EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Stanowisko Europejskiego Kongresu Finansowego[1] w konsultacjach Europejskiego Urzędu Nadzoru Bankowego w sprawie wytycznych dotyczących outsourcingu[2]

Metodologia opracowania stanowiska

Opracowanie stanowiska przebiegało w następujących etapach:

Etap 1
Do wzięcia udziału w badaniu zaproszono grupę ekspertów z polskiego sektora finansowego. Przesłano im wybrane fragmenty dokumentu konsultacyjnego Europejskiego Urzędu Nadzoru Bankowego oraz przetłumaczone pytania konsultacyjne. Ekspertom zagwarantowana została anonimowość.

Etap 2
Zebrano odpowiedzi od ponad 30 ekspertów z:

- banków komercyjnych,
- firm z sektorów IT, FinTech oraz e-commerce,
- organów regulacyjnych,
- firm konsultingowych oraz kancelarii prawnych,
- środowiska akademickiego.

Etap 3
W ramach Klubu EKFintech prowadzonego przez Europejski Kongres Finansowy zorganizowano seminarium na temat regulacji outsourcingu w sektorze finansowym, w którym uczestniczyli eksperci zaproszeni do konsultacji oraz członkowie Klubu.

Etap 4
Na bazie uzyskanych opinii opracowana została propozycja syntezy odpowiedzi. Propozycję tę przekazano ekspertom, którzy wzięli udział w konsultacjach. Zwrócono się do nich z prośbą o zaznaczenie w syntezie tych sformułowań, które powinny zostać zmodyfikowane i zaproponowanie modyfikacji czy dodatkowych zapisów, jak również zaznaczenie tych opinii, z którymi się nie zgadzają i które powinny być z ostatecznej syntezy usunięte.

Etap 5
Na bazie uzyskanych odpowiedzi opracowana została ostateczna wersja syntetycznego stanowiska Europejskiego Kongresu Finansowego.

---

[1] Celem Europejskiego Kongresu Finansowego (www.efcongress.com) jest debata nt. bezpieczeństwa i stabilności systemu finansowego Unii Europejskiej i Polski.
[2] https://www.eba.europa.eu/documents/10180/2260326/Consultation+Paper+on+draft+Guidelines+on+outsourcing+arrangements+%28EBA-CP-2018-11%29.pdf

Odpowiedzi Europejskiego Kongresu Finansowego na pytania konsultacyjne

P1: Czy wytyczne dotyczące przedmiotu, zakresu, w tym stosowania wytycznych dla instytucji pieniądza elektronicznego i instytucji płatniczych, definicje i wdrożenie (cz. 2 i 3) są odpowiednie i wystarczająco jasne?

1.Definicje są na pozór jasne, aczkolwiek niektóre kwestie mogą wprowadzać niepotrzebny nadmiar pojęć. Sekcja rozpoczyna się definicją *outsourcingu / sub – outsourcingu* oraz wskazuje co to są funkcje krytyczne lub ważne i dotykają zagadnień przetwarzania danych w chmurze.

2. Zgodnie z przedmiotową definicją sub-outsourcing oznacza sytuację, w której usługodawca w ramach umowy outsourcingowej dalej przekazuje proces, usługę, działanie, lub ich części do innego usługodawcy. Proces, usługa czy działalnie nie są natomiast zdefiniowane, w związku z czym za sub-outsourcing można uznać zlecenie przez dostawcę jakiejkolwiek funkcji dotyczącej świadczonych przez niego usług. Ważne jest zatem ustalenie, co może być przedmiotem outsourcingu, ponieważ definicja w Wytycznych jest bardzo szeroka i w zasadzie mogłaby obejmować wszelkie usługi, czynności, procesy, które wspólnie składają się na działanie banku.

3.Wątpliwości pojawiają się przy pojęciu „Critical function", które jest znane z innych regulacji, ale inaczej definiowane (np. w BRRD). Autorzy mają tego świadomość jednak powinni wyeksponować ten fakt nie tylko w przypisie nr 11..

4.Podobnie nie jest jasne pojęcie przeglądu (*review)*. Biorąc pod uwagę, że zdarzenie polegające na odnowieniu (*renewal*) umowy może być bardzo odwleczone w czasie, może powstać luka co do istniejących umów, która spowoduje, że zbyt długo nie będą one dostosowane do nowych standardów

5.W odniesieniu do daty wprowadzenie Wytycznych – dla nowych i dotychczasowych umów outsourcingowych, terminy przejściowe należy uznać za wystarczające w celu odpowiedniego uzgodnienia z dostawcami usług nowych wymogów wynikających z Wytycznych. Wątpliwość może jednakże budzić konieczność uwzględnienia wymogów Wytycznych przy pierwszym odnowieniu umowy outsourcingowej po 30 czerwca 2019 roku – nie jest jasne, czy chodziłoby o każde pierwsze aneksowanie umowy outsourcingowej, czy też jedynie o sytuację przedłużenia umowy na kolejny okres?
6.Definicje chmury prywatnej, publicznej, wspólnej i hybrydowej zawierają w sobie odniesienie do niezdefiniowanego pojęcia „cloud infrastructure" (zamiast do zdefiniowanego pojęcia „cloud services"), co może budzić wątpliwości interpretacyjne.
7.Wskazanym byłoby też ograniczenie liczby podoutsourcerów w łańcuchu dostaw (ograniczenie ryzyka). Należałoby też poważnie rozważyć zakaz stosowania sub-outsourcingu w przypadku funkcji ważnych i krytycznych. Outsourcing zwiększa poziom ryzyka, sub-outsourcing jeszcze dodatkowo go powiększa. W przypadku funkcji ważnych

i krytycznych może to być groźne, zwłaszcza przy bardzo gęstych powiązaniach transgranicznych w unijnym sektorze bankowym.
Wytyczne powinny jasno określać czy dopuszczalny jest wielopoziomowy *sub-outsourcing*, tzn. czy dopuszczalnym jest, aby *sub-outsourcer* powierzał wykonanie części usług powierzonych mu przez outsourcera dalszym podmiotom (kolejnym *sub-outsourcerom*), czy też dopuszczalny jest tylko 1 poziom *sub-outsourcingu* – bezpośrednio pomiędzy outsourcerem i sub-outsourcerem. Treśc par. 60 lit. b sugeruje, że wielopoziomowy *sub-outsourcing* jest dopuszczalny, ale zagadnienie to jest kontrowersyjne i ze względu na praktyczną istotność, jest warte opisania i jasnego uregulowania.

P2: Czy wytyczne dotyczące zasady proporcjonalności i stosowania outsourcingu w grupie (cz. 4 Title I) są odpowiednie i wystarczająco jasne?

1.Przedstawione rozwiązania wydają się nie budzić zastrzeżeń. Kwestie dotyczące proporcjonalności zaprezentowane są w sposób zwięzły, lecz pełny i oddający ich istotę. W wytycznych znajduje się wskazanie, że podczas stosowania zasady proporcjonalności powinny być brane pod uwagę kryteria określone w tym zakresie w Wytycznych EUNB w sprawie zarządzania wewnętrznego. Zasady te są jasne i odpowiednio sformułowane. Odnoszą się one do grup unijnych. Dzięki temu wchodzące w jej skład banki podlegają tym samym zharmonizowanym przepisom. Ale nawet najlepsze przepisy nie wystarczą, jeśli nie będą należycie i jednolicie egzekwowane. Nie stanowi to problemu w bankach strefy euro, ponieważ podlegają one nadzorowi EBC, który – jako jedyny nadzorca – taką jednolitość gwarantuje. W takim przypadku nawet świadczenie usług w obszarze kontroli wewnętrznej nie musi być nadmiernie ryzykowne. Ale ryzyko to znacznie wzrasta, gdy unijny bank zależny znajduje się poza strefą euro i w związku z tym nadzorowany jest przez swego nadzorcę lokalnego. Dlatego Wytyczne powinny uwzględniać fakt, iż nie wszystkie banki unijne są nadzorowane przez EBC i w stosunku do pozostałych stosować bardziej restrykcyjne zasady.

2. Popieramy wprowadzenie zasady proporcjonalności na potrzeby stosowania wytycznych EBA w zakresie outsourcingu, w szczególności zasada proporcjonalności powinna mieć zastosowanie przy określaniu (na potrzeby stosowania wytycznej 10.3) dokładnego zakresu wymaganego dostępu do danych oraz infrastruktury podmiotów świadczących usługi outsourcingowe przez podmioty zobowiązane, ich organy nadzoru, czy inne podmioty przez nie zatrudnione (np. audytorów).

3.W kwestii stosowania outsourcingu w grupie doprecyzowania wymaga podejście określone w paragrafie. 18 – 19 Wytycznych. Występuje konieczność doprecyzowania, o jaki poziom skonsolidowany / sub-skonsolidowany chodzi ? Jak się wydaje, odwołanie się w Wytycznych do reżimu CRD/CRR wskazuje, że konsolidacja obejmowałby również inne niż instytucje podmioty (tj. instytucje finansowe, do których na poziomie indywidulanym zakres Wytycznych z założenia nie ma zastosowania). Byłoby to ze wszech miar pożądane, ale wymagałoby bardziej jednoznacznego ujęcia.

4.Zasady, procedury i mechanizmy, o których mowa w par. 1, muszą być kompleksowe i proporcjonalne w stosunku do charakteru, skali i złożoności rodzajów ryzyka nieodłącznie związanych z danym modelem biznesowym oraz działalnością danej instytucji. Uwzględnia się kryteria techniczne ustanowione w art. 76–95. Dyr. 2013/36/EU.

P3: Czy wytyczne zawarte w cz. 4 Title II, a w szczególności gwarancje, zapewniające właściwym władzom możliwość skutecznego nadzorowania działalności i usług instytucji kredytowych i firm inwestycyjnych oraz instytucji płatniczych wymagających zezwolenia lub rejestracji (tj. działań wymienionych w załączniku I do dyrektywy 2013/36 / UE i usług płatniczych wymienionych w załączniku I do dyrektywy (UE) 2366/2015) są odpowiednie i wystarczająco jasne, czy też należy wprowadzić dodatkowe zabezpieczenia?

1.Katalog uprawnień jest opisany dość szeroko i zawiera ważne wskazanie o uprawnieniach nadzoru w kraju trzecim, do którego jest kierowana usługa w oparciu o outsourcing. Dokument wskazuje, jakie uprawnienia nadzorcze ma instytucja i jakie działania może podjąć.

2. Brak jasnego wskazania, jakie sankcje może nakładać nadzór. Właściwym podejściem byłoby kierowanie się ogólnie stosowanymi zasadami, ale powinno to być potwierdzone w Wytycznych.

3. Wytyczne w punkcie 25 i 26 nie są do końca precyzyjne i wskazane byłoby ich przeformułowanie. Wynika z nich pośrednio, że wszystkie czynności mogą być przedmiotem outsourcingu (nie wymienia się żadnych ograniczeń), a więc i te, które wymagają licencjonowania. W szczególności oznaczałoby to, że outsourcingowi mogą podlegać czynności bankowe, które dany bank (A) będzie zlecał innemu bankowi (B), nawet w kraju trzecim. Mogłoby to prowadzić do obchodzenia w ten sposób zasady jednolitego paszportu przez bank z kraju trzeciego, przed czym, nie chroniłyby zasady sformułowane w paragrafie 26. W efekcie byłaby to zgoda na funkcjonowanie "empty shells".

4. Jak się wydaje, celem paragrafów 25 i 26 jest podkreślenie, że instytucja może zlecać wykonywanie licencjonowanych lub inaczej reglamentowanych czynności wyłącznie tym podmiotom, które – przy spełnieniu ekwiwalentności systemów prawnych – podlegają w swoim kraju co najmniej równoważnym wymaganiom, co w kraju instytucji zlecającej. Jest to racjonalny wymóg, ale wymaga bardziej jednoznacznego wskazania w treści Wytycznych.

5.Wydaje się, że wprowadzenie wymogu, aby instytucja umownie zobowiązała każdy podmiot świadczący usługi outsourcingowe do dostarczania wszelkich danych na żądanie regulatora właściwego dla instytucji, a w przypadku odmowy – obowiązek rozwiązania umowy outsourcingowej.

6.Ocena, czy spełniony jest wymóg par. 26 (a) dotyczący „*podlegania skutecznemu nadzorowi*" w odniesieniu do dostawcy z państwa trzeciego jest prosta w przypadku kraju, o ekwiwalentnym systemie nadzoru, z tym, że takiej oceny powinien dokonywać nadzorca, a nie instytucja, która z reguły nie ma odpowiednich narzędzi do oceny skuteczności nadzoru sprawowanego w państwie trzecim. Może ona jedynie sprawdzić fakt podlegania nadzorowi, ale nie oceni jego jakości czy skuteczności. Dalsze warunki (par. 26 b) i c)) dotyczące istnienia umowy pomiędzy właściwymi organami nadzoru oraz definiujące minimalny zakres współpracy wydają się wystarczającym zabezpieczeniem .

7.Co do zasady należy przyjąć, że dostęp do danych osobowych klientów przez podmiot trzeci możliwy jest jedynie na podstawie umowy outsourcingowej. Niemniej jednak powinny być przewidziane przypadki awaryjne, szczególnie uzasadnione, kiedy dostęp taki może uzyskać podmiot zewnętrzny bez umowy outourcingowej. Na przykład gdy żaden z podmiotów świadczących daną usługę (w praktyce dotyczyłoby to niemal wyłącznie serwisu IT) na podstawie umowy outsourcingowej nie byłby dostępny.

P4: Czy wytyczne w cz. 4 Title III sekcja 4 dotyczące polityki outsourcingu są odpowiednie i wystarczająco jasne?

1.Wytyczne dotyczące polityki outsourcingu są jasno napisane, a jednocześnie wydają się być opisane w sposób skomplikowany. Zawierają kluczowe elementy, jakie instytucja powinna wziąć pod uwagę, konstruując proces outsorcowania od podziału kompetencji i odpowiedzialności, poprzez planowania i weryfikację podmiotu, do którego przeniesiona zostanie określona część działalności po elementy związane z zaprzestaniem działalności.
Następujące kwestie budzą duże wątpliwości:

- Paragraf 31 lit c) mówi o outsourcingu funkcji kontroli wewnętrznej. Funkcje kontroli wewnętrznej, podobnie jak zarzadzania ryzykiem, nie powinny być zlecany przez bank nikomu, ponieważ są to najbardziej istotne elementy zarządzania bankiem, mające istotny wpływ na ryzyka działalności bankowej. O ile można rozważać pewne wyjątki od tej zasady, to tylko na przykład relacji w grupie nadzorowanej przez tego samego nadzorcę (np. bank uniwersalny i jego hipoteczny bank zależny w tym samym kraju), nie sposób uznać, że ten obszar outsourcingu może generować wysokie ryzyko, a co za tym idzie powinien być wyłączony z outsourcingu

- Paragraf 32 lit d) pozostaje w sprzeczności z paragrafem 31 lit c). Nie można jednocześnie dopuszczać outsourcingu funkcji kontroli wewnętrznej i oczekiwać od niej (słusznie) zgodności z paragrafem 32 d. Ta koncepcja wymaga przemyślenia, z uwzględnieniem organizacji obu instytucji (zleceniodawcy i wykonawcy), podległości, linii raportowania, itp.

- Paragraf 33 wymaga, aby polityka outsourcingu była zatwierdzana na poziomie zarządu. Ponieważ jednak ma ona zasadniczy wpływ na funkcjonowanie banku i

może nieść ze sobą dalekosiężne skutki, powinna być zatwierdzana na szczeblu rady nadzorczej.

2.Bank powinien uwzględnić w swej polityce stronę ekonomiczną tego przedsięwzięcia, wprowadzając zasady ustalania korzyści i kosztów oraz kryteria oceny opłacalności. Powinny się tu wreszcie znaleźć warunki brzegowe dla poszczególnych parametrów opisanych w sekcjach 9.1 – 9.3, których przekroczenie dyskwalifikowałoby dane przedsięwzięcie. Jest to istotne, ponieważ przy braku założonych na wstępie wartości granicznych realne stawałoby się niebezpieczeństwo kierowania się korzyściami biznesowymi kosztem ograniczania nadmiernego ryzyka.

3.Wytyczne przewidują wymóg powołania komórki/funkcji ds. outsourcingu raportującej bezpośrednio do organu zarządzającego instytucji, przy czym w takim przypadku należałoby zdecydowanie odnieść się do zasady proporcjonalności, przewidując również możliwość realizacji ww. funkcji na poziomie organu zarządzającego (szczególnie w mniejszych podmiotach, zwłaszcza w odniesieniu do instytucji płatniczych i instytucji pieniądza elektronicznego). W przypadku instytucji (przede wszystkim instytucji kredytowych) zasady ładu korporacyjnego w zakresie outsourcingu powinny wpisywać się w funkcjonujący w instytucjach model trzech linii obrony.

4.Przedmiotowe Wytyczne nie odnoszą się do przypadku, w którym instytucja, instytucja płatnicza lub instytucja pieniądza elektronicznego występowałaby w roli podmiotu świadczącego usługi na rzecz innych podmiotów (np. podmiotów z grupy) - do rozważenia pozostaje kwestia zaadresowania przez Wytyczne takiej okoliczności.

P5: Czy wytyczne w cz. 4 Title III sekcje 5-7 są odpowiednie i wystarczająco jasne?

1.Wytyczne odnoszące się do kwestii konfliktu interesów, planów ciągłości działania i funkcji audytu wewnętrznego są czytelne i wydają się jednoznaczne. Wytyczne wskazują m.in., że instytucje i instytucje płatnicze powinny, identyfikować, oceniać i zarządzać konfliktami interesów w kontekście outsourcingu, posiadać plany ciągłości działania w kontekście outsourcingu krytycznych i znaczących funkcji, jak również wskazują elementy, które powinny być zapewnione w ramach funkcji audytu wewnętrznego.

2.Sekcja 5 dotycząca konfliktu interesów jest napisana w sposób jasny. Byłoby jednak z korzyścią dla czytelności dla Wytycznych, gdyby zasady dotyczące konfliktu interesów zostały uzupełnione przykładami takich przypadków, w których ów konflikt nie jest bezpośrednio widoczny.

3.Sekcje 6 i 7 które poruszają temat planów kontynuacji działania oraz audytu wewnętrznego są opisane w skomplikowany, sposób aby za pomocą tych punktów odbiorca mógł ustalić podejście w poruszanych kwestiach.

4.W odniesieniu do zarządzania konfliktami interesów należałoby wprowadzić wymóg ujawniania przypadków zidentyfikowanych konfliktów interesów, których nie udało się rozwiązać, ze wskazaniem działań podjętych w celu łagodzenia konfliktów, wraz z oceną ich skuteczności. Należałoby też rozważyć, czy w przypadku nierozwiązanych konfliktów interesu możliwe jest bezpieczne stosowanie outsourcingu.

5.Zawarty w par. 40 wymóg włączenia dostawcy usług w planowanie ciągłości działania nie jest określony w sposób precyzyjny. Plan ciągłości działania powinien mieć zarówno dostawca usług, jak i zlecająca instytucja. Jako pierwszy powinien być uruchamiany plan dostawcy usług. Gdyby w zadanym czasie dostawca nie przywrócił świadczenia usług, uruchamiany by był plan instytucji.

P6: Czy wytyczne w cz. 4 Title III sekcja 8 dotyczące wymaganej dokumentacji są odpowiednie i wystarczająco jasne?

1.Rozdział dotyczący kwestii dokumentacji outsourcingu jest opisany szczegółowo z katalogiem informacji, jakie powinna zwierać dokumentacja. Dodatkowa sekcja jest poświęcona dokumentacji funkcji krytycznych oraz outsourcingu funkcji z wykorzystaniem przetwarzania w chmurze. Dodatkowo przyjęto opcję rozdziału pomiędzy dokumentacją outsourcingu krytycznego i pozostałego, co pokazuje dużą dbałość o precyzję.

2.Wymóg weryfikowania struktury udziałowej podmiotu, w szczególności gromadzenie i analizowanie informacji o głównym udziałowcu jest ze wszech miar wskazany. Powinien on jednak ograniczać się do czynności ważnych i krytycznych, oraz tych, w przypadku których może wystąpić konflikt interesów.

3.Uzasadnione jest prowadzenie rejestru umów/uzgodnień outsourcingowych w zaproponowanym w Wytycznych podziale na outsourcing „funkcji ważnych lub krytycznych" i pozostały outsourcing. Zasady prowadzenia takiego rejestru powinny określać procedury wewnętrzne. Rejestr powinien obejmować informacje dotyczące wymogu przekazania informacji o zamiarze zawarcia umowy outsourcingowej do właściwego organu nadzoru (w przypadku, kiedy taka notyfikacja jest wymagana), a w szczególności o dacie takiej notyfikacji oraz ewentualnej komunikacji z organem w tej sprawie/rozstrzygnięciach.

4.W ramach zawartych w Par. 47 wymogów dotyczących zawartości dokumentacji czynności podlegających outsourcingowi warto uwzględnić również odwołanie do zasobów IT (w szczególności systemów informatycznych) instytucji objętych zakresem umowy outsourcingowej.

5.Wprowadzenie zasad certyfikacji albo zezwoleń (ewentualnie obowiązek poddania się cyklicznym audytom) dla dostawców usług chmurowych świadczących usługi dla

podmiotów finansowych pozwoliłoby ograniczyć ilość dokumentacji oraz ograniczyłoby ryzyko korzystania z tego rodzaju usług.

6. Wymogi dokumentacyjne wskazujące na minimalny zakres informacji wydają się zawierać najbardziej istotny zestaw informacji z podziałem na te dotyczące umów outsourcingowych, dostawców i poddostawców usług, oraz dodatkowe, obejmujące minimalny zakres informacji odnoszący się do krytycznych i znaczących funkcji oraz tzw. dostawców usług w chmurze („cloud service providers").

P7: Czy wytyczne w cz. 4 Title IV sekcja 9.1 dotyczące oceny krytyczności lub znaczenia danej funkcji są odpowiednie i wystarczająco jasne?

1.Część 9.1 dość wyczerpująco odnosi się do oceny, na ile dana funkcja jest ważna lub krytyczna. Niemniej jednak należałoby jeszcze wyraźnie odnieść się do klasyfikowania poszczególnych czynności na poziomie jednostkowym i grupowym. Jest rzeczą oczywistą, że w grupie złożonej strukturze, czy zróżnicowanych podmiotach będzie zawsze można zidentyfikować czynności, które z perspektywie grupy są nieistotne, choć dla podmiotu, w którym występują, mogą mieć znaczenie krytyczne. Należałoby zatem wyraźnie stwierdzić, że klasyfikacja powinna być prowadzona na każdym z poziomów, a jeśli dana czynność zostanie zaklasyfikowana jako ważna lub krytyczna na którymkolwiek poziomie, to co najmniej na tym poziomie powinna ona być traktowana zgodnie z dokonana klasyfikacją. Byłoby rzeczą niewłaściwą, gdyby czynność sklasyfikowana jako ważna, lub krytyczna na poziomie, na przykład, podmiotu zależnego, nie była za taka uznana, ze względu na jej nieistotność w ujęciu grupowym.

2. Brakuje też wyraźnego wskazania, że ocena istotności powinna być dokonana przed podjęciem decyzji o outsourcingu danej czynności. Ponadto, instytucja powinna regularnie (np. raz na rok) dokonywać oceny, czy w instytucji miały miejsce zmiany, zdarzenia, itp., które miałyby wpływ na ocenę zleconych czynności.

P8: Czy wytyczne w cz. 4 Title IV sekcja 9.2 dotyczące procesu due diligence są odpowiednie i wystarczająco jasne?

1.Wytyczne dotyczące „*due diligence*" wydają się nie budzić wątpliwości. Wytyczne wskazują, że przed zastosowaniem outsourcingu instytucje i instytucje płatnicze w procesie wyboru i oceny dostawcy usług powinny się upewnić, że spełnia on szereg warunków dotyczących m.in. posiadania odpowiednich zdolności, możliwości, zasobów, struktury organizacyjnej i odpowiednich zezwoleń (jeżeli są wymagane). W wytycznych zawarta jest również lista dodatkowych czynników, które powinny być brane pod uwagę podczas „*due diligence*".

2.Nie ma natomiast wytycznych dotyczących np. odniesienia rezultatów badania do wytycznych tego jak powinno się je interpretować na potrzeby uznania czy dany

podmiot może być wykonawcą usług w ramach outsourcingu. Wytyczne w sekcji 9.2 dotyczące procesu due diligence powinny wprost wskazywać, iż proces ten może mieć charakter uproszczony, jeśli druga strona także jest instytucją lub instytucją płatniczą. Wskazane jest, dla jasności, rozszerzenie sekcji choćby o przykładowe, dopuszczalne metody ustalania informacji o dostawcy usług w ramach procesu due diligence – czy mogą być to dokumenty pochodzące od tego dostawcy, ankiety i oświadczenia wypełniane przez dostawcę, inne niezależne źródła.

3.Proponuje się uwzględnienie dodatkowo odniesienia do mechanizmów certyfikacji określonych w art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, oraz uchylenia dyrektywy 95/46/WE (dalej: GDPR), a także ewentualnego faktu podlegania przez danego dostawcę usług wymogom określonym dla dostawców usług cyfrowych w Dyrektywie NIS.

4.Z Wytycznych EBA powinno jednoznacznie wynikać, że obowiązek przeprowadzenia procesu „due diligence" obejmuje, oprócz podmiotów świadczących bezpośrednio usługę outsourcingową na rzecz instytucji, instytucji pieniądza elektronicznego czy instytucji płatniczych także dostawców usługi sub-outsourcingu (wybranych przez podstawowego dostawcę outsourcingowej usługi).

P9: Czy wytyczne w cz. 4 Title IV sekcja 9.3 dotyczące oceny ryzyka są odpowiednie i wystarczająco jasne?

1.Rozdział rozpoczyna się od odniesienia do zasady proporcjonalności, która nie jest wystarczająco zdefiniowana i pozostawia duży margines interpretacji. W tym miejscu powtórzona jest uwaga, jak przy kwestii proporcjonalności.

2.W odniesieniu do oceny ryzyka Wytyczne odnoszą się bezpośrednio do ryzyka operacyjnego i ryzyka koncentracji. Do rozważania (w odniesieniu do instytucji kredytowych i firm inwestycyjnych – przy zachowaniu zasady proporcjonalności) czy zasadna jest ocenianie ryzyk w odniesieniu do innych rodzajów ryzyk (np. ryzyko biznesowe, ryzyko strategiczne).

3. Ponieważ cała sekcja 9.3 odnosi się raczej do zarządzania ryzykiem niż wyłącznie do jego oceny, stąd propozycja zmiany jej tytuły na „Risk management of outsourcing arrangements".

4. Zgodnie z Wytycznymi dopuszczalny jest outsourcing łańcuchowy. Co jednak w przypadku, gdy zgodnie z prawodawstwem państwa członkowskiego nie jest to dozwolone (zezwolony jest natomiast sub-outsourcing wyłącznie do jednego poziomu)? Czy takie państwo może stosować swoje dotychczasowe, bardziej restrykcyjne podejście? W zakresie sub-outsourcingu warto rozważyć dodatkowo uwzględnienie

wymogu, aby odpowiedzialność w stosunku do usługobiorcy zawsze leżała po stronie głównego dostawcy usług (niezależnie od korzystania przez niego z poddostawców).

5.Ocena ryzyka braku lub ograniczenia możliwości odpowiedniego nadzoru nad czynnościami w przypadku istnienia długiego/ złożonego łańcucha sub-outsourcerów wydaje się być złożonym procesem, o niepewnym wyniku i stąd ten rodzaj ryzyka powinien być ustawowo mitygowany.

P10: Czy wytyczne w cz. 4 Title IV sekcja 10 dotyczące umowy outsourcingu są odpowiednie i wystarczająco jasne? Czy propozycje dotyczące korzystania z prawa dostępu i audytu mogą powodować poważne prawne lub praktyczne wyzwania dla instytucji kredytowych i firm inwestycyjnych oraz instytucji płatniczych?

1.Istnieje poważne ryzyko, że ważne postanowienia znajdujące się w punkcie 10.3 Wytycznych w części pozostaną martwe. Usługodawcy, zwłaszcza liczący się dostawcy usług IT, są zawsze zdecydowanie niechętni kontrolom, o których mowa w tym punkcie. Zważywszy na zasadę comply or explain istnieje duże ryzyko, że instytucje i władze nadzorcze, jako słabsza strona, będą odstępować od wymagań zapisanych w tym punkcie. Należałoby zatem dążyć do uregulowania tej kwestii w regulacji, a nie w wytycznych.

2.Kwestia dostępu instytucji, nadzoru, oraz audytora do danych i informacji stanowiących tajemnicę outsourcera budzi zawsze kontrowersje. Dlatego, aby zapewnić choć minimalny stopień porównywalności byłoby rzeczą pożyteczną wskazanie minimalnego zakresu informacji, do których kontrolujące podmioty muszą mieć zagwarantowany dostęp.

3. Pojawia się wątpliwość, czy wyrażony w par. 63 lit. b) obowiązek wskazania daty końcowej oznacza, że umowa outsourcingowa nie może być zawarta na czas nieokreślony. jeśli tak, powinno to być jednoznacznie wskazane.

4.Wskazane byłoby jednoznaczne stwierdzenie, że czynności zlecone outsourcerowi podlegają badaniu audytora co najmniej w takim zakresie, w jakim byłyby badane w trakcie audytu w zlecającej instytucji.

5.Wytyczne w par. 64 pkt c) nakładają wymóg uzgodnienia poziomu usług, które powinny zawierać precyzyjne ilościowe i jakościowe cele wydajności. Należy zwrócić uwagę, że nie dla każdej usługi jest to możliwe. Wydaje się zatem, że dodanie zastrzeżenia „o ile mają zastosowanie" pozwoli uniknąć niepotrzebnego tworzenia sztucznych konstrukcji wyłącznie na potrzeby uczynienia zadość Wytycznym.

6.Paragraf 65 lit. d) – treść postanowienia niezrozumiała, w zakresie w jakim w postanowieniu chodzi o zgodę na *sub-outsourcing,* dla jasności należałoby

doprecyzować, czy zgoda może być generalna, czy też instytucja powinna każdorazowo wyrażać zgodę na każdy *sub-outsourcing*

7.Paragraf 72 lit a) wprowadza wymóg zapewnienia- w ramach pisemnej umowy outsourcingowej, że usługodawca udziela instytucjom i ich właściwym władzom oraz każdej innej osobie pełny dostęp do wszystkich odpowiednich lokali biznesowych, w tym do pełnego zakresu urządzeń, systemów, sieci, informacji i danych wykorzystywanych do dostarczania zleconego procesu, usługi lub działalności, informacji finansowych, personelu i zewnętrznych audytorów usługodawcy ("prawa dostępu").

Wprowadzenie prawa dostępu uważamy za zbyt szerokie i tym samym powodujące utrudnienia zarówno natury prawnej, jak i praktycznej, a nadto powodujące zmaterializowanie się ryzyka, o którym mowa we wstępnie niniejszej odpowiedzi.

Udostępnienie sprzętu instytucji lub innym podmiotom wskazanym może doprowadzić do ujawnienia tajemnicy przedsiębiorstwa dostawcy, a nawet tajemnicy zawodowej. Wydaje się zatem, że prawo wstępu powinno zostać pozostawione wyłącznie organom nadzorczym nad instytucją. Natomiast samej instytucji należy przyznać umownie prawo otrzymania informacji, danych i wyjaśnień. Prawo dostępu można rozważyć jako nieobligatoryjne zobowiązanie dostawcy wyłącznie dla samej instytucji (a nie także innych podmiotów), z zastrzeżeniem uzgodnienia terminu oraz obecności wskazanej przez dostawcę osoby lub osób.

8.W sekcji 10.3 par. 75 wprowadzono możliwość przeprowadzania audytów organizowane wspólnie z innymi instytucjami. Rozwiązanie to może zostać uznane za ryzykowne dla dostawcy, który może oferować różne warunki współpracy i różny zakres usług dla innych instytucji. Wspólny audyt może doprowadzić do niecelowego ujawnienia tajemnicy przedsiębiorstwa dostawcy i jako taki powinien zależeć od zgody outsourcera. Proponujemy zatem wprowadzenie zastrzeżenia, że przeprowadzenie wspólnego audytu wymaga szczególnej, każdorazowej zgody dostawcy.

9.Paragraf 81 – zgodnie z treścią tego paragrafu umowa outsourcingowa powinna jasno wskazywać na możliwość wypowiedzenia jej przez instytucje zgodnie z przepisami prawa krajowego („*in accordance with national law*"). To stwierdzenie wymaga większej precyzji. W przypadku outsourcingu transgranicznego instytucja i outsourcer mogą działać w różnych reżimach prawnych. Nie jest jasne czy chodzi o przepisy prawa krajowego właściwe dla instytucji, czy dostawcy usług? Umowa outsourcingowa może być zawarta pod prawem obcym, innym niż właściwe dla instytucji, zwłaszcza w sytuacji, w której dostawca usług jest z państwa trzeciego.

10.Przewidziane w Wytycznych „prawa dostępu" i „prawa audytu" należy uznać za istotne narzędzia kontroli powierzonych czynności, jednakże w praktyce ich zastosowanie może być istotnie utrudnione. Co więcej, wprowadzenie do umów outsourcingowych nieograniczonego prawa dostępu do siedziby/miejsca wykonywania operacji („all relevant business premises") może być problematyczne ze strony

dostawców usług. Może być to trudne, kiedy dostawcą jest instytucja nadzorowana lub podmiot świadczący usługi na rzecz kilku różnych instytucji/instytucji płatniczych czy instytucji pieniądza elektronicznego.Tryb „kontroli na miejscu" powinien być zapewniony wyłączenie w odniesieniu do outsourcingu funkcji krytycznych i ważnych, zgodnie z zasadą proporcjonalności.

11.Przewidziana w Wytycznych instytucji „pooled audits", czyli audytów organizowanych wspólnie z innymi klientami tego samego dostawcy usług, może w wielu przypadkach być wyzwaniem, biorąc pod uwagę aspekt konkurencji pomiędzy instytucjami, jak również tajemnicę handlową. Ponadto, nie jest jasne czy, a jeśli tak – w jakim zakresie, „prawo dostępu" i „prawo audytu" miałyby zastosowanie do podwykonawców dostawcy usługi (sub-outsourcing).

12. Wytyczne nie onoszą się do odpowiedzialności kontraktowej outsource'era. Oznacza to przeniesienie wytycznych na poziom lokalnego nadzoru i/lub ograniczenie go do zapisów kontraktowych, co może być bardzo niekorzystne dla mniejszych organizacji, takich, których siła negocjacyjna wobec dostawców jest mniejsza. W efekcie, wytyczne w obecnej postaci wprowadzają nierówne traktowania banku i outsourcera. Powinno się jednak przyjąć, jako zasadę, że wykonawca odpowiada za spowodowane straty banku, a w konsekwencji również klienta, do wysokości faktycznie poniesionej straty. Doświadczenia zebrane na rynku nakazują dodanie, że odpowiedzialność wykonawcy za spowodowane przez niego, udokumentowane straty nie może być ograniczana w umowie z bankiem, ani w żaden inny sposób. Dlatego jego odpowiedzialność wobec banku musi być jasno zdefiniowana w kontrakcie.

P11: Czy wytyczne w cz. 4 Title IV sekcja 11 dotyczące nadzoru nad ustaleniami o outsourcingu są odpowiednie i wystarczająco jasne?

1. Wytyczne dotyczące nadzoru nad funkcjami, które podlegają outsourcingowi, wydają się klarowne. Wytyczne zawarte w sekcji 11 wyczulają zlecającego usługi outsourcingu na pewnego rodzaju ciągłość tego procesu i konieczność stałego monitorowania tego, co dzieje się u dostawcy. Największym wyzwaniem będzie wymóg: "*payment institutions should follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirement",* ponieważ w praktyce będzie on oznaczał stały nadzór nad tym, co robi dostawca i czy jego działalność jest zgodna z przepisami.

2.W odniesieniu do nadzoru nad uzgodnieniami w zakresie outsourcingu, w ramach systemu informacji zarządczej funkcjonujących w instytucjach należałoby przewidzieć oprócz raportów przekazywanych do organu zarządzającego, również odpowiednie informacje przekazywane do komitetów (o ile funkcjonują w banku), jak również okresowe sprawozdania do rady nadzorczej.

P12: Czy wytyczne w cz. 4 Title IV sekcja 12 dotyczące strategii wyjścia są odpowiednie i wystarczająco jasne?

1.Wytyczne dotyczące strategii wyjścia wydają się być napisane jasno. Jednocześnie rozdział zawiera wiele elementów, jakie, powinna wziąć pod uwagę instytucja, która spisuje plany wyjścia jako rodzaj zabezpieczenia na wypadek potrzeby rozwiązania umowy o outsourcing. Obok takich elementów, jak potrzeba dokładnego udokumentowania planów wyjścia, EBA wskazuje na potrzebę przetestowania planów oraz zabezpieczenia nowego dostawcy usług na okres po opuszczeniu dotychczasowego.

2.Reguły „wyjścia" są przedstawione jasno i przejrzyście. Do rozważanie pozostaje, czy ta sekcja nie powinna stanowić elementów umowy outsourcingowej oraz czy powinna być wyraźnie umieszczona w wewnętrznych regulacjach.

3.W ramach strategii zakończenia współpracy podmiot outsourcujący usługę powinien mieć zagwarantowaną w warunkach umowy możliwość bezpiecznego zakończenia korzystania z usługi, w tym zwrot danych w odpowiednim formacie, zakresie i trybie, a także powinien mieć opracowane odpowiednie plany ciągłości działania na tę okoliczność.

P13: Czy wytyczne w cz. 4 Title IV sekcja 13 są odpowiednie i wystarczająco jasne, w szczególności czy istnieją sposoby ograniczania informacji w rejestrze, które instytucje kredytowe i firmy inwestycyjne oraz instytucje płatnicze są zobowiązane przekazać właściwym organom jako istotne i zgodne z zasadą proporcjonalności? Aby zapewnić odpowiednią proporcjonalność, EBA rozważy wartość i znaczenie dla nadzoru rejestru obejmującego wszystkie ustalenia dotyczące outsourcingu w ramach każdego cyklu SREP lub co najmniej co 3 lata w odniesieniu do obciążenia operacyjnego i administracyjnego.

1. Patrząc z perspektywy treści Wytycznych w zakresie możliwości ograniczania informacji w rejestrze, wydaje się, że są one na tyle precyzyjne i wyczerpujące, że nie pozostaje wiele pola do ograniczania zakresu przekazywanych informacji do regulatora, zwłaszcza w sytuacji przeglądu informacji na żądanie.

2.Ponieważ celem Wytycznych jest m.in. wprowadzenie jednolitych zasad dotyczących outsourcingu w Państwach Członkowskich, sekcja ta powinna uregulować wprost kwestie wyrażania zgody na outsourcing przez organy nadzoru. Po pierwsze, czy taki wymóg powinien istnieć, a jeśli tak, to w jakich okolicznościach zgoda powinna być wymagana. Szczególnie istotne byłoby wyraźne rozstrzygnięcie, czy zawarcie umowy outsourcingowej z podmiotem z innego kraju (również członkowskiego) wymaga jedynie poinformowania, czy jednoznacznej zgody nadzoru. W pierwszym przypadku nadzór opierałby się na zapewnieniu instytucji, że wymogi Wytycznych są spełnione, a ewentualne nieprawidłowości byłyby identyfikowane w trakcie działań nadzorczych, gdy umowa jest już od pewnego czasu wykonywana. W drugim przypadku nadzór

weryfikowałby zgodność z Wytycznymi i udzielał zgody po uzyskaniu tej zgodności Zgoda w przypadku wykonawcy z kraju członkowskiego wiązałaby się przede wszystkim z możliwością wykonywania funkcji kontrolnych przez samą instytucję, nadzór, oraz audytora. To drugie podejście pozwoliłoby uniknąć niepotrzebnych kosztów, gdyby nieprawidłowości zostały stwierdzone w trakcie normalnej działalności.

3. Nie znajduje uzasadnienia żądanie przedstawiania raz na 3 lata rejestru umów outsourcingowych. Rejestr taki powinien być dostępny jedynie na żądanie i w czasie kontroli prowadzonej przez organ nadzorczy. Wynikające z wytycznych uzasadnienie badania przez organ nadzorczy faktu konsolidacji usług outsourcingowych na rynku czy istnienia wąskiej grupy outsourcerów dla wielu dostawców może być z powodzeniem realizowane w trybie weryfikacji ad hoc.

P14: Czy wytyczne dla właściwych organów w cz. 4 Title V są odpowiednie i wystarczająco jasne?

1.Wytyczne dla właściwych organów powinny zostaćwkomponowane / wspólne z zasadami przeprowadzenia badania i oceny nadzorczej (SREP). Wśród czynników branych pod uwagę przez właściwe organy przy ocenie ustaleń w zakresie outsourcingu funkcjonujących w instytucjach należy uwzględnić ryzyko systemowe generowane przez daną instytucję, w tym status instytucji jako G-SIIF lub O-SIIF. Ponadto, uzasadniona wydaje się w tym zakresie współpraca właściwych organów i organów „resoulution" w celu skoncentrowania uwagi nadzorczej nad ustaleniami w zakresie outsourcingu w odniesieniu do instytucji systemowo ważnych, pełniących funkcje krytyczne dla systemu finansowego i gospodarki realnej.

2. Proponuje się uwzględnienie sugestii współpracy przez organy nadzoru instytucji finansowych z organami nadzoru dla dostawców usług cyfrowych określonymi w Dyrektywie NIS. Wprowadzenie zasady wzajemnego informowania o istotnych nieprawidłowościach dotyczących dostawców usług outsourcingu, jako element umowy pomiędzy właściwymi organami nadzoru, znacznie przyczyniłby się do ograniczenia ryzyka outsourcingu.

P16: Czy ustalenia i wnioski z oceny skutków są właściwe? W przypadku dodatkowych obciążeń, w szczególności kosztów finansowych, proszę podać opis obciążenia oraz, w możliwym zakresie, oszacować koszty wdrożenia wytycznych, różnicując koszty jednorazowej i bieżące oraz czynniki kosztów (np. zasoby ludzkie, IT, koszty administracyjne itp.

1. W analizie nie zostały wskazane wyzwania i ewentualne koszty związane z tzw. *Brexitem*. Wyjście UK z UE spowoduje, że ośrodki w tym infrastruktura IT - znajdujące się dotychczas w UE staną się lokalizacjami państw trzecich. Dodatkowo wydaje się, że znaczącym wysiłkiem po stronie instytucji finansowych będzie przeniesienie

określonych działalności do outsourcingu wykonywanego w formule chmury. Formuła ta będzie wiązać się z kosztami przede wszystkim IT oraz osobowymi (eksperci IT).

2.Należy wziąć pod uwagę podział czynności na dwie grupy: ważne lub krytyczne, oraz pozostałe. W przypadku pierwszej grupy niezbędny jest duży konserwatyzm. Tym większy, że Wytyczne w swoim obecnym kształcie nie przewidują, by konkretne czynności nie mogły być outsourcowane

3.Nie można lekceważyć ryzyka powstawania w niektórych krajach członkowskich banków zależnych od podmiotów z krajów trzecich, które – za zgodą lokalnego nadzoru – wyprowadzą szereg istotnych czynności do firmy matki. Mogą temu przeszkodzić sprawy formalne. Ale jeśli będą one uporządkowane ograniczenie skali outsourcingu czy jego zakresu merytorycznego byłoby bardzo trudne.
Podsumowując:

- wytyczne powinny wskazywać czynności, których outsourcować nie wolno, w tym kontrola wewnętrzna, zarządzanie ryzykiem, czynności licencjonowanie;
- outsourcing czynności ważnych lub krytycznych powinien być możliwy jedynie na podstawie jednoznacznej zgody nadzoru, tak jak przy licencjonowaniu;
- outsourcing do kraju trzeciego powinien być możliwy jedynie na podstawie jednoznacznej zgody nadzoru, tak jak przy licencjonowaniu;
- umowa outsourcingu koniecznie powinna zawierać jednoznaczne postanowienie dotyczące odpowiedzialności outsourcera za straty banku / klienta do wysokości strat, wynikające z niewłaściwego wykonania umowy lub niewykonania jej;
- zabezpieczenia przed tworzeniem banków o charakterze „empty shells" powinno być dopracowane, ponieważ taki model biznesowy banku zależnego w kraju członkowskim może być w pełni zgodny z projektowanymi wytycznymi.

4. Rozpoczęcie stosowania wobec potencjalnych outsourcerów choćby „due diligence" wiąże się z ogromnymi jednostkowymi kosztami badania. Poniesienie tych kosztów ma uzasadnienie jedynie dla outsourcingu kwalifikowanego. Niezrozumienie budzi stosowanie wszystkich wymogów w odniesieniu do outsourcerów bez względu na to, czy outsourcingiem objęte są zwykłe czy istotne czynności operacyjne.