

EBA/GL/2019/02

25 lutego 2019 r.

Wytyczne w sprawie outsourcingu

1. Obowiązki w zakresie zgodności z przepisami i sprawozdawczości

Status niniejszych wytycznych

1. Niniejszy dokument zawiera wytyczne wydane na mocy art. 16 rozporządzenia (UE) nr 1093/2010¹. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy i instytucje finansowe dokładają wszelkich starań, aby zastosować się do wytycznych.
2. W wytycznych podano stanowisko EUNB w sprawie właściwych praktyk nadzorczych w ramach Europejskiego Systemu Nadzoru Finansowego oraz w sprawie tego, jak należy stosować prawo Unii w danym obszarze. Właściwe organy określone w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez wprowadzenie ich odpowiednio do swoich praktyk (np. poprzez dostosowanie swoich ram prawnych lub procesów nadzorczych), również jeżeli wytyczne są skierowane przede wszystkim do instytucji.

Wymogi w zakresie sprawozdawczości

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 w terminie do ([dd.mm.rrrr]) właściwe organy muszą powiadomić EUNB, czy stosują się lub czy zamierzają zastosować się do niniejszych zaleceń, albo podać uzasadnienie niestosowania się do nich. Jeżeli w wyznaczonym terminie właściwe organy nie prześlą żadnego powiadomienia, EUNB uzna, że nie stosują się do niniejszych wytycznych. Informacje należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB na adres compliance@eba.europa.eu z dopiskiem „EBA/GL/2019/02”. Powiadomienia przekazują osoby odpowiednio upoważnione do informowania o stosowaniu się do wytycznych w imieniu właściwych organów. Wszelkie zmiany dotyczące stosowania się do wytycznych także należy zgłaszać do EUNB.
4. Powiadomienia zostaną opublikowane na stronie internetowej EUNB, zgodnie z art. 16 ust. 3.

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

2. Przedmiot, zakres stosowania i definicje

Przedmiot

5. Niniejsze wytyczne określają ustalenia dotyczące zasad zarządzania wewnętrznego, w tym rozsądnego zarządzania ryzykiem, które instytucje, instytucje płatnicze oraz instytucje pieniądza elektronicznego powinny wdrażać przy outsourcingu funkcji, w szczególności w przypadku outsourcingu funkcji krytycznych lub ważnych.
6. W niniejszych wytycznych określono, w jaki sposób ustalenia, o których mowa we wcześniejszym ustępie, powinny być poddawane przeglądowi i monitorowane przez właściwe organy w kontekście art. 97 dyrektywy 2013/36/UE², procesu przeglądu i oceny nadzorczej (SREP), art. 9 ust. 3 dyrektywy (UE) 2015/2366³, art. 5 ust. 5 dyrektywy 2009/110/WE⁴ poprzez wypełnianie obowiązku monitorowania zachowania ciągłej zgodności z warunkami określonymi w zezwoleniu przez podmioty, do których niniejsze wytyczne są skierowane.

Adresaci

7. Niniejsze wytyczne skierowane są do właściwych organów określonych w art. 4 ust. 1 pkt 40 rozporządzenia (UE) nr 575/2013⁵, w tym Europejskiego Banku Centralnego w odniesieniu do spraw związanych z powierzonymi mu zadaniami zgodnie z rozporządzeniem (UE) nr 1024/2013⁶; instytucji kredytowych określonych w art. 4 ust. 1 pkt 3 rozporządzenia (UE) 575/2013; instytucji płatniczych określonych w art. 4 ust. 4 dyrektywy (UE) 2015/2366 oraz instytucji pieniądza elektronicznego w rozumieniu art. 2 ust. 1 dyrektywy 2009/110/WE. Dostawcy świadczący usługę dostępu do informacji o rachunku, którzy świadczą jedynie usługę, o której mowa w załączniku I pkt 8 do dyrektywy (UE) 2015/2366 nie są objęci zakresem stosowania niniejszych wytycznych zgodnie z art. 33 tej dyrektywy.

² Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE.

³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE.

⁴ Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE.

⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 176 z 27.6.2013, s. 1).

⁶ Rozporządzenie Rady (UE) nr 1024/2013 z dnia 15 października 2013 r. powierzające Europejskiemu Bankowi Centralnemu szczególne zadania w odniesieniu do polityki związanej z nadzorem ostrożnościowym nad instytucjami kredytowymi

8. Dla celów niniejszych wytycznych wszelkie odniesienia do „instytucji płatniczych” obejmują „instytucje pieniądza elektronicznego”, a wszelkie odniesienia do „usług płatniczych” obejmują „emisję pieniądza elektronicznego”.

Zakres stosowania

9. Bez uszczerbku dla dyrektywy 2014/65/UE⁷ i rozporządzenia delegowanego Komisji (UE) 2017/565⁸ (które zawiera wymogi dotyczące outsourcingu przez instytucje wykonujące zawodowo usługi inwestycyjne oraz prowadzące działalność inwestycyjną, jak również odpowiednie wytyczne wydane przez Europejski Urząd Nadzoru Giełd i Papierów Wartościowych w odniesieniu do usług inwestycyjnych i działalności inwestycyjnej), instytucje, o których mowa w art. 3 ust. 1 lit. c) dyrektywy 2013/36/UE, powinny spełniać niniejsze wytyczne na zasadzie indywidualnej, subskonsolidowanej i skonsolidowanej. Zastosowanie ujęcia indywidualnego może zostać uchylone przez właściwe organy na podstawie art. 21 dyrektywy 2013/36/UE lub art. 109 ust. 1 dyrektywy 2013/36/UE w związku z art. 7 rozporządzenia (UE) nr 575/2013. Instytucje podlegające dyrektywie 2013/36/UE powinny stosować się do tej dyrektywy oraz niniejszych wytycznych na zasadzie skonsolidowanej i subskonsolidowanej, zgodnie z art. 21 oraz art. 108–110 dyrektywy 2013/36/UE.
10. Bez uszczerbku dla art. 8 ust. 3 dyrektywy (UE) 2015/2366 i art. 5 ust. 7 dyrektywy 2009/110/WE instytucje płatnicze i instytucje pieniądza elektronicznego powinny przestrzegać niniejszych wytycznych w ujęciu indywidualnym.
11. Właściwe organy odpowiedzialne za nadzorowanie instytucji, instytucji płatniczych oraz instytucji pieniądza elektronicznego powinny przestrzegać niniejszych wytycznych.

Definicje

12. O ile nie określono inaczej, pojęcia stosowane i zdefiniowane w dyrektywie 2013/36/UE, rozporządzeniu (UE) nr 575/2013, dyrektywie 2009/110/WE, dyrektywie (UE) 2015/2366 lub w Wytycznych EUNB w sprawie zarządzania wewnętrznego⁹ mają w niniejszych wytycznych takie samo znaczenie. Ponadto do celów niniejszych wytycznych stosuje się następujące definicje:

Outsourcing	oznacza umowę w dowolnej formie zawartą między instytucją, instytucją płatniczą lub instytucją pieniądza elektronicznego a usługodawcą, na mocy której usługodawca realizuje proces, usługę lub zadanie, które w przeciwnym razie byłoby realizowane przez
-------------	--

⁷ Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.U. L 173 z 12.6.2014, s. 349)

⁹ <https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised->

	samą instytucję, instytucję płatniczą lub instytucję pieniądza elektronicznego.
Funkcja	oznacza wszelkie procesy, usługi lub działania.
Funkcja krytyczna lub ważna ¹⁰	oznacza dowolną funkcję uznaną za krytyczną lub ważną w myśl części 4 niniejszych wytycznych.
Podoutsourcing	oznacza sytuację, w której usługodawca związany umową outsourcingu przekazuje powierzona sobie funkcję kolejnemu usługodawcy ¹¹ .
Usługodawca	oznacza podmiot zewnętrzny, który podejmuje się realizacji procesu, usługi lub zadania będącego przedmiotem outsourcingu lub ich części na podstawie umowy outsourcingu.
Usługi w chmurze	oznaczają usługi dostarczone przy wykorzystaniu przetwarzania w chmurze, to znaczy modelu umożliwiającego dogodny dostęp na żądanie z dowolnego miejsca, za pośrednictwem sieci, do wspólnej puli konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, przechowywania danych, aplikacji i usług), które można szybko zapewniać i udostępniać przy minimalnych działaniach w zakresie zarządzania czy też minimalnej interakcji z dostawcą usługi.
Chmura publiczna	oznacza infrastrukturę chmury dostępną do użytku publicznego.
Chmura prywatna	oznacza infrastrukturę chmury dostępną do wyłącznego użytku jednej instytucji lub instytucji płatniczej.
Chmura społecznościowa	oznacza infrastrukturę chmury dostępną do wyłącznego użytku konkretnej wspólnoty instytucji lub instytucji płatniczych, w tym kilku instytucji z jednej grupy.
Chmura hybrydowa	oznacza infrastrukturę chmury złożoną z dwóch lub więcej odrębnych infrastruktur chmury.
Organ zarządzający	oznacza organ lub organy instytucji lub instytucji płatniczej, które są powoływane zgodnie z prawem krajowym, uprawnione do ustalania strategii, celów i ogólnego kierunku funkcjonowania instytucji lub instytucji płatniczej, nadzorują i monitorują decyzje zarządcze i skupiają osoby, które faktycznie

¹⁰ Sformułowanie „funkcja krytyczna lub ważna” [funkcja o podstawowym lub ważnym znaczeniu] opiera się na brzmieniu dyrektywy 2014/65/UE (MiFID II) oraz rozporządzenia delegowanego Komisji (UE) 2017/565 uzupełniającego dyrektywę MiFID II i stosowane jest wyłącznie dla celów outsourcingu; nie jest powiązane z definicją „funkcji krytycznych” dla celów ram restrukturyzacji i uporządkowanej likwidacji zawartą w art. 2 ust. 1 pkt 35 dyrektywy 2014/59/UE (dyrektywy BRRD).

¹¹ Dla celów oceny mają zastosowanie zapisy zawarte w części 3; podoutsourcing w innych dokumentach EUNB określany jest również mianem „łańcucha outsourcingowego” lub „outsourcingu łańcuchowego”;

kierują działalnością instytucji lub instytucji płatniczej oraz członków zarządu i osoby odpowiedzialne za zarządzanie instytucją płatniczą.

