz dla podmiotu który byłby dostawcą w razie zaistnienia zdarzenia uruchamiającego plan awaryjny. Dla podmiotów działających w ramach grup kapitałowym może to oznaczać konieczności indywidualnego zorganizowania danego obszaru dla banku polskiego, podczas gdy pozostali członkowie grupy korzystają ze wspólnych rozwiązań. Alternatywą byłoby opóźnienie wdrożenia w całej grupie.

Istotnym problemem zdaje się być także kwestia prawa właściwego dla umowy o świadczenie usług chmury bankowej w przypadku, gdy strony zdecydują się na zastosowania prawa państwa innego, niż ojczyste.

W przypadku stosowania przez bank chmury obliczeniowej źródłem trudności może być również outsourcing awaryjny – bank zabezpieczając ciągłość działania zawrzeć może umowę o świadczenie usług w chmurze, która uchroni go przed przerwaniem ciągłości działania. W takim wypadku bank powinien – pomimo, że świadczenie usługi ma charakter doraźny – realizować nałożone na niego obowiązki prawne.

Spełnienie niezbędnych wymagań regulacyjnych dotyczących kwestii organizacyjnych (ocena umowy, dostawcy, ryzyka itp.) może być znacznym obciążeniem w szczególności dla mniejszych organizacji. To samo dotyczy wymogów prawnych, ponieważ dostawcy niechętnie się im poddają. Dotyczy to w pierwszym rzędzie wymagań dotyczących audytu, odpowiedzialności, lokalizacji przetwarzanych danych, zwłaszcza w przypadku dostawców usług chmury obliczeniowej. Istnieje zresztą pewne ryzyko, że pełny audyt i kontrola mogą być niemal niewykonalne. Problem z audytem uwidoczni się szczególnie w dużych strukturach, korzystających ze skomplikowanej infrastruktury chmurowej, składającej się z wielu poddostawców.

Dostawcy usług chmury obliczeniowej są to w większości duże podmioty, świadczące swoje usługi globalnie (Microsoft, Google, Amazon Web Services). Nie są one skłonne brać na siebie zobowiązania w zakresie szerszym, niż mają to określone w swoich standardowych umowach, regulaminach, w szczególności jeżeli wynikają one wyłącznie z wymagań polskich przepisów lub wytycznych organów nadzorczych, a nie są powszechnie obowiązującym przepisami w Unii Europejskiej lub w jurysdykcji krajów, w oparciu o które kształtowane są umowy tych dostawców usług chmury obliczeniowej. Pewnym wyjściem z tej sytuacji byłoby przeprowadzenie zewnętrznego audytu przez uznanego audytora.

Istotnym wyzwaniem wiążącym się z outsourcingiem jest przekazanie na zewnątrz procesu biznesowego, co wiąże się z utratą pełnej kontroli nad jego realizacją – w tym wypadku należy zadbać i zapewnić pełne, rozliczalne mechanizmy monitorowania stanu usługi i jej bezpieczeństwa. Wyzwaniem jest monitorowanie i zarządzanie dostawcami i ich podwykonawcami – w szczególności audytowalność ustalonych warunków i zasad outsourcingu bankowego zarówno w zakresie poprawności samych usług jak i w szczególności w zakresie danych i informacji które zostają powierzone, oraz ich przepływów. Dotyczy to w szczególności danych osobowych (wymogi RODO) oraz informacji chronionych tajemnicą bankową. Aby to było możliwe istotne jest precyzyjne określenie granic odpowiedzialności i obowiązków obu stron w umowie.

Odnosząc się do kwestii bezpieczeństwa w przypadku umów outsourcingowych, jako jeden z głównych problemów należy wskazać brak rzeczywistego rozproszenia baz danych, w których przechowywane będą dane przekazane przez banki w ramach zawartej umowy o świadczenie usług w chmurze.

Jeden z podstawowych nurtów dyskusji wokół outsourcingu bankowego dotyczy poziomu odpowiedzialności dostawców. Należy się zatem spodziewać, że temat ten pozostanie jednym z głównych obszarów negocjacyjnych w umowach

outsourcingowych. Wiąże się to z określeniem nie poziomu, a granic odpowiedzialności. Dobrą i chyba najważniejszą ilustracją tego problemu jest kwestia bezpieczeństwa. W przypadku nieograniczonej odpowiedzialności dostawcy, dyskusje o tym, w jakim zakresie odpowiada on za bezpieczeństwo będą bardzo trudne, zwłaszcza gdyby dostawca nie dał należytej rękojmi w zakresie usług wykonywanych przez siebie lub swojego podwykonawcę.

Wyzwaniem mogą się wiązać z ujęciem w umowie obszarów trudnych do określenia w formie parametrycznej. Łatwo jest zapisać np. jaka przepustowość łącza, czy też maksymalny obszar dyskowy ma zostać udostępniony. Dużo trudniej jest zdefiniować efektywną pracę systemu (np. „response time"), zwłaszcza w bardziej złożonych scenariuszach. W standardowym outsourcingu dostępne zasoby były z definicji ograniczone do określonych w umowie. Jedną z cech „chmury obliczeniowej" jest jej elastyczne reagowanie na okresowe duże zapotrzebowania na moc. Opisanie tych sytuacji w umowach może nie być łatwe.

W przypadku outsourcingu funkcji istotnych lub krytycznych wymagane jest wzmocnienie reżimu w zakresie samej konstrukcji umów outsourcingowych, zawartości rejestru tych umów, planów ciągłości działania czy oceny ryzyka i kontroli wewnętrznej. Tymczasem istotną trudnością jest klasyfikacja danej umowy jako umowy outsourcingu oraz funkcji krytycznej i ważnej w rozumieniu Wytycznych EBA. Chociaż Wytyczne wskazują szczegółowe kryteria (czynniki) przy określaniu, czy umowa outsourcingu dotyczy funkcji krytycznej lub istotnej, instytucje mają pewną swobodę w zakresie kalibracji tych kryteriów oraz powinny bazować na ocenie ryzyka relacji ze stroną trzecią. Może to prowadzić do tego, że umowa z tym samym dostawcą o analogiczny zakres usług będzie inaczej postrzegana (i klasyfikowana) przez różne banki, a to w konsekwencji prowadzi do konieczności uwzględnienia w umowach i spełnienia różnych wymogów.

Należy dążyć do adekwatnego do poziomu ryzyka monitorowania stron trzecich (zakresu, częstotliwości), dokonywania przeglądów i ocen dostawców w kontekście posiadanych przez banki zasobów. Nieuniknione jest większe wsparcie technologii w celu realizacji efektywnego systemu zarządzania ryzykiem stron trzecich, obejmującego zarówno I, jak i II linię obrony, w celu osiągnięcia – tam, gdzie to możliwe – automatyzacji i standaryzacji procesu.

Biorąc pod uwagę bieżący kontekst współpracy z podmiotami trzecimi, uwzględniający niestandardowe działania organizacji w czasie pandemii COVID-19, banki stanęły przed nowymi wyzwaniami i trudnościami dotyczącymi odporności operacyjnej oraz finansowej swoich dostawców, jak również bezpieczeństwa danych przetwarzanych w ramach realizacji umów outsourcingowych.

Problemy pojawiające się, lub nasilające się w związku z epidemią, to między innymi:

- trudności w ocenie zakresu, w jakim dostawcy usług mogą kontynuować swoją działalność w warunkach stresowych przez dłuższy okres;
- trudności w identyfikacji i zrozumieniu zależności i wrażliwości na otaczające zmiany;

- obawy dotyczące bezpieczeństwa danych oraz ryzyka wycieku danych spowodowane; upowszechnieniem pracy zdalnej po stronie dostawców;
- brak możliwości przeprowadzenia odpowiedniego procesu oceny ryzyka stron trzecich opartego na aktualnych danych w czasie pandemii;
- możliwości techniczne przeprowadzenia monitoringu sytuacji finansowej stron trzecich.

Wreszcie, szczególnie trudną kwestią jest zakończenie współpracy z dostawcą. Umowa powinna dokładnie określać ten proces. Najczęściej będzie się to wiązać ze zmianą dostawcy usługi. Tak jak w przypadku klasycznej zmiany dostawcy niezbędna jest migracja danych – czynność, która jest zawsze złożona i często jest to przyczyna wydłużania się czasu trwania projektów. W klasycznej sytuacji oznacza to tylko wydłużenie czasu korzystania z dotychczasowego rozwiązania na bazie posiadanej licencji (ew. niezbędne może być wydłużenie czasu trwania umowy wsparcia technicznego z dotychczasowym dostawcą). W przypadku rozwiązań chmurowych niezbędne jest wydłużenie umowy i świadczenie usług. O takiej ewentualności należy pamiętać już w momencie podpisywania umowy, aby zapewnić sobie możliwość jej przedłużenia na nie zmienionych warunkach.

P6: Jakie ograniczenia regulacyjne dotyczące outsourcingu bankowego mogą być najtrudniejsze do spełnienia?

Najtrudniejsze do spełnienia ograniczenia regulacyjne wynikają z braku spójności pomiędzy zapisami dotyczącymi outsourcingu bankowego w Prawie Bankowym oraz zapisami w Wytycznych EBA dotyczących outsourcingu. Wynika to między innymi z przyjęcia przez KNF krajowego podejścia do wytycznych EBA w zakresie usług chmury obliczeniowej. Polski nadzorca, jako jedyny, zgłosił, iż nie będzie się stosował do Wytycznych EBA dotyczących rozwiązań chmurowych. Trzeba zaś pamiętać, że zdecydowana większość dostawców usług chmury obliczeniowej to instytucje zagraniczne stosujące prawo międzynarodowe. Negocjacje umów podlegających pod krajowe przepisy prawa z zagranicznym dostawcą wymaga ekspertów w dziedzinie prawa krajowego i międzynarodowego. Dodatkowo, dużym wyzwaniem dla zapewnienia jakości, ciągłości, odpowiedzialności dla usług zlecanych przez podmioty, które podlegają rygorowi outsourcingu bankowego są uwarunkowania prawne oraz zróżnicowanie wynikające z regulacji obowiązujących zarówno lokalnie dla różnych sektorów.

Przykładem może być ograniczenie łańcucha outsourcingowego zgodnie z art. 6a Prawa bankowego. W szczególności trudność ta będzie się ujawniać w przypadku, gdy dostawca świadczy powierzone mu przez bank czynności w oparciu o usługi chmury obliczeniowej, które dostarcza mu jego podwykonawca. Powstaje wtedy łańcuch:

bank → insourcer → dostawca chmury obliczeniowej (podwykonawca dostawcy)

W praktyce jednak dostawcy usług chmury obliczeniowej często są dostawcą platformy chmurowej, w ramach której udostępniają również inne, szczególne usługi, które jednak świadczone są przez kolejnych poddostawców, współpracujących z dostawcą chmury obliczeniowej. Na gruncie obowiązujących przepisów korzystanie przez bank z takich

dodatkowych usług byłoby niemożliwe w modelu współpracy, w ramach którego bezpośrednim dostawcą tych usług dla banku byłby dostawca – dostarczający zagregowane usługi własne, dostawcy chmury obliczeniowej i jego poddostawcy – ponieważ zbytnio by to wydłużyło łańcuch outsourcingowy.

Tak więc, z jednej strony, rozwiązania chmurowe są co do zasady akceptowane, ale z drugiej regulacje nie są zbieżne z praktyką. Od regulatora należałoby zatem oczekiwać dogłębnej analizy problemu i możliwych rozwiązań. Być może, zważywszy na priorytety nadzoru, nie istnieje akceptowane rozwiązanie, ale wtedy należy to jasno powiedzieć, ponieważ rozwiązania problemów wynikających z regulacji, z którymi muszą się zmierzyć banki, pozostają w kompetencji regulatora.

Oddzielnym problemem jest dostosowanie regulacji wewnętrznych w przedsiębiorstwie oraz umów z dostawcami do wytycznych UKNF dotyczących chmury rozliczeniowej.

Często wykonawca nie chce się zgodzić na narzucone zapisy w umowach, których nie jest w stanie wykonać, szczególnie w dobie pandemii, a jeśli nawet się zgodzi, to często pozostają one „puste", szczególnie w przypadku globalnych dostawców chmury obliczeniowej.

Poważnym problemem jest prowadzenie audytów, kontrola i nadzór nad wykonywaniem czynności powierzonych oraz w szczególności bezpieczeństwa powierzonych danych i informacji. Są obszary, w których nie rodzi to problemów, np. prowadzenie placówki bankowej, ale są obszary, w których jest to trudne, a w szczególnych przypadkach rozwiązań chmurowych niemal niewykonalne. Powinno się przesądzić czy warto trwać przy rygorystycznych obostrzeniach, których przestrzeganie znacznie utrudnia pozyskanie bezpiecznego technologicznie outsourcera.

Zamawiający powinien sprawować właściwy nadzór nad wykonawcą. Spełnienie tak sformułowanego wymagania może być trudne. Właściwy nadzór to dość trudne do definiowania pojęcie i wymaga przeprowadzenia analizy ryzyka i zaangażowania dość szeroko zakrojonych metod organizacyjnych i technicznych gwarantujących możliwość dokumentowania wszelkich działań po stronie wykonawcy zapewniając sobie materiał dowodowy w kwestiach spornych. Dla przykładu, w przypadku dużych, rozproszonych baz danych – może to być weryfikacja przez bank prawidłowości przetwarzania danych w chmurze obliczeniowej z perspektywy nałożonych na ten podmiot obowiązków – szczególnie w zakresie okresowej analizy ryzyka i dostosowywania do niej odpowiednich mechanizmów. Z drugiej jednak strony, należy unikać sytuacji, w których dane kilku banków będą przechowywane w bazach danych znajdujących się w tym samym miejscu.

Bank wymaga możliwości wglądu w procedury wewnętrzne dostawcy (np. obowiązek wskazywania przez bank metod zarządzania zmianą, procedur testowania etc.). Podmioty nie bankowe w obszarze obsługi banków są w tym zakresie traktowane jak banki, co może być poważnym wyzwaniem dla wszystkich zainteresowanych stron, w tym również dla regulatorów i podmiotów nadzorczych. Dlatego regulator musi albo zaproponować bankom realistyczne rozwiązanie, zapewniające należyty poziom bezpieczeństwa, albo zabronić korzystania z outsourcingu, zwłaszcza z rozwiązań chmurowych.

Kolejnym wyzwaniem jest obowiązek opracowania i wdrożenia planów ciągłości działania w odniesieniu do funkcji istotnych i krytycznych, w szczególności na poziomie dostawcy usługi oraz zapewniania strategii „wyjścia" dla funkcji istotnych i krytycznych. Bariery dotyczą możliwości identyfikacji alternatywnych rozwiązań i przygotowania planów na okres przejściowy tj. do momentu przekazania świadczenia usługi do innego dostawcy lub z powrotem do instytucji finansowej, jak również testowania planów ciągłości i strategii wyjścia.

Oddzielną sprawą jest nieproporcjonalne do skali ryzyka podejście regulacyjne. Jednym z ograniczeń regulacyjnych dotyczących outsourcingu bankowego jest bezwzględny obowiązek stosowania wszystkich narzędzi i obowiązków outsourcingowych określonych w obowiązujących przepisach (np. art. 6a-6d Prawa bankowego) w tym samym zakresie i wymiarze wobec wszystkich dostawców, niezależnie od rozmiaru dostawcy lub zakresu powierzanych mu prac. Powinna być możliwość stosowania tych narzędzi i obowiązków w oparciu o przeprowadzoną analizę ryzyka, przy uwzględnieniu zasady proporcjonalności.

Przykładowo inne są możliwości dużego przedsiębiorcy, korzystającego z różnych centrów przetwarzania danych (CPD), do opracowania i realizacji planu awaryjnego, przy wykorzystaniu tych różnych CPD. Tymczasem mikroprzedsiębiorca lub mały przedsiębiorca, a wiele fintechów dostarczających innowacyjne rozwiązania, to właśnie podmioty nie dysponujące pokaźnymi zasobami, dopiero budujące swój potencjał rynkowy, nie ma takich samych możliwości do zagwarantowania realizacji planu awaryjnego, jak duży przedsiębiorca.

Jest to faktycznie duże utrudnienie, ale problem ten wykracza poza dyskusję na temat outsourcingu i w pierwszym rzędzie się wiąże się z fintechami. Z jednej strony nie można dopuścić, by od małego podmiotu zależało bezpieczeństwo dużego banku. Niezbędna jest zatem szczegółowa ocena ryzyka, ale tej nie da się przeprowadzić bez testowania danego rozwiązania w warunkach rzeczywistych, w małej skali. Być może pomocna byłaby tu piaskownica regulacyjna.

P7: Jak powinno się zbierać zgody na ujawnienie tajemnicy bankowej tam, gdzie dana umowa nie jest zawierana w reżimie outsourcingu bankowego, a dochodzi do ujawnienia tajemnicy bankowej?

W takiej sytuacji (jeśli nie zachodzi możliwość przekazania tajemnicy bankowej na podstawie przepisu szczególnego) zastosowanie ma art. 104 ust 3. Prawa bankowego, a zatem taka zgoda powinna być przekazana na piśmie lub na informatycznym nośniku danych i zawierać zgodę na przekazanie określonych informacji oraz wskazanie jednostki organizacyjnej, do której dane mogą być przekazane.

Zgodnie z regulacjami Kodeksu cywilnego forma elektroniczna wymaga opatrzenia kwalifikowanym podpisem elektronicznym. Wydaje się, że na potrzeby przetwarzania danych w zakresie przekraczającym dopuszczalne ustawowo udostępnianie informacji objętych tajemnicą bankową, należy uzyskać zgodę w jednej z powyższych form. Zasadna przy tym może być próba uzyskania zgody na przetwarzanie tych danych przez Bank w postaci elektronicznej – w postaci zaadresowanej do klienta informacji

zawierającej zarazem instrukcję postępowania, na przykład stosując komunikację za pośrednictwem elektronicznego dostępu do konta bankowego po zalogowaniu. Klient, udzielając zgody, dochowując rygorów przewidzianych w kodeksie cywilnym, powinien zgodę taką opatrzyć podpisem kwalifikowanym. Wyrażenie przez Klienta zgody powinno być udokumentowane i zarchiwizowane przez bank.

Postulaty ekspertów

Odpowiedzi na pytania udzielone przez ekspertów pokazują, że regulacje dotyczące outsourcingu, oraz ich interpretacja, budzą szereg wątpliwości, albo ze względu na niespójności definicji, niespójności wymagań, albo ze względu na odstępstwa od praktyki powszechnie stosowanej na unijnym rynku finansowym. Ma to kilka konsekwencji:

- Polskie banki mają niejednokrotnie słabszą pozycję konkurencyjną w porównaniu z bankami z innych państw członkowskich.
- Polskie banki mają większe trudności przy negocjowaniu i zawieraniu umów outsourcingowych z dostawcami działającymi na rynku unijnym, zwłaszcza największymi podmiotami, które działając na rynku unijnym z konieczności godzą się z wymogami prawa unijnego, ale nie chcą akceptować polskich przepisów, odmiennych niż unijne.
- W przypadku grup bankowych konieczność stosowania w Polsce innych standardów i rozwiązań niż w pozostałych krajach członkowskich znacząco podnosi koszty działalności, co odbija się na wynikach polskich banków.

Nie sposób a priori stwierdzić, w których przypadkach możliwa jest zmiana zasad, albo zmiana praktyki. Natomiast wszędzie tam, gdzie rynek sygnalizuje wątpliwości, niezbędny jest dialog regulatora z rynkiem, aby doprowadzić do zmiany, albo satysfakcjonująco wyjaśnić rynkowi racjonalność przesłanek, którymi kieruje się regulator.

Najważniejsze kwestie pojawiające się w odpowiedziach ekspertów przedstawione są poniżej.

1. Niespójność regulacji

   Banki są zobowiązane stosować się do Wytycznych EBA w sprawie outsourcingu. KNF potwierdził, że zamierza się do nich stosować. Jednocześnie, jako jedyny nadzorca zgłosił, iż nie będzie się stosował do wytycznych z wyjątkiem części dotyczącej chmury i usług chmurowych. Ten obszar regulowany jest odpowiednim Komunikatem KNF. Niestety, w Wytycznych EBA usługi chmurowe są jedną z outsourcowanych usług, natomiast Komunikat KNF odnosi się do przetwarzania informacji w chmurze obliczeniowej. Z odpowiedzi ekspertów wynika, że – jak dotąd – nie dało się zachować spójności pomiędzy tymi dwoma dokumentami, ze

względu na odmienną konstrukcję każdego z nich. Tymczasem niespójność przepisów przekłada się na niespójność decyzji, co w dłuższej perspektywie rozregulowuje rynek. Dlatego ważne jest, by regulator, wespół z rynkiem, dokonał krytycznej analizy obu regulacji i wypełnił luki oraz usunął sprzeczne postanowienia.

Dla przykładu, jeden z ekspertów wskazuje, że nie jest jasne, co kryje się pod pojęciem outsourcingu bankowego tj. czy jest on tożsamy z outsourcingiem regulowanym w Prawie bankowym, czy też ma znaczenie szersze zgodnie z wytycznymi EBA w sprawie outsourcingu wydanymi w dniu 25 lutego 2019 r.

Stanowisko KNF z dnia 16 września 2019 r. dotyczące wybranych zagadnień związanych z wejściem w życie Wytycznych EBA i ich uwzględnieniem w działalności banku wprost wskazuje, że z uwagi na definicję „outsourcingu" zawartą w Wytycznych EBA, należy przyjąć że „outsourcing" jest pojęciem szerszym niż powierzenie wykonywania czynności w rozumieniu Prawa bankowego. Istnieje wobec tego możliwość, że dana umowa będzie kwalifikowana jako outsourcing zarówno z punktu widzenia prawa krajowego oraz Wytycznych EBA, jak również że będzie ona outsourcingiem wyłącznie na podstawie Wytycznych EBA.

2. Pytania bez odpowiedzi

Eksperci wskazują niejasności dotyczące klasyfikacji konkretnych przypadków.

- Czy tzw. umowy B2B stanowiące standard na rynku IT (standardowy typ umowy z programistami) powinny być traktowane jak outsourcing tj. czy programista wewnętrzny zatrudniony na umowie typu B2B powinien być traktowany zgodnie z zasadami dla typowych dostawców i objęty zakresem wytycznych dotyczących outsourcingu? Analogiczne problemy pojawiają się przy dostawcach korzystających z programistów zatrudnionych na umowach B2B w kontekście ewentualnego występowania podoutsourcingu. Interpretacji wymaga czy podejście zostanie oparte na ekonomicznym sensie umowy zgodnie z rynkiem IT (i wówczas nie będzie traktowane jak outsourcing/podoutsourcing) czy na literalnym czytaniu wytycznych EBA (outsourcing jako dowolna umowa z dostawcą).
- Jeśli dostawca rozwiązania chmurowego nie ma dostępu do danych prawnie chronionych, które są przekazywane przez bank do jego dostawcy, jeśli dane są szyfrowane, czy zasadne jest klasyfikowanie rozwiązań chmurowych jako podwykonawców, niezależnie od formuły takiego rozwiązania (IaaS, PaaS, SaaS) oraz od tego czy chmura ma charakter publiczny czy współdzielony? Fakt korzystania z rozwiązań chmurowych przez ich dostawców, powinien być postrzegany jako jedna z przesłanek w procesie oceny ryzyka związanego z korzystaniem z danego dostawcy, natomiast nie powinien być to element przesądzający i powinien być ewentualnie brany pod uwagę z punktu widzenia planów ciągłości działania i bezpieczeństwa w zakresie nieprzerwanego

świadczenia usług dla klienta, a nie z punktu widzenia kwalifikowania jako tego podmiotu trzeciego jako podwykonawcy.

3. Wymóg nieograniczonej odpowiedzialności outsourcera za szkody wyrządzone klientom banku.

   Większość ekspertów krytykuje ten wymóg. Jednocześnie wielu ekspertów postuluje pełną odpowiedzialność podwykonawcy outsourcera za wyrządzone straty, posługując się racjonalnymi argumentami. Oczywiście, w żadnym przypadku nie może ona przekraczać faktycznie wyrządzonej klientowi lub bankowi szkody.

   Niektórzy eksperci wskazują, że wobec bezwzględnie obowiązującego przepisu banki wymuszają odpowiednie klauzule w umowie, ale – jak sami twierdzą – klauzule te są „puste" i wiadomo, że w razie pojawienia się problemu będą one nieskuteczne. To jest zapewne najgorsze z możliwych rozwiązań, ponieważ w praktyce uniemożliwia ocenę ryzyka.

   Podchodząc do zagadnienia bez emocji należałoby stwierdzić, że powierzenie outsourcerowi wykonywanie pewnych czynności, zwłaszcza krytycznych, nie może zwiększać ryzyka działalności banku. Oczywiście, bank musi należycie oceniać wszystkie czynnika ryzyka, monitorować wykonywanie powierzonych czynności, ale outsourcer powinien ponosić pełną odpowiedzialność za spowodowane przez siebie, zawinione straty. Najbardziej protestują przeciwko temu przepisowi najwięksi outsourcerzy. Ale jednocześnie są to najbardziej zaawansowane przedsiębiorstwa, więc ryzyko tego, że będą narażone na odszkodowania, które mogłyby nimi zachwiać, jest znikome.

   Od wprowadzenia tego przepisu minęło blisko 20 lat, zmieniły się realia, otoczenie. W tej sytuacji wskazane byłoby przeprowadzenie przez KNF analizy prawnej, biznesowej tego zagadnienia, aby rozwiązać ten problem. Dogłębna, rzetelna analiza, która brałaby pod uwagę zarówno korzyści dla banku płynące z obecnie obowiązującego przepisu, jak i straty, które mogłyby się pojawić w wyniku utrzymania obecnego prawa, powinna odpowiedzieć regulatorowi i bankom na pytanie o ewentualną zmianę dyskutowanego przepisu i o konsekwencje każdej z możliwych do podjęcia decyzji.

4. Różnica między outsourcingiem i insourcingiem.

   Jedno z pytań dotyczyło zakresu odpowiedzialności podwykonawcy insourcera. Nadesłane odpowiedzi każą podejrzewać, że niezbędne są dodatkowe objaśnienia regulatora, dotyczące różnicy między outsourcingiem i outsourcingiem, zwłaszcza w zakresie podwykonawstwa. Ma to istotne znaczenie, ponieważ, o ile w przypadku outsourcingu, zasady są uniwersalne i nie zależą od struktury, w jakiej funkcjonuje rozwiązanie outsourcingowe, w przypadku insourcingu będzie to zależało od

podejścia do grupy, zlecaniu czynności podmiotowi należącemu do grupy, a w konsekwencji konieczności (lub nie) uzyskiwania zezwoleń, itp.

5. Pozostałe postulaty dotyczące outsourcingu

   Jeden z ekspertów postuluje dalszą liberalizację Prawa bankowego w zakresie możliwości korzystania z podoutsourcingu, eliminując ograniczenia i wymogi bardziej restrykcyjne niż wynikające z Wytycznych EBA:

   - Należy dopuścić możliwość łańcucha podwykonawców. Może należałoby rozważyć ograniczenie długości łańcucha, ale powinien on być przynajmniej kilku stopniowy.
   - Podwykonawca podwykonawcy powinien być zgłaszany zleceniodawcy/bankowi, ale podwykonawca nie powinien uzyskiwać zgody na wybór danego podwykonawcy, a gdyby uznać zgodę za wymaganą, jej cofnięcie musiałoby być uzasadnione nieprawidłowościami po stronie dalszego podwykonawcy.
   - Podwykonawca mógłby przedstawiać zasady świadczenia usług przez dalszego podwykonawcę, w szczególności w formie Regulaminu czy Specyfikacji. Zasady zmiany tych dokumentów przez dalszego podwykonawcę powinny wiązać zleceniodawcę/bank.
   - Należałoby postulować zniesienie zakazu dalszego podoutsourcingu (art. 6a ust. 7 Prawa bankowego). Uprościłoby to wiele kwestii regulacyjno-prawnych. Zakaz ten nie przystaje do rzeczywistości i złożoności świata IT.

6. Proporcjonalne podejście do wymogów

   Jednym z ograniczeń regulacyjnych dotyczących outsourcingu bankowego jest bezwzględny obowiązek stosowania wszystkich narzędzi i obowiązków outsourcingowych określonych w obowiązujących przepisach (np. art. 6a-6d Prawa bankowego) w tym samym zakresie i wymiarze wobec wszystkich dostawców, niezależnie od skali jego działania, lub zakresu powierzanych mu prac. Powinna być możliwość stosowania tych narzędzi i obowiązków w oparciu o przeprowadzoną analizę ryzyka, przy uwzględnieniu zasady proporcjonalności.

   Przykładowo inne są możliwości dużego przedsiębiorcy, korzystającego z różnych centrów przetwarzania danych (CPD), do opracowania i realizacji planu awaryjnego, przy wykorzystaniu tych różnych CPD. Tymczasem mikroprzedsiębiorca lub mały przedsiębiorca, a wiele fintechów dostarczających innowacyjne rozwiązania, to właśnie podmioty nie dysponujące pokaźnymi zasobami, dopiero budujące swój potencjał rynkowy, nie ma takich samych możliwości do zagwarantowania realizacji planu awaryjnego, jak duży przedsiębiorca.

   Jest to istotny problem. Niewątpliwie niezbędne jest podejście oparte na ocenie ryzyka, a nie ograniczanie się do sztywnych zasad prawa. Z tego punktu widzenia usługi proponowane przez małego przedsiębiorcę, albo przez innowacyjny fintech

są bardzo ryzykowne i mogą wręcz zagrozić bezpieczeństwu banku, jeśli nie zostaną odpowiednio przetestowane. Jednak takie podejście prowadziłoby do błędnego koła: aby ocenić ryzyko podmiotu trzeba by było przetestować jego działanie, a nie można tego zrobić, ponieważ byłoby to zbyt duże ryzyko dla banku. W takiej sytuacji właściwym rozwiązanie byłoby testowanie w małej skali, w warunkach rzeczywistych, czyli w piaskownicy regulacyjnej.

7. Zgoda na dostęp do tajemnicy bankowej

Wymagania nadzoru bankowego dotyczące zbierania zgody i jej konkretności w zasadzie wykluczają ujawnianie tajemnicy bankowej wobec dostawcy usług na bazie zgody pochodzącej od klientów. Prowadzi to w efekcie do kwalifikowania szeregu usług, których związek z działalnością bankowa jest luźny, do zakresu outsourcingu bankowego.

Należałoby zatem oczekiwać zmian w prawie umożliwiających przekazywanie informacji objętych tajemnicą bankową do dostawców usług bez konieczności uzyskiwania zgód klienta przy spełnieniu przez bank warunków brzegowych takiego dzielenia się informację. Mogłoby to być przykładowo:

- dokonanie oceny ryzyka podmiotu,
- zawarcie umowy dotyczącej świadczenia usług, która zawiera klauzule dotyczące bezpieczeństwa danych (na kształt European Model Clauses dot. danych osobowych)
- nieograniczona odpowiedzialności takiego podmiotu względem podmiotu danych.

Jak się wydaje, ograniczenia jakim podlega dzielenie się z podmiotem trzecim informacjami objętymi tajemnicą bankową podlega w Polsce znacznie dalej idącym ograniczeniom niż w innych krajach europejskich. Dlatego ważne, by i w tym przypadku regulator dokonał analizy obecnych przepisów, ich wpływu na funkcjonowanie banków i – jeśli analiza wskazałby zasadność zastrzeżeń – przeprowadził odpowiednią korektę przepisów.