3. Wdrożenie

Data rozpoczęcia stosowania

13. Z zastrzeżeniem ust. 63 lit. b) niniejsze wytyczne mają zastosowanie od dnia 30 września 2019 r. do wszystkich umów outsourcingu zawartych, odnowionych lub zmienionych po tej dacie. Ustęp 63 lit. b) ma zastosowanie od dnia 31 grudnia 2021 r.
14. Instytucje i instytucje płatnicze powinny dokonywać przeglądu i odpowiednich zmian istniejących umów outsourcingu w celu zapewnienia zgodności z niniejszymi wytycznymi.
15. Jeżeli przegląd umów outsourcingu krytycznych lub ważnych funkcji nie zakończy się do 31 grudnia 2021 r., instytucje i instytucje płatnicze powinny powiadomić właściwy organ o tym fakcie, w tym o działaniach, które planuje się w celu zakończenia przeglądu lub, potencjalnej strategii wyjścia.

Przepisy przejściowe

16. Instytucje i instytucje płatnicze powinny uzupełnić dokumentację wszystkich istniejących umów outsourcingu innych niż umowy outsourcingu zawarte z dostawcami usług w chmurze zgodnie z niniejszymi wytycznymi po pierwszej dacie odnowy każdej z istniejących umów outsourcingu, przy czym nie później niż w dniu 31 grudnia 2021 r.

Uchylenie

17. Wytyczne Komitetu Europejskich Organów Nadzoru Bankowego (CEBS) z dnia 14 grudnia 2006 r. dotyczące zlecenia zadań dostawcom usług oraz zalecenia EUNB dotyczące outsourcingu w chmurze¹² zostają uchylone z dniem 30 września 2019 r.

¹² Zalecenia dotyczące zlecenia zadań dostawcom usług w chmurze (EBA/REC/2017/03).

4. Wytyczne w sprawie outsourcingu

Tytuł I — Zasada proporcjonalności: stosowanie w ramach grupy i instytucjonalne systemy ochrony

1 Zasada proporcjonalności

18. Instytucje, instytucje płatnicze i właściwe organy stosując niniejsze wytyczne lub sprawując nadzór nad ich stosowaniem, uwzględniają zasadę proporcjonalności. Celem zasady proporcjonalności jest zapewnienie, aby zasady zarządzania, w tym te dotyczące outsourcingu, były spójne z indywidualnym profilem ryzyka, charakterem i modelem biznesowym instytucji lub instytucji płatniczej oraz skalą i złożonością jej działalności, tak aby skutecznie osiągnąć cele wymogów regulacyjnych.
19. Instytucje i instytucje płatnicze stosując wymogi określone w treści niniejszych wytycznych, powinny uwzględniać złożony charakter funkcji zleczanych na zasadzie outsourcingu, ryzyko wynikające z umowy outsourcingu, krytyczne lub istotne znaczenie funkcji zleczanej na zasadzie outsourcingu oraz potencjalny wpływ outsourcingu na ciągłość wykonywanej działalności.
20. Instytucje, instytucje płatnicze¹³ i właściwe organy stosując zasadę proporcjonalności, powinny uwzględniać kryteria określone w tytule I wytycznych EUNB w sprawie zarządzania wewnętrznego zgodnie z art. 74 ust. 2 dyrektywy 2013/36/UE.

2 Outsourcing przez grupy i instytucje będące członkami instytucjonalnego systemu ochrony

21. Zgodnie z art. 109 ust. 2 dyrektywy 2013/36/UE, niniejsze wytyczne stosuje się również na zasadzie subskonsolidowanej i skonsolidowanej z uwzględnieniem zakresu konsolidacji ostrożnościowej.¹⁴ W tym celu podmioty dominujące w UE lub podmiot dominujący w państwie członkowskim powinny zapewnić, aby wewnętrzne zasady, procesy i mechanizmy zarządzania obowiązujące w ich podmiotach zależnych, w tym w instytucjach płatniczych były spójne,

¹³ Instytucje płatnicze powinny odnieść się również do wytycznych EUNB dotyczących informacji, które należy przedstawić w celu uzyskania zezwolenia przez instytucje płatnicze i instytucje pieniądza elektronicznego oraz zarejestrowania dostawców świadczących usługi dostępu do informacji o rachunku na podstawie dyrektywy (UE) 2015/2366, które są dostępne na stronie internetowej EUNB pod następującym adresem: <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2>

¹⁴ Zakres konsolidacji określa art. 4 ust. 1 pkt 47 i 48 rozporządzenia (UE) nr 575/2013.

dobrze zintegrowane i adekwatne do celów skutecznego stosowania niniejszych wytycznych na wszystkich odpowiednich szczeblach.

22. Instytucje i instytucje płatnicze, zgodnie z ust. 21, oraz instytucje, które jako członkowie instytucjonalnego systemu ochrony, stosują zasady zarządzania określone na szczeblu centralnym, powinny spełniać następujące warunki:
- a. w sytuacji gdy takie instytucje lub instytucje płatnicze zawarły umowy outsourcingu z dostawcami usług w ramach grupy lub instytucjonalnego systemu ochrony¹⁵, organ zarządzający takich instytucji lub instytucji płatniczych ponosi pełną odpowiedzialność, również w odniesieniu do takich umów outsourcingu, za zgodność ze wszelkimi wymogami regulacyjnymi oraz skuteczne stosowanie niniejszych wytycznych;
 - b. w sytuacji gdy takie instytucje lub instytucje płatnicze zlecają na zasadzie outsourcingu zadania operacyjne funkcji kontroli wewnętrznej dostawcy usług w ramach grupy lub instytucjonalnego systemu ochrony, w zakresie monitorowania i audytu umów outsourcingu instytucje dopilnowują, również w odniesieniu do takich umów outsourcingu, aby takie zadania operacyjne były realizowane skutecznie, w tym poprzez otrzymywanie odpowiednich sprawozdań.
23. W uzupełnieniu ust. 22 instytucje i instytucje płatnicze należące do grupy, w odniesieniu do których nie udzielono zwolnienia na podstawie art. 109 dyrektywy 2013/36/UE i art. 7 rozporządzenia (UE) nr 575/2013, instytucje będące organem centralnym lub są trwale powiązane z organem centralnym, w odniesieniu do których nie udzielono zwolnienia na podstawie art. 21 dyrektywy 2013/36/UE, lub instytucje będące członkami instytucjonalnego systemu ochrony powinny uwzględniać co następuje:
- a. W sytuacji gdy operacyjne monitorowanie outsourcingu jest scentralizowane (np. w ramach umowy ramowej dotyczącej monitorowania umów outsourcingu), instytucje i instytucje płatnicze dopilnowują, przynajmniej w odniesieniu do krytycznych lub istotnych funkcji zleczanych na zasadzie outsourcingu, aby możliwe było zarówno niezależne monitorowanie dostawcy usług jak i sprawowanie odpowiedniego nadzoru przez każdą instytucję lub instytucję płatniczą, w tym poprzez otrzymywanie, co najmniej raz do roku oraz na wniosek scentralizowanej funkcji monitorowania, sprawozdań obejmujących co najmniej podsumowanie oceny ryzyka i monitorowania wyników. Ponadto instytucje i instytucje płatnicze powinny otrzymywać od scentralizowanej funkcji monitorowania streszczenie odpowiednich sprawozdań z audytu dotyczących outsourcingu krytycznych lub istotnych funkcji oraz, na żądanie, pełne sprawozdanie z audytu.

¹⁵ Zgodnie z art. 113 ust. 7 rozporządzenia w sprawie wymogów kapitałowych (CRR), instytucjonalny system ochrony stanowi umowne lub ustawowe uzgodnienie w sprawie odpowiedzialności, które chroni te instytucje, które są członkami systemu, a w szczególności gwarantuje ich płynność i wypłacalność w celu uniknięcia upadłości, gdyby okazała się ona konieczna.

- b. Instytucje i instytucje płatnicze dopilnowują, aby ich organ zarządzający był należycie informowany o istotnych planowanych zmianach dotyczących dostawców usług monitorowanych na szczeblu centralnym oraz potencjalnym wpływie takich zmian na krytyczne i istotne funkcje, w tym otrzymywał podsumowanie analizy ryzyka obejmującej ryzyko prawne, zgodności z wymogami regulacyjnymi oraz wpływie na gwarantowany poziom usług, aby umożliwić im ocenę wpływu tych zmian.
 - c. W sytuacji gdy takie instytucje lub instytucje płatnicze w ramach grupy, instytucje powiązane z organem centralnym lub stanowiące część instytucjonalnego systemu ochrony polegają na ocenie umowy outsourcingu dokonanej przed zleceniem usługi na szczeblu centralnym, o której mowa w sekcji 12, każda instytucja i instytucja płatnicza powinna otrzymać podsumowanie oceny i dopilnować, aby uwzględniała ona jej szczególną strukturę i ryzyko w ramach procesu decyzyjnego;
 - d. W przypadku utworzenia i prowadzenia rejestru wszystkich istniejących umów outsourcingu na szczeblu centralnym w ramach grupy lub instytucjonalnego systemu ochrony, o którym mowa w sekcji 11, właściwe organy, wszystkie instytucje i instytucje płatnicze powinny mieć możliwość otrzymania bez zbędnej zwłoki dotyczącego ich rejestru. Rejestr obejmuje wszystkie umowy outsourcingu, w tym umowy outsourcingu zawarte z dostawcami usług wewnątrz takiej grupy lub instytucjonalnego systemu ochrony.
 - e. Jeżeli takie instytucje lub instytucje płatnicze polegają na planie wyjścia dotyczącym krytycznych i istotnych funkcji opracowanym na szczeblu grupy, w ramach instytucjonalnego systemu ochrony lub przez organ centralny, wszystkie instytucje i instytucje płatnicze powinny otrzymać streszczenie planu i upewnić, się że plan może zostać skutecznie zrealizowany.
24. Jeżeli udzielono zwolnień na podstawie art. 21 dyrektywy 2013/36/UE lub art. 109 ust. 1 dyrektywy 2013/36/UE w związku z art. 7 rozporządzenia (UE) nr 575/2013, postanowienia niniejszych wytycznych stosuje jednostka dominująca w państwie członkowskim w odniesieniu do siebie i swoich jednostek zależnych lub organ centralny i jego instytucje powiązane tworzące cały podmiot.
25. Instytucje i instytucje płatnicze będące jednostkami zależnymi jednostki dominującej UE lub jednostki dominującej w państwie członkowskim, w odniesieniu do których nie udzielono zwolnienia na podstawie art. 21 dyrektywy 2013/36/UE lub art. 109 ust. 1 dyrektywy 2013/36/UE w związku z art. 7 rozporządzenia (UE) nr 575/2013 dopilnowują, aby stosowany się do niniejszych wytycznych na zasadzie indywidualnej.

Tytuł II — Ocena umów outsourcingu

3 Outsourcing

26. Instytucje lub instytucje płatnicze ustalają, czy umowa zawarta z osobą trzecią wchodzi w zakres definicji outsourcingu. W ramach tej oceny należy rozważyć czy funkcja (lub jej część) zlecana na zasadzie outsourcingu dostawcy usług jest przez niego wykonywana regularnie czy na bieżąco oraz czy funkcja ta (lub jej część) zasadniczo wchodzi w zakres funkcji, które byłyby lub mogłyby rzeczywiście być wykonywane przez instytucje lub instytucje płatnicze, nawet jeżeli dana instytucja lub instytucja płatnicza nie wykonywała takiej funkcji w przeszłości.
27. Jeżeli umowa z dostawcą usług obejmuje wiele funkcji, instytucje i instytucje płatnicze w ramach swojej oceny uwzględniają wszystkie aspekty umowy, np. czy usługa obejmuje dostarczanie sprzętu do przechowywania danych i tworzenie kopii zapasowych danych, oba te aspekty należy rozpatrywać łącznie.
28. Co do zasady instytucje i instytucje płatnicze nie powinny traktować jako outsourcingu:
- a. funkcji, której wykonanie przez dostawcę usług jest wymagane na mocy prawa, np. badanie ustawowe;
 - b. usług związanych z dostarczaniem informacji rynkowych (np. udostępnienie danych przez Bloomberg, Moody's, Standard & Poor's, Fitch);
 - c. infrastruktury globalnej sieci (np. Visa, MasterCard);
 - d. systemów rozliczeniowych i rozrachunku pomiędzy izbami rozliczeniowymi, CCP i instytucjami rozliczeniowymi oraz ich członkami;
 - e. infrastruktury globalnej komunikacji finansowej podlegającej nadzorowi właściwych organów;
 - f. usług bankowości korespondencyjnej; oraz
 - g. nabycia usług, które w innym przypadku nie zostałyby wykonane przez instytucję lub instytucję płatniczą (np. porada architekta, udzielenie opinii prawnej i reprezentacja przed sądem i organami administracyjnymi, usługi sprzątnięcia, ogrodnictwo i utrzymanie pomieszczeń instytucji lub instytucji płatniczej, usługi medyczne, serwisowanie samochodów służbowych, catering, usługi związane z automatami sprzedającymi, usługi biurowe, usługi turystyczne, usługi pocztowe, usługi związane z obsługą recepcji, sekretariatu lub centrali), towarów (np. plastikowych kart, czytników kart, towarów biurowych, komputerów osobistych, mebli) lub mediów (np. energii elektrycznej, gazu, wody, linii telefonicznej).

4 Funkcje krytyczne lub istotne

29. Instytucje i instytucje płatnicze uznają funkcję za krytyczną lub istotną:¹⁶

- a. o ile błąd lub niepowodzenie w ich wykonaniu zagrażałoby w sposób istotny:
 - i. ciągłości wypełniania warunków zezwolenia lub innych zobowiązań wynikających z dyrektywy 2014/65/UE, rozporządzenia (UE) nr 575/2013, dyrektywy (UE) 2015/2366 i dyrektywy 2009/110/WE oraz obowiązków regulacyjnych;
 - ii. wynikiem finansowym; lub
 - iii. niezawodności lub ciągłości wykonywanych usług bankowych i płatniczych oraz działalności w tym zakresie;
- b. w sytuacji gdy zleca się zadania operacyjne funkcji kontroli wewnętrznej na zasadzie outsourcingu, chyba że ocena wykaże, że niewykonanie funkcji będącej przedmiotem outsourcingu lub niewłaściwe jej wykonanie nie będzie miało niekorzystnego wpływu na skuteczność funkcji kontroli wewnętrznej;
- c. w sytuacji gdy przedmiotem outsourcingu ma być działalność bankowa lub usługi płatnicze w zakresie wymagającym udzielenia zezwolenia¹⁷ przez właściwy organ, zgodnie z sekcją 12.1.

30. W przypadku instytucji należy zwrócić szczególną uwagę na krytyczność i wagę funkcji, jeżeli przedmiotem outsourcingu są funkcje związane z głównymi liniami biznesowymi i funkcjami krytycznymi zgodnie z definicją zawartą w art. 2 ust 1 pkt 35 i 36 dyrektywy 2014/59/WE¹⁸ i zidentyfikowane przez instytucje na podstawie kryteriów określonych w art. 6 i 7 rozporządzenia delegowanego Komisji (UE) 2016/778.¹⁹ Na potrzeby niniejszych wytycznych za krytyczne lub istotne uznaje się funkcje niezbędne do wykonywania działań w ramach głównych linii biznesowych lub funkcji krytycznych, chyba że w wyniku oceny dokonanej przez instytucję okaże się, że niewykonanie funkcji będącej przedmiotem outsourcingu lub niewłaściwe jej wykonanie nie będzie miało niekorzystnego wpływu na ciągłość operacyjną głównych linii biznesowych lub funkcji krytycznych.

¹⁶ Zobacz również art 30 rozporządzenia delegowanego Komisji (UE) 2017/565 z dnia 25 kwietnia 2016 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez firmy inwestycyjne oraz pojęć zdefiniowanych na potrzeby tej dyrektywy.

¹⁷ Zobacz czynności wymienione w załączniku 1 do dyrektywy 2013/36/UE.

¹⁸ Dyrektywa Parlamentu Europejskiego i Rady 2014/59/UE z dnia 15 maja 2014 r. ustanawiająca ramy na potrzeby prowadzenia działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji w odniesieniu do instytucji kredytowych i firm inwestycyjnych oraz zmieniająca dyrektywę Rady 82/891/EWG i dyrektywy Parlamentu Europejskiego i Rady 2001/24/WE, 2002/47/WE, 2004/25/WE, 2005/56/WE, 2007/36/WE, 2011/35/UE, 2012/30/UE i 2013/36/EU oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 i (UE) nr 648/2012 (Dz.U. L 173 z 12.6.2014, s. 190).

¹⁹ Rozporządzenie delegowane Komisji (UE) 2016/778 z dnia 2 lutego 2016 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2014/59/UE w odniesieniu do okoliczności i warunków, w jakich zapłata nadzwyczajnych składek ex post może zostać częściowo lub całkowicie odroczone, oraz w zakresie kryteriów służących określeniu działań, usług i operacji w odniesieniu do funkcji krytycznych oraz określeniu linii biznesowych wraz z powiązanymi usługami w odniesieniu do głównych linii biznesowych (Dz.U. L 131 z 20.5.2016, s. 41).

31. Instytucje i instytucje płatnicze dokonują oceny czy umowa outsourcingu dotyczy funkcji krytycznej lub istotnej waz z wynikiem oceny ryzyka, o której mowa w sekcji 12.2. uwzględnia przynajmniej następujące czynniki:

- a. czy umowa outsourcingu dotyczy bezpośrednio świadczenia usług działalności bankowej i usług płatniczych²⁰, w odniesieniu do których udzielono zezwolenia;
- b. potencjalny wpływ zakłócenia funkcji zleconych w ramach outsourcingu lub niewykonania przez dostawcę usługi na uzgodnionym gwarantowanym poziomie usług trybie ciągłym na:
 - i. krótko- i długoterminową odporność i kondycję finansową, w tym, jeżeli dotyczy, jej aktywa, kapitał, koszty, finansowanie, płynność, zyski i straty;
 - ii. ciągłość działania i odporność operacyjną;
 - iii. ryzyko operacyjne, w tym prowadzenie działalności, technologie informacyjne i komunikacyjne (ICT) i ryzyko prawne;
 - iv. ryzyko utraty reputacji;
 - v. w stosownych przypadkach, planowanie w zakresie działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji, możliwość przeprowadzenia skutecznej restrukturyzacji i uporządkowanej likwidacji oraz ciągłość operacyjną w sytuacji wczesnej interwencji, działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji;
- c. potencjalny wpływ umowy outsourcingu na zdolność instytucji do:
 - i. identyfikacji ryzyka, zarządzania ryzykiem i jego monitorowania;
 - ii. spełnienia wszystkich wymogów prawnych i regulacyjnych;
 - iii. przeprowadzenia stosownych audytów dotyczących funkcji będących przedmiotem outsourcingu;
- d. potencjalny wpływ na usługi świadczone na rzecz klientów;
- e. wszelkie umowy outsourcingu, łączna ekspozycja instytucji lub instytucji płatniczej na tego samego dostawcę usług oraz potencjalny łączny wpływ umów outsourcingu w tym samym obszarze działalności;
- f. rozmiar i złożoność danego obszaru działalności;

²⁰ Zobacz czynności wymienione w załączniku 1 do dyrektywy 2013/36/UE.

- g. możliwość rozszerzenia zakresu proponowanej umowy outsourcingu bez zastępowania lub zmiany umowy bazowej;
- h. zdolność do przeniesienia proponowanej umowy outsourcingu na innego dostawcę usług, jeżeli jest to niezbędne lub pożądane, zarówno na podstawie umowy jak i w praktyce, w tym szacunkowe ryzyko, przeszkody dla ciągłości działania, koszty i ramy czasowe z tym związane („substytucyjność”);
- i. zdolność do reintegracji funkcji zleconej na zasadzie outsourcingu do instytucji lub instytucji płatniczej, jeżeli jest to niezbędne lub pożądane;
- j. ochronę danych i możliwy wpływ naruszenia poufności lub niezapewnienie dostępności i integralności danych na instytucję lub instytucję płatniczą i jej klientów, w tym między innymi zgodność z rozporządzeniem (UE) 2016/679²¹.

²¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Tytuł III — Ramy zarządzania

5 Należyte zasady zarządzania i ryzyko osoby trzeciej

32. Elementem ogólnych ram kontroli wewnętrznej²², w tym mechanizmów kontroli wewnętrznej²³ instytucji i instytucji płatniczych powinien być kompleksowy ramowy system zarządzania ryzykiem obejmujący całą instytucję i wszystkie linie biznesowe oraz wewnętrzne jednostki instytucjonalne. Na podstawie tych ram instytucje i instytucje płatnicze identyfikują ryzyko, w tym ryzyko wynikające z ustaleń z osobami trzecimi, i zarządzają nim. Ramowy system zarządzania ryzykiem umożliwia również instytucjom i instytucjom płatniczym podejmowanie uzasadnionych decyzji dotyczących podejmowania ryzyka i zapewnienie prawidłowego wdrożenia środków zarządzania ryzykiem, w tym ryzykiem w cyberprzestrzeni²⁴.
33. Instytucje i instytucje płatnicze, uwzględniając zasadę proporcjonalności zgodnie z sekcją 1, identyfikują, oceniają, monitorują wszelkie ryzyka wynikające z ustaleń z osobami trzecimi, na które są lub mogą być narażone i zarządzają takimi ryzykami, niezależnie od czy są to ustalenia dotyczące outsourcingu czy nie. Ryzyka, w szczególności ryzyka operacyjne, związane ze wszelkimi umowami z osobami trzecimi, w tym te, o których mowa w ust. 26 i 28, należy oceniać zgodnie z sekcją 12.2.
34. Instytucje i instytucje płatnicze zapewniają zgodność ze wszelkimi wymogami wynikającymi z rozporządzenia (UE) 2016/679, również w odniesieniu do ustaleń z osobami trzecimi i umów outsourcingu.

6 Należyte zasady zarządzania i outsourcing

35. Outsourcing funkcji nie może skutkować oddelegowaniem odpowiedzialności organu zarządzającego. Instytucje i instytucje płatnicze pozostają w pełni odpowiedzialne za wykonywanie obowiązków regulacyjnych, w tym zdolność do nadzorowania outsourcingu funkcji krytycznych i istotnych.
36. Organ zarządzający pozostaje zawsze w pełni odpowiedzialny przynajmniej za:
- a. zapewnienie, aby instytucja lub instytucja płatnicza na bieżąco spełniała warunki niezbędne do utrzymania zezwolenia, w tym warunki nałożone przez właściwy organ;
 - b. wewnętrzną organizację instytucji lub instytucji płatniczej;
 - c. identyfikację, ocenę konfliktu interesów i zarządzanie nim;

²² Instytucje powinny odnieść się do tytułu V wytycznych EUNB w sprawie zarządzania wewnętrznego.

²³ Zobacz również art. 11 dyrektywy 2015/2366 (druga dyrektywa w sprawie usług płatniczych).

²⁴ Zobacz również wytyczne EUNB w sprawie technologii informacyjno-komunikacyjnych i zarządzania ryzykiem związanym z bezpieczeństwem (<https://eba.europa.eu/-/eba-consults-on-guidelines-on-ict-and-security-risk-management>) oraz zasadnicze elementy dotyczące zarządzania ryzykiem w cyberprzestrzeni osób trzecich w sektorze finansowym G-7 (https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en).

- d. ustalanie strategii i polityki instytucji lub instytucji płatniczej (np. modelu biznesowego, apetytu na ryzyko, ramowego systemu zarządzania ryzykiem);
 - e. nadzorowanie bieżącego zarządzania instytucją lub instytucją płatniczą, w tym zarządzanie ryzykiem związanym z outsourcingiem; oraz
 - f. pełnienie roli organu zarządzającego pełniącego funkcję nadzorczą, w tym nadzorowanie i monitorowanie procesu podejmowania decyzji przez kierownictwo.
37. Outsourcing nie ogranicza wymogu należytej staranności do organu zarządzającego instytucji, jej dyrektorów i osób odpowiedzialnych za zarządzanie instytucją płatniczą oraz osób pełniących najważniejsze funkcje. Instytucje i instytucje płatnicze posiadają stosowne kompetencje oraz wystarczające i odpowiednio wykwalifikowane zasoby, aby zapewnić odpowiednie zarządzanie umowami outsourcingu i nadzór nad nimi.
38. Instytucje i instytucje płatnicze powinny:
- a. jednoznacznie przydzielić obowiązki w zakresie dokumentowania umów outsourcingu, zarządzania i kontroli nad takimi umowami;
 - b. przypisać dostateczne zasoby, aby zapewnić zgodność z wymogami prawnymi i regulacyjnymi, w tym z niniejszymi wytycznymi, oraz zapewnić dokumentowanie i monitorowanie wszystkich umów outsourcingu;
 - c. uwzględniając postanowienia sekcji 1 niniejszych wytycznych, ustanowić funkcję w zakresie outsourcingu lub wyznaczyć pracownika wyższego szczebla, który będzie bezpośrednio odpowiadał przez organem zarządzającym (np. osobę pełniącą najważniejsze funkcje w zakresie kontroli) i ponosił odpowiedzialność za zarządzanie ryzykiem dotyczącym umów outsourcingu i zarządzał takim ryzykiem w ramach kontroli wewnętrznej oraz nadzorował dokumentację dotyczącą umów outsourcingu. Małe i mniej złożone instytucje lub instytucje płatnicze powinny zapewnić co najmniej jednoznaczny podział zadań i obowiązków w zakresie zarządzania umowami outsourcingu i kontroli nad nimi, przy czym mogą przydzielić funkcję w zakresie outsourcingu członkowi organu zarządzającego instytucji lub instytucji płatniczej.
39. Instytucje i instytucje płatnicze w każdym czasie zachowują swoją istotę i nie stają się „pustą strukturą” (ang. *empty shell*) ani „podmiotem-skrzynką pocztową”. W tym celu powinny:
- a. w każdym czasie spełniać wszystkie warunki zezwolenia²⁵, w tym organ zarządzający powinien skutecznie wykonywać swoje obowiązki określone w ust. 36 niniejszych wytycznych;

²⁵ Zobacz również regulacyjne standardy techniczne na podstawie art. 8 ust. 2 dyrektywy 2013/36/UE dotyczące informacji, które należy przekazać we wniosku o udzielenie instytucji kredytowej zezwolenia oraz wykonawcze standardy techniczne na podstawie art. 8 ust. 3 dyrektywy 2013/36/UE dotyczące standardowych formularzy, szablonów i procedur

- b. zachować jasne i przejrzyste ramy organizacyjne i strukturę umożliwiającą im zapewnienie zgodności z wymogami prawnymi i regulacyjnymi;
 - c. w sytuacji gdy przedmiotem outsourcingu są zadania w ramach funkcji kontroli wewnętrznej (np. w przypadku outsourcingu w ramach grupy kapitałowej lub w ramach systemu ochrony instytucjonalnej), sprawować odpowiedni nadzór i posiadać zdolność zarządzania ryzykiem związanym z outsourcingiem funkcji krytycznych i istotnych; oraz
 - d. posiadać dostateczne zasoby i zdolności do zapewnienia zgodności z treścią lit. a) i c).
40. Instytucje i instytucje płatnicze zlecające na zasadzie outsourcingu powinny co najmniej zapewnić, aby:
- a. mogły podejmować i realizować decyzje dotyczące ich działalności oraz krytycznych istotnych funkcji, w tym w odniesieniu do tych funkcji, które są przedmiotem outsourcingu;
 - b. zachowały prawidłowość prowadzenia działalności oraz świadczenia usług bankowych i płatniczych;
 - c. ryzyko związane z bieżącymi i planowanymi umowami outsourcingu zostało odpowiednio zidentyfikowane, ocenione, zarządzane i ograniczone, w tym ryzyko związane z technologiami informacyjnymi i komunikacyjnymi oraz technologią finansową (FinTech);
 - d. zawarto stosowne umowy o zachowaniu poufności w zakresie danych i innych informacji;
 - e. zachowano odpowiedni przepływ stosownych informacji z dostawcami usług;
 - f. w odniesieniu do outsourcingu krytycznych i istotnych funkcji, są w stanie podjąć w stosownym terminie przynajmniej jedno z następujących działań:
 - i. przeniesienie funkcji do innych dostawców usług;
 - ii. reintegracja funkcji; lub

służących przekazywaniu informacji, które należy przekazać we wniosku o udzielenie zezwolenia instytucji kredytowej (<https://eba.europa.eu/regulation-and-policy/other-topics/rts-and-its-on-the-authorisation-of-credit-institutions>).

W przypadku instytucji płatniczych zobacz wytyczne dotyczące informacji, które należy przedstawić w celu uzyskania zezwolenia

przez instytucje płatnicze i instytucje pieniądza elektronicznego oraz zarejestrowania dostawców świadczących usługi dostępu do

informacji o rachunku zgodnie z art. 5 ust. 5 dyrektywy (UE) 2015/2366 (https://eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_PL.pdf/06b0a678-ecb-4d58-8268-e0e22b0c3c23).

- iii. przerwanie wykonywania działalności, które są zależne od funkcji;
- g. w sytuacji gdy dostawcy usług są zlokalizowani na obszarze UE lub państw trzecich, wdrożenie odpowiednich środków i przetwarzanie a danych zgodnie z rozporządzeniem (UE) 2016/679.

7 Polityka w zakresie outsourcingu

41. Organ zarządzający instytucji lub instytucji płatniczej²⁶, która zawarła umowę outsourcingu lub planuje zawarcie takiej umowy, dokonuje przeglądu i aktualizacji pisemnej polityki w zakresie outsourcingu oraz zapewnia jej wdrażanie, w zależności od przypadku, na zasadzie indywidualnej, subskonsolidowanej lub skonsolidowanej. W przypadku instytucji polityka w zakresie outsourcingu powinna być zgodna z sekcją 8 wytycznych EUNB w sprawie zarządzania wewnętrznego, a w szczególności powinna uwzględniać wymogi określone w sekcji 18 (nowe produkty i istotne zmiany) tych wytycznych. Instytucje płatnicze również mogą dostosować swoją politykę do treści sekcji 8 i 18 wytycznych EUNB w sprawie zarządzania wewnętrznego.
42. Polityka powinna obejmować główne fazy cyklu funkcjonowania umów outsourcingu i określać zasady, zakres odpowiedzialności i procesy dotyczące outsourcingu. W szczególności polityka powinna obejmować co najmniej:
 - a. zakres odpowiedzialności organu zarządzającego zgodnie z ust. 36, w tym w razie potrzeby jego zaangażowania w proces podejmowania decyzji dotyczących outsourcingu funkcji krytycznych i istotnych;
 - b. zaangażowanie linii biznesowych, funkcji kontroli wewnętrznej i innych osób fizycznych w związku z umowami outsourcingu;
 - c. planowanie w zakresie umów outsourcingu, w tym:
 - i. definicję wymogów biznesowych dotyczących umów outsourcingu;
 - ii. kryteria, w tym kryteria o których mowa w sekcji 4, oraz procesy służące identyfikacji krytycznych i istotnych funkcji;
 - iii. identyfikacja i ocena ryzyka oraz zarządzanie ryzykiem zgodnie z sekcją 12.2;
 - iv. kontrole due diligence dotyczące przyszłych dostawców usług, w tym środki wymagane na podstawie sekcji 12.3;

²⁶ Zobacz również wytyczne EUNB w sprawie środków bezpieczeństwa dotyczących ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych na mocy dyrektywy (UE) 2015/2366 (druga dyrektywa w sprawie

usług płatniczych), dostępne pod adresem: <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2>

- v. procedury w zakresie identyfikacji, oceny i ograniczania potencjalnych konfliktów interesów oraz zarządzania nimi zgodnie z sekcją 8;
 - vi. planowanie ciągłości działania zgodnie z sekcją 9;
 - vii. proces zatwierdzania nowych umów outsourcingu;
- d. wdrożenie umów outsourcingu, monitorowanie ich oraz zarządzanie nimi, w tym:
- i. bieżąca ocena wyników dostawcy usług zgodnie z sekcją 14;
 - ii. procedury otrzymywania powiadomień o zmianach w umowie outsourcingu lub u dostawcy usług (np. dotyczących jego sytuacji finansowej, struktury organizacyjnej lub własnościowej, podoutsourcingu) oraz reagowania na takie zmiany;
 - iii. niezależna weryfikacja i audyt zgodności z wymogami prawnymi i regulacyjnymi oraz strategiami;
 - iv. procesy dotyczące wznowienia;
- e. dokumentacja i prowadzenie rejestrów z uwzględnieniem wymagań zawartych w sekcji 11;
- f. strategie wyjścia i procesy dotyczące rozwiązania umowy, w tym wymóg dotyczący udokumentowanego planu wyjścia dla każdej krytycznej i istotnej funkcji, która ma być przedmiotem outsourcingu, jeżeli wyjście uznaje się na możliwe biorąc pod uwagę ewentualne zakłócenia świadczenia usługi lub nieoczekiwane rozwiązanie umowy outsourcingu.

43. W polityce outsourcingu należy rozróżnić:

- a. outsourcing krytycznych i istotnych funkcji od pozostałych umów;
- b. outsourcing na rzecz dostawców usług upoważnionych przez właściwy organ od outsourcingu na rzecz dostawców usług nieupoważnionych;
- c. wewnątrzgrupowe umowy outsourcingu, umowy outsourcingu w ramach tego samego systemu ochrony instytucjonalnej (w tym na rzecz podmiotów, których właścicielami, indywidualnie lub wspólnie, są instytucje w ramach systemu ochrony instytucjonalnej) od outsourcingu na rzecz podmiotów spoza grupy; oraz
- d. outsourcing na rzecz dostawców usług znajdujących się w państwie członkowskim od dostawców znajdujących się w państwach trzecich.

44. Instytucje i instytucje płatnicze dopilnowują, aby polityka obejmowała kwestię identyfikacji następujących potencjalnych skutków wynikających z krytycznych lub istotnych umów outsourcingu oraz ich uwzględniania w procesie podejmowania decyzji:
- a. profil ryzyka instytucji;
 - b. możliwość nadzorowania dostawcy usług i zarządzania ryzykiem;
 - c. środki na rzecz zapewnienia ciągłości działania; oraz
 - d. wyniki ich działalności.

8 Konflikty interesów

45. Zgodnie z sekcją 11 tytułu IV wytycznych EUNB w sprawie zarządzania wewnętrznego²⁷, instytucje płatnicze identyfikują i oceniają konflikty interesów dotyczące zawartych przez nie umów outsourcingu i zarządzają nimi.
46. Jeżeli w związku z outsourcingiem wystąpi istotny konflikt interesów, w tym konflikt pomiędzy podmiotami w ramach tej samej grupy lub systemu ochrony instytucjonalnej, instytucje i instytucje płatnicze podejmują odpowiednie środki na rzecz rozwiązywania takich konfliktów interesów.
47. Jeżeli funkcje pełni dostawca usług należący do grupy lub będący członkiem systemu ochrony instytucjonalnej, lub który jest własnością instytucji, instytucji płatniczej, grupy lub instytucji będących członkami systemu ochrony instytucjonalnej, warunki, w tym warunki finansowe, dotyczące usługi będącej przedmiotem outsourcingu będą ustalone na zasadach obowiązujących pomiędzy niezależnymi kontrahentami. Przy kształtowaniu cen usług można wykorzystywać efekt synergii wynikający ze świadczenia tych samych lub podobnych usług na rzecz kilku instytucji w ramach grupy lub systemu ochrony instytucjonalnej, o ile dostawca usługi pozostaje rentowny jako niezależny podmiot; w ramach grupy warunek ten pozostaje niezależny od spełnienia tego warunku przez jakiegokolwiek inny podmiot grupy.

²⁷ Instytucje płatnicze również mogą dostosować swoją politykę do tych wytycznych.

9 Plany ciągłości działania

48. Zgodne z wymogami art. 85 ust. 2 dyrektywy 2013/36/UE i tytułu VI wytycznych EUNB w sprawie zarządzania wewnętrznego²⁸, instytucje oraz instytucje płatnicze ustanawiają, utrzymują i poddają regularnym testom odpowiednie plany ciągłości działania dotyczące krytycznych i istotnych funkcji będących przedmiotem outsourcingu. Instytucje i instytucje płatnicze w ramach grupy lub systemu ochrony instytucjonalnej mogą polegać na planach ciągłości działania dotyczących funkcji będących przedmiotem outsourcingu ustanowionych na szczeblu centralnym.
49. Plany ciągłości działania powinny uwzględniać sytuację, w której jakość realizacji funkcji krytycznej lub istotnej będącym przedmiotem outsourcingu spadnie do niedopuszczalnego poziomu lub zawiedzie. Plany powinny uwzględniać również potencjalny wpływ niewypłacalności lub niewykonania zobowiązań przez dostawców usług, oraz w razie potrzeby, ryzyko o charakterze politycznym w jurysdykcji dostawcy usług.

10 Funkcja audytu wewnętrznego

50. Czynności w ramach funkcji audytu wewnętrznego²⁹ powinny zgodnie z podejściem opartym na analizie ryzyka obejmować niezależną weryfikację czynności zleconych na zasadzie outsourcingu. Plan³⁰ i program audytu powinny w szczególności obejmować umowy outsourcingu funkcji krytycznych i istotnych.
51. Odnośnie do procesu outsourcingu, funkcja audytu wewnętrznego zapewnia co najmniej:
- a. aby ramy outsourcingu instytucji lub instytucji płatniczej, w tym polityka w zakresie outsourcingu, zostały prawidłowo i skutecznie wdrożone i były zgodne z obowiązującymi przepisami prawa, strategią w zakresie ryzyka i decyzjami organu zarządzającego;
 - b. odpowiedniość, jakość i skuteczność oceny krytycznego lub istotnego znaczenia funkcji;
 - c. odpowiedniość, jakość i skuteczność oceny ryzyka dotyczącej umów outsourcingu oraz aby ryzyka były zgodne ze strategią instytucji w zakresie ryzyka;

²⁸ Dostępne pod adresem: <https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised->

²⁹ Obowiązki w zakresie funkcji audytu wewnętrznego dla instytucji określono w sekcji 22 wytycznych EUNB w sprawie zarządzania wewnętrznego (<https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised->) a dla instytucji płatniczych w wytycznej nr 5 wytycznych EUNB dotyczących udzielenia zezwolenia instytucjom płatniczym (https://eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+of+Payment+Institutions+%28EBA-GL-2017-09%29_PL.pdf/06b0a678-eccb-4d58-8268-e0e22b0c3c23).

³⁰ Zobacz również wytyczne EUNB dotyczące wspólnych procedur i metod stosowanych w ramach procesu przeglądu i oceny nadzorczej: <https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-for-common-procedures-and-methodologies-for-the-supervisory-review-and-evaluation-process-srep-and-supervisory-stress-testing>

- d. odpowiednie zaangażowanie organów zarządzających;
- e. odpowiednie monitorowanie i zarządzanie umowami outsourcingu.

11 Wymogi dotyczące dokumentacji

- 52. Instytucje i instytucje płatnicze w ramach swojego ramowego systemu zarządzania ryzykiem prowadzą zaktualizowany rejestr informacji na temat wszystkich umów outsourcingu na szczeblu instytucji oraz, w stosownych przypadkach, na szczeblu subskonsolidowanym lub skonsolidowanym, zgodnie z sekcją 2, oraz odpowiednio dokumentują wszystkie aktualne umowy outsourcingu dokonując rozróżnienia pomiędzy outsourcingiem funkcji krytycznych i istotnych a pozostałymi umowami outsourcingu. Instytucje przy uwzględnieniu przepisów prawa krajowego przechowują w rejestrze przez odpowiedni okres dokumentację zakończonych umów outsourcingu i dokumentację uzupełniającą.
- 53. Uwzględniając postanowienia tytułu I niniejszych wytycznych oraz na warunkach określonych w ust. 23 lit. d), w odniesieniu do instytucji i instytucji płatniczych w ramach grupy, instytucji trwale powiązanych z organem centralnym lub instytucji będących członkami tego samego systemu ochrony instytucjonalnej, rejestr może być prowadzony na szczeblu centralnym.
- 54. Rejestr zawiera co najmniej następujące informacje na temat wszystkich istniejących umów outsourcingu:
 - a. numer referencyjny każdej z umów outsourcingu;
 - b. termin rozpoczęcia, oraz w zależności od przypadku, datę odnowienia umowy, datę zakończenia lub okresy wypowiedzenia obowiązujące dostawcę usług i instytucję lub instytucję płatniczą;
 - c. krótki opis funkcji zleconej na zasadzie outsourcingu obejmujący dane będące przedmiotem outsourcingu oraz informację, czy przekazano dane osobowe (np. poprzez wpisanie „tak” lub „nie” w osobne pole danych) oraz czy zleca się ich przetworzenie przez dostawcę usług;
 - d. kategorię przypisaną przez instytucję lub instytucję płatniczą odzwierciedlającą charakter funkcji zgodnie z opisem zawartym w lit. c) (np. technologia informacyjna, funkcja kontroli), co powinno ułatwić identyfikację poszczególnych rodzajów umów;
 - e. nazwę dostawcy usług, numer ewidencyjny przedsiębiorstwa, identyfikator podmiotu prawnego (jeżeli jest dostępny), adres i inne stosowne dane kontaktowe oraz nazwę jednostki dominującej (jeżeli istnieje);
 - f. państwo lub państwa, na terenie których usługa będzie wykonywana, w tym lokalizacja (tj. kraj lub region) danych;

- g. informację (tak/nie) czy zlecona funkcja jest uznawana za krytyczną lub istotną, w tym w stosownych przypadkach, krótki opis przyczyn uznania funkcji za krytyczną lub istotną;
- h. w przypadku zlecenia dostawcy usług w chmurze, usługę w chmurze i modele wdrażania, tj. publiczny/prywatny/hybrydowy/społecznościowy, oraz szczególny charakter danych, które mają być przechowywane oraz lokalizację (tj. kraje lub regiony), gdzie dane będą przechowywane;
- i. datę ostatniej oceny krytycznego lub istotnego znaczenia funkcji.

55. Rejestr zawiera co najmniej następujące informacje w odniesieniu do outsourcingu krytycznych i istotnych funkcji:

- a. instytucje, instytucje płatnicze i inne przedsiębiorstwa wchodzące w zakres konsolidacji ostrożnościowej lub systemu ochrony instytucjonalnej, w stosownych przypadkach, które korzystają z outsourcingu;
- b. niezależnie od tego, czy dostawca usług lub poddostawca usług należy do grupy, jest członkiem systemu ochrony instytucjonalnej, stanowi własność instytucji lub instytucji płatniczych w ramach grupy lub stanowi własność członków systemu ochrony instytucjonalnej;
- c. datę ostatniej oceny ryzyka i krótkie streszczenie ogólnych wyników;
- d. wskazanie osoby lub organu decyzyjnego (np. organu zarządzającego) w instytucji lub instytucji płatniczej, którzy zatwierdzili umowę outsourcingu;
- e. prawo właściwe dla umowy outsourcingu;
- f. daty ostatnich i kolejnych zaplanowanych audytów, w stosownych przypadkach;
- g. w stosownych przypadkach nazwy podwykonawców, którym zlecane są na zasadzie outsourcingu istotne części krytycznych i istotnych funkcji, w tym kraj, gdzie są zarejestrowani, gdzie wykonywana będzie usługa oraz, jeżeli dotyczy, lokalizacja (tj. kraj lub region) przechowywania danych;
- h. wynik oceny substytucyjności dostawcy usług (łatwy, trudny lub niemożliwy), możliwość reintegracji krytycznych lub istotnych funkcji do instytucji lub instytucji płatniczej lub wpływ przerwania wykonywania krytycznych i istotnych funkcji;
- i. wskazanie alternatywnych dostawców usług zgodnie z lit. h);
- j. czy krytyczna lub istotna funkcja będąca przedmiotem outsourcingu wspiera działalność, która jest zależna od czasu;
- k. szacowane roczne koszty budżetowe.

56. Instytucje i instytucje płatnicze udostępniają właściwemu organowi na jego prośbę pełen rejestr wszystkich istniejących umów outsourcingu³¹ lub określonych jego sekcji, takich jak informacje dotyczące umów outsourcingu należącego do jednej z kategorii, o których mowa w ust. 54 lit. d) niniejszych wytycznych (np. wszystkie umowy outsourcingu dotyczące technologii informacyjnej). Instytucje i instytucje płatnicze udostępniają te informacje w możliwej do przetworzenia formie elektronicznej (np. powszechnie używany format bazy danych, wartości oddzielone przecinkiem).
57. Instytucje i instytucje płatnicze udostępniają właściwemu organowi na jego prośbę wszelkie informacje umożliwiające temu organowi skuteczne nadzorowanie instytucji lub instytucji płatniczej, w tym, o ile to konieczne, kopię umowy outsourcingu.
58. Nie naruszając przepisów art. 16 ust. 6 dyrektywy (UE) 2015/2366, instytucje oraz instytucje płatnicze odpowiednio terminowo powiadamiają właściwe organy lub nawiązują z nimi dialog w zakresie nadzoru dotyczący planowego outsourcingu krytycznych lub istotnych funkcji lub jeżeli funkcja zlecona na zasadzie outsourcingu stała się krytyczna lub istotna oraz dostarczają co najmniej informacje określone w ust. 54.
59. Instytucje i instytucje płatnicze³² terminowo informują właściwe organy o istotnych zmianach lub poważnych zdarzeniach dotyczących umów outsourcingu, które mogą mieć istotny wpływ na ciągłość prowadzenia działalności przez instytucje lub instytucje i instytucje płatnicze.
60. Instytucje i instytucje płatnicze stosownie dokumentują oceny przeprowadzone na podstawie postanowień tytułu IV oraz wyniki bieżącego monitorowania (np. wyniki działania dostawcy usług, zgodność z uzgodnionymi gwarantowanymi poziomami usług lub inne wymogi umowne i regulacyjne, aktualizacje oceny ryzyka).

Tytuł IV – Proces outsourcingu

12 Analiza przed zawarciem umowy outsourcingu

61. Przed zawarciem umowy outsourcingu instytucje i instytucje płatnicze powinny:
- ocenić, czy umowa outsourcingu dotyczy krytycznej lub istotnej funkcji zgodnie z tytułem II;
 - ocenić, czy spełniono warunki w zakresie nadzoru dotyczące outsourcingu określone w sekcji 12.1;

³¹ Zobacz również wytyczne EUNB dotyczące oceny nadzorczej i procesu przeglądu dostępne pod adresem: <https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2>

³² Zobacz również wytyczne EUNB dotyczące zgłaszania poważnych incydentów zgodnie z dyrektywą (UE) 2015/2366 (PSD2) dostępne pod adresem: <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2>

- c. zidentyfikować i ocenić wszystkie istotne zagrożenia umowy outsourcingu zgodnie z sekcją 12.2;
- d. przeprowadzić odpowiednią analizę due diligence dotyczącą przyszłego dostawcy usług zgodnie z sekcją 12.3;
- e. zidentyfikować i ocenić konflikty interesów, do których może doprowadzić outsourcing, zgodnie z sekcją 8.

12.1 Warunki w zakresie nadzoru dotyczące outsourcingu

62. Instytucje i instytucje płatnicze dopilnowują, aby zlecenie na zasadzie outsourcingu funkcji wykonywania działalności bankowej³³ lub świadczenia usług płatniczych w zakresie, w jakim wykonanie tej funkcji wymaga udzielenia zezwolenia lub zarejestrowania przez właściwy organ w państwie członkowskim, w którym uzyskały zezwolenie, na rzecz dostawcy usług zlokalizowanemu w tym samym lub innym państwie członkowskim zostało udzielone, jeżeli spełnione zostały następujące warunki:

- a. dostawca usług posiada zezwolenie lub jest zarejestrowany przez właściwy organ na potrzeby wykonywania działalności bankowej lub świadczenia usług płatniczych; lub
- b. dostawca usług jest uprawniony na innej podstawie do prowadzenia działalności bankowej lub świadczenia usług płatniczych zgodnie ze stosownymi krajowymi ramami prawnymi.

63. Instytucje i instytucje płatnicze dopilnowują, aby zlecenie na zasadzie outsourcingu funkcji wykonywania działalności bankowej lub świadczenia usług płatniczych, w zakresie w jakim wykonanie tej funkcji wymaga udzielenia zezwolenia lub zarejestrowania przez właściwy organ w państwie członkowskim, w którym uzyskały zezwolenie, na rzecz dostawcy usług zlokalizowanemu w państwie trzecim zostało udzielone, jeżeli spełnione zostały następujące warunki:

- a. dostawca usług posiada zezwolenie lub jest zarejestrowany na potrzeby wykonywania działalności bankowej lub świadczenia usług płatniczych w państwie trzecim i podlega stosownemu nadzorowi właściwego organu w tym państwie trzecim (zwanemu „organem nadzoru”);
- b. istnieje odpowiednia umowa o współpracy np. w formie porozumienia lub umowy kolegium pomiędzy właściwymi organami odpowiedzialnymi za nadzór nad instytucją a organami nadzoru odpowiedzialnymi za nadzór nad dostawcą usług; oraz

³³ Zobacz art. 9 dyrektywy w sprawie wymogów kapitałowych odnośnie do zakazu prowadzenia przez osoby lub przedsiębiorstwa inne niż instytucje kredytowe działalności polegającej na przyjmowaniu od ludności depozytów lub innych środków podlegających zwrotowi.

- c. w umowie o współpracy, o której mowa w lit. b), zastrzega się, że właściwe organy są w stanie co najmniej:
- i. uzyskać, na wniosek, informacje niezbędne do realizacji ich zadań z zakresu nadzoru określonych w dyrektywie 2013/36/UE, rozporządzeniu (UE) nr 575/2013, dyrektywie (UE) 2015/2366 i dyrektywie 2009/110/WE;
 - ii. uzyskać odpowiedni dostęp do wszelkich danych, dokumentów, pomieszczeń lub personelu w państwie trzecim istotnych do celów wykonywania ich zadań z zakresu nadzoru;
 - iii. niezwłocznie otrzymywać informacje od organu nadzoru w państwie trzecim do celów zbadania przypadków jawnego naruszania wymogów określonych w dyrektywie 2013/36/UE, rozporządzeniu (UE) nr 575/2013, dyrektywie (UE) 2015/2366 i dyrektywie 2009/110/WE; oraz
 - iv. współpracować z odpowiednimi organami nadzoru w państwie trzecim w celu egzekwowania prawa, jeśli dojdzie do naruszenia obowiązujących wymogów regulacyjnych i przepisów krajowych państwa członkowskiego. Współpraca powinna obejmować, między innymi, otrzymywanie w możliwie najkrótszym terminie informacji dotyczących potencjalnego naruszenia obowiązujących wymogów regulacyjnych od organów nadzoru w państwie trzecim.

12.2 Ocena ryzyka umów outsourcingu

64. Instytucje i instytucje płatnicze oceniają potencjalny wpływ umów outsourcingu na ich ryzyko operacyjne, uwzględniają wyniki oceny na potrzeby podjęcia decyzji, czy daną funkcję należy zlecić na zasadzie outsourcingu dostawcy usług, oraz podejmują odpowiednie kroki w celu uniknięcia dodatkowego ryzyka operacyjnego przed zawarciem umów outsourcingu.
65. W stosownych przypadkach ocena powinna obejmować scenariusze ewentualnych zdarzeń ryzyka, w tym zdarzeń ryzyka operacyjnego mających poważne skutki. W ramach analizy scenariuszowej instytucje i instytucje płatnicze oceniają potencjalny wpływ niewykonania usługi lub niewłaściwego jej wykonania, w tym ryzyko związane z procesami, systemami, ludźmi lub zdarzeniami zewnętrznymi. Instytucje i instytucje płatnicze, uwzględniając zasadę proporcjonalności, o której mowa w sekcji 1, dokumentują przeprowadzoną analizę i jej wyniki oraz szacują zakres, o jaki zwiększy lub zmniejszy się ich ryzyko operacyjne na skutek zawarcia umowy outsourcingu. Uwzględniając postanowienia tytułu I, małe instytucje i instytucje płatnicze o niezłożonej strukturze mogą stosować podejście do oceny ryzyka oparte na jakości, podczas gdy duże i złożone instytucje powinny stosować bardziej zaawansowane podejście, w tym zasilić analizę scenariuszową dostępnymi wewnętrznymi i zewnętrznymi danymi na temat strat.
66. W ramach oceny ryzyka instytucje i instytucje płatnicze uwzględniają również przewidywane korzyści i koszty proponowanej umowy outsourcingu, w tym oceniają ryzyko, które można

ograniczyć lub którym można skuteczniej zarządzać względem ryzyka, które może wystąpić na skutek zawarcia proponowanej umowy outsourcingu, uwzględniając co najmniej:

- a. ryzyko koncentracji, w tym ryzyko wynikające z:
 - i. zawarcia umowy outsourcingu z dostawcą usług o dominującej pozycji, zastąpienie którego nie jest łatwe; oraz
 - ii. zawarcia wielu umów outsourcingu z tym samym dostawcą usług lub dostawcami usług blisko ze sobą związanych;
- b. zagregowane ryzyko wynikające z outsourcingu kilku funkcji w całej instytucji płatniczej oraz – w przypadku grup instytucji lub instytucjonalnych systemów ochrony – zagregowane ryzyko na zasadzie skonsolidowanej lub na podstawie instytucjonalnego systemu ochrony;
- c. w przypadku istotnych instytucji, ryzyko związane ze wstąpieniem w prawa i obowiązki, tj. ryzyko, które może wynikać z konieczności udzielenia wsparcia finansowego dostawcy usług znajdującego się z sytuacji zagrożenia lub przejścia jego działalności; oraz
- d. środki wdrożone przez instytucję lub instytucję płatniczą oraz przez dostawcę usług w celu zarządzania ryzykiem oraz ograniczenia ryzyka.

67. Jeżeli umowa outsourcingu przewiduje możliwość zlecenia przez dostawcę usług krytycznych lub istotnych funkcji na zasadzie podoutsourcingu innym dostawcom usług, instytucje i instytucje płatnicze uwzględniają:

- a. ryzyko związane z podoutsourcingiem, w tym dodatkowe ryzyko, jakie może wystąpić, jeżeli podwykonawca ma siedzibę w państwie trzecim lub w państwie innym niż dostawca usług;
- b. ryzyko, że długie i złożone łańcuchy podoutsourcingu ograniczą zdolność instytucji lub instytucji płatniczych do nadzorowania zleconej na zasadzie outsourcingu krytycznej lub istotnej funkcji oraz zdolność właściwych organów do skutecznego ich nadzorowania.

68. Dokonując oceny ryzyka przed zleceniem na zasadzie outsourcingu oraz w ramach bieżącego monitorowania wyników dostawcy usług, instytucje i instytucje płatnicze powinny co najmniej:

- a. określić i sklasyfikować odpowiednie funkcje i związane z nimi dane oraz systemy w odniesieniu do ich wrażliwości i wymaganych środków ochrony;
- b. przeprowadzić dogłębną ocenę opartą na analizie ryzyka w odniesieniu do funkcji i związanych z nimi danych i systemów, które mają zostać zlecone lub zostały zlecone na zasadzie outsourcingu, oraz wyeliminować potencjalne ryzyko, w szczególności ryzyko

operacyjne, w tym ryzyko prawne, ryzyko związane z technologiami informacyjnymi i komunikacyjnymi, ryzyko braku zgodności z przepisami i ryzyko utraty reputacji, a także ograniczenia w zakresie nadzoru dotyczące krajów, gdzie zlecone usługi są lub mogą być świadczone oraz gdzie są lub mogą być przechowywane dane;

- c. uwzględnić skutki wynikające z lokalizacji dostawcy usług (na terenie UE lub poza nią);
- d. uwzględnić stabilność polityczną i sytuację w zakresie bezpieczeństwa odnośnych jurysdykcji, w tym:
 - i. obowiązujące przepisy, w tym przepisy prawa w zakresie ochrony danych;
 - ii. obowiązujące przepisy w zakresie egzekwowania prawa; oraz
 - iii. przepisy prawa dotyczącego niewypłacalności, które miałyby zastosowanie w przypadku niewykonania przez dostawcę usług oraz wszelkie ograniczenia, jakie powstałyby w szczególności w związku z pilnym odzyskaniem danych instytucji lub instytucji płatniczej;
- e. określić odpowiedni poziom ochrony poufności danych, ciągłości działań zleconych na zasadzie outsourcingu oraz integralności i identyfikowalności danych i systemów w kontekście planowego outsourcingu i podjąć decyzję w tej sprawie. Instytucje i instytucje płatnicze w stosownych przypadkach uwzględniają również podjęcie szczególnych środków w odniesieniu do przesyłanych danych, danych znajdujących się w urządzeniu pamięciowym i danych odłożonych, takich jak wykorzystanie technologii szyfrowania w połączeniu z odpowiednią architekturą zarządzania kluczami;
- f. rozważyć, czy dostawca usług jest jednostką zależną lub jednostką dominującą instytucji, czy jest objęty zakresem konsolidacji na potrzeby rachunkowości, czy jest członkiem lub stanowi własność instytucji będących członkami instytucjonalnego systemu ochrony, a jeżeli tak, to w jakim zakresie instytucja go kontroluje lub może wpływać na jego działania zgodnie z sekcją 2.

12.3 Analiza due diligence

- 69. Przed zawarciem umowy outsourcingu oraz uwzględniając ryzyko operacyjne związane z funkcją, która ma zostać zlecona na zasadzie outsourcingu, instytucje i instytucje płatnicze, w ramach swoich procesów dotyczących wyboru i oceny dopilnowują, aby dostawca usług był odpowiedni.
- 70. W odniesieniu do krytycznych i istotnych funkcji instytucje i instytucje płatnicze zapewniają, aby dostawca usług posiadał reputację biznesową, odpowiednie i wystarczające umiejętności, fachową wiedzę, zdolność, zasoby (np. ludzkie, informatyczne, finansowe), strukturę organizacyjną oraz, w stosownych przypadkach, wymagane zezwolenia regulacyjne lub rejestrację (wymagane zezwolenia regulacyjne) lub został zarejestrowany na potrzeby

wykonywania krytycznej lub istotnej funkcji w sposób wiarygodny i profesjonalny, aby wywiązać się ze swoich zobowiązań w okresie obowiązywania projektu umowy.

71. Dodatkowe czynniki, które należy uwzględnić podczas analizy due diligence potencjalnego dostawcy usług, obejmują między innymi:

- a. jego model biznesowy, charakter, skalę, złożoność, sytuację finansową, strukturę własnościową i grupy;
- b. długoterminowe relacje z dostawcami usług, którzy zostali już poddani ocenie i świadczą usługi na rzecz instytucji i instytucji płatniczej;
- c. czy dostawca usług jest jednostką dominującą lub zależną instytucji lub instytucji płatniczej, czy jest objęty zakresem konsolidacji instytucji na potrzeby rachunkowości lub jest członkiem lub stanowi własność instytucji będących członkami tego samego instytucjonalnego systemu ochrony, do którego należy instytucja;
- d. czy dostawca usług jest nadzorowany przez właściwe organy.

72. Jeżeli outsourcing wiąże się z przetwarzaniem danych osobowych lub poufnych, instytucje i instytucje płatnicze powinny mieć pewność, że dostawca usług wdraża odpowiednie środki techniczne i organizacyjne w celu ochrony danych.

73. Instytucje i instytucje płatnicze podejmują odpowiednie kroki w celu zapewnienia, aby dostawcy usług działali w sposób zgodny z ich wartościami i kodeksem postępowania. W szczególności w odniesieniu do dostawców usług z państw trzecich oraz, w stosownych przypadkach, ich podwykonawców, instytucje i instytucje płatnicze powinny mieć pewność, że dostawca usług działa w sposób etyczny i społecznie odpowiedzialny i przestrzega międzynarodowych norm dotyczących praw człowieka (np. europejskiej konwencji praw człowieka), ochrony środowiska oraz odpowiednich warunków pracy, w tym przestrzega zakazu pracy dzieci.

13 Etap umowy

74. Prawa i obowiązki instytucji, instytucji płatniczej i dostawcy usług są w sposób jasny rozdzielone i określone w pisemnej umowie.

75. Umowa outsourcingu dotycząca krytycznych lub istotnych funkcji powinna określać co najmniej:

- a. jasny opis funkcji zleconych na zasadzie outsourcingu;
- b. datę rozpoczęcia i zakończenia, w stosownych przypadkach, umowy i okresy wypowiedzenia dla dostawcy usług oraz instytucji lub instytucji płatniczej;
- c. prawo właściwe dla umowy;

- d. zobowiązania finansowe stron;
- e. czy dopuszcza się podoutsourcingu danej krytycznej lub istotnej funkcji lub jej istotnych części, a jeżeli tak – warunki określone w sekcji 13.1, którym podlega podoutsourcing;
- f. lokalizację (tj. regiony lub państwa), w których będzie wykonywana krytyczna lub istotna funkcja lub gdzie będą przechowywane i przetwarzane odpowiednie dane, w tym ewentualne miejsce przechowywania, oraz warunki, jakie należy spełnić, w tym wymóg dotyczący powiadamiania instytucji lub instytucji płatniczej, jeżeli dostawca usług zaproponuje zmianę lokalizacji;
- g. w stosownych przypadkach, przepisy dotyczące dostępności, osiągalności, integralności, prywatności i bezpieczeństwa odpowiednich danych, określone w sekcji 13.2;
- h. prawo instytucji lub instytucji płatniczej do bieżącego monitorowania wyników dostawcy usług;
- i. uzgodnione gwarantowane poziomy usług, które powinny obejmować dokładne cele ilościowe i jakościowe dla funkcji zleconej na zasadzie outsourcingu, które można terminowo monitorować , tak aby umożliwić bezzwłoczne podjęcie odpowiednich działań naprawczych, jeżeli gwarantowane poziomy usług nie zostaną osiągnięte;
- j. obowiązki sprawozdawcze spoczywające na dostawcy usług wobec instytucji lub instytucji płatniczej, w tym powiadomienie przez dostawcę usług o wszelkich zmianach, które mogą mieć istotny wpływ na jego zdolność do skutecznego wykonywania krytycznej lub istotnej funkcji zgodnie z uzgodnionymi gwarantowanymi poziomami usług oraz zgodnie z obowiązującymi przepisami i wymogami regulacyjnymi oraz, w stosownych przypadkach, obowiązki dostawcy usług w zakresie przedkładania sprawozdań dotyczących funkcji audytu wewnętrznego;
- k. czy dostawca usług powinien wykupić obowiązkowe ubezpieczenie od określonych rodzajów ryzyka oraz, w stosownych przypadkach, wymagany poziom ochrony;
- l. wymogi dotyczące wdrażania i testowania planów awaryjnych przedsiębiorstwa;
- m. postanowienia zapewniające dostęp do danych stanowiących własność instytucji lub instytucji płatniczej w przypadku niewypłacalności, restrukturyzacji i uporządkowanej likwidacji lub zaprzestania działalności dostawcy usług;
- n. obowiązek współpracy dostawcy usług z właściwymi organami i organami ds. restrukturyzacji i uporządkowanej likwidacji instytucji lub instytucji płatniczej, w tym z innymi osobami przez nie wyznaczonymi;
- o. w przypadku instytucji – wyraźne odniesienie do uprawnień organu ds. restrukturyzacji i uporządkowanej likwidacji, w szczególności do art. 68 i 71 dyrektywy 2014/59/UE

(dyrektywa w sprawie naprawy oraz restrukturyzacji i uporządkowanej likwidacji banków), w szczególności opis „istotnych zobowiązań” umowy w rozumieniu art. 68 tej dyrektywy;

- p. nieograniczone prawo instytucji, instytucji płatniczych i właściwych organów do przeprowadzania kontroli i audytu u dostawcy usług, w szczególności w odniesieniu do krytycznej lub istotnej funkcji zleconej na zasadzie outsourcingu, jak określono w sekcji 13.3;
- q. prawa do rozwiązania umowy, jak określono w sekcji 13.4.

13.1 Podoutsourcing krytycznych lub istotnych funkcji

- 76. Umowa outsourcingu powinna określać, czy dozwolony jest podoutsourcing krytycznych lub istotnych funkcji bądź ich istotnych części.
- 77. Jeżeli dopuszcza się podoutsourcing krytycznych lub istotnych funkcji, instytucje i instytucje płatnicze określają czy dana część funkcji, która ma być zlecona na zasadzie podoutsourcingu, jest, jako taka, krytyczna lub istotna (tj. stanowi istotną część krytycznej lub istotnej funkcji), a jeżeli tak – wpisują ją do rejestru.
- 78. Jeżeli dopuszcza się podoutsourcing krytycznych lub istotnych funkcji, pisemna umowa powinna:
 - a. określać rodzaje działalności, które są wyłączone z podoutsourcingu;
 - b. określać warunki, które muszą być spełnione w przypadku podoutsourcingu;
 - c. wskazywać, że dostawca usług jest zobowiązany do nadzorowania tych usług, które zlecił na zasadzie podoutsourcingu w celu zapewnienia, by wszystkie zobowiązania umowne między dostawcą usług a instytucją lub instytucją płatniczą były spełniane w sposób nieprzerwany;
 - d. zobowiązywać dostawcę usług do uzyskania uprzedniej szczegółowej lub ogólnej pisemnej zgody od instytucji lub instytucji płatniczej przed udostępnieniem danych na podstawie podoutsourcingu³⁴;
 - e. obejmować zobowiązanie dostawcy usług do informowania instytucji lub instytucji płatniczej o jakimkolwiek planowanym podoutsourcingu lub istotnych zmianach dotyczących podoutsourcingu, w szczególności jeżeli może to mieć wpływ na zdolność dostawcy usług do wywiązywania się z jego obowiązków wynikających z umowy outsourcingu. Powyższe obejmuje planowane istotne zmiany podwykonawców i okres powiadamiania; w szczególności okres powiadamiania powinien umożliwiać zlecającej instytucji lub instytucji płatniczej co najmniej przeprowadzanie oceny ryzyka w

³⁴ Zobacz art. 28 rozporządzenia (UE) nr 2016/679.

odniesieniu do proponowanych zmian oraz wniesienie sprzeciwu wobec zaproponowanym zmianom, zanim planowany podoutsourcing lub dotyczące go istotne zmiany wejdą w życie;

- f. zapewniać, w stosownych przypadkach, prawo instytucji lub instytucji płatniczej do sprzeciwu wobec zamierzonego podoutsourcingu lub istotnych zmian go dotyczących lub wymóg uzyskania wyraźnej zgody;
- g. zapewniać wynikające z umowy prawo instytucji lub instytucji płatniczej do rozwiązania umowy w przypadku nieuzasadnionego podoutsourcingu, np. w przypadku, gdy podoutsourcing istotnie zwiększa ryzyko dla instytucji lub instytucji płatniczej lub w przypadku, gdy dostawca usług podzleca bez powiadomienia o tym instytucji lub instytucji płatniczej.

79. Instytucje i instytucje płatnicze wyrażają zgodę na podoutsourcing wyłącznie w przypadku, gdy podwykonawca zobowiązuje się do:

- a. przestrzegania wszystkich obowiązujących przepisów prawa, wymogów regulacyjnych i zobowiązań wynikających z umowy; oraz
- b. przyznania instytucji, instytucji płatniczej i właściwemu organowi takich samych wynikających z umowy praw dostępu i kontroli, co prawa przyznane przez dostawcę usług.

80. Instytucje i instytucje płatnicze zapewniają, aby dostawca usług odpowiednio nadzorował poddostawców usług, zgodnie z polityką określoną przez instytucję lub instytucję płatniczą. Jeżeli proponowany podoutsourcing mógłby mieć istotny niekorzystny wpływ na umowę outsourcingu dotyczącą krytycznej lub istotnej funkcji lub mógłby doprowadzić do znacznego wzrostu ryzyka, również w przypadku, gdy warunki określone w ust. 79 nie zostałyby spełnione, instytucja lub instytucja płatnicza powinna wykonywać swoje prawo do wniesienia sprzeciwu wobec podoutsourcingu, jeżeli takie prawo zostało uzgodnione lub rozwiązać umowę.

13.2 Bezpieczeństwo danych i systemów

81. Instytucje i instytucje płatnicze zapewniają, aby dostawcy usług, w stosownych przypadkach, przestrzegali odpowiednich standardów bezpieczeństwa IT.

82. W stosownych przypadkach (np. w kontekście outsourcingu w chmurze lub innego rodzaju outsourcingu dotyczącego ICT) instytucje i instytucje płatnicze określają wymagania dotyczące bezpieczeństwa danych i systemów w umowie outsourcingu i na bieżąco monitorują zgodność z tymi wymogami.

83. W przypadku zlecenia na zasadzie outsourcingu dostawcom usług w chmurze oraz innych umów outsourcingu obejmujących obsługę lub przekazywanie danych osobowych lub poufnych, instytucje i instytucje płatnicze powinny przyjąć podejście oparte na analizie ryzyka w

odniesieniu do lokalizacji przechowywania i przetwarzania danych (tj. kraju lub regionu) i kwestii bezpieczeństwa informacji.

84. Z zastrzeżeniem wymogów rozporządzenia (UE) 2016/679, instytucje i instytucje płatnicze, zlecając na zasadzie outsourcingu (w szczególności do państw trzecich) powinny uwzględniać różnice w przepisach krajowych dotyczących ochrony danych. Instytucje i instytucje płatnicze dopilnowują, aby umowa outsourcingu zawierała zobowiązanie, że dostawca usług zapewni ochronę informacji poufnych, osobowych lub innych informacji szczególnie chronionych i spełnia wszystkie wymogi prawne dotyczące ochrony danych, które mają zastosowanie do instytucji lub instytucji płatniczej (np. ochrona danych osobowych, oraz w stosownych przypadkach przestrzeganie obowiązku zachowania tajemnicy bankowej lub podobnych obowiązków w zakresie poufności w odniesieniu do informacji klientów).

13.3 Prawa do dostępu, informacji i audytu

85. W ramach pisemnej umowy outsourcingu instytucje i instytucje płatnicze powinny zapewnić, aby funkcja audytu wewnętrznego była w stanie dokonać przeglądu funkcji zleconych na zasadzie outsourcingu stosując podejście oparte na analizie ryzyka.
86. Niezależnie od krytycznego lub istotnego znaczenia funkcji zleconej na zasadzie outsourcingu, pisemne umowy outsourcingu zawierane pomiędzy instytucjami a dostawcami usług powinny odnosić się do gromadzenia informacji i uprawnień dochodzeniowych właściwych organów i organów ds. restrukturyzacji i uporządkowanej likwidacji na mocy art. 63 ust. 1 lit. a) dyrektywy 2014/59/UE i art. 65 ust. 3 dyrektywy 2013/36/UE w odniesieniu do dostawców usług znajdujących się w państwie członkowskim, a także zapewniać te prawa w odniesieniu do dostawców usług znajdujących się w państwach trzecich.
87. Odnośnie do outsourcingu krytycznych lub istotnych funkcji instytucje i instytucje płatnicze powinny zapewnić, w ramach pisemnej umowy outsourcingu, że dostawca usług udzieli im oraz ich właściwym organom, w tym organom ds. restrukturyzacji i uporządkowanej likwidacji, oraz każdej innej osobie wyznaczonej przez te instytucje lub właściwe organy:
- a. pełnego dostępu do wszystkich odpowiednich lokali (np. siedziby firmy i centrów operacyjnych), w tym do pełnego zakresu odpowiednich urządzeń, systemów, sieci, informacji i danych wykorzystywanych do wykonywania funkcji zleconych na podstawie outsourcingu, w tym do powiązanych informacji finansowych, dotyczących personelu i audytorów zewnętrznych dostawcy usług („prawa do dostępu i informacji”); oraz
 - b. nieograniczonych praw w zakresie kontroli i audytu związanych z umową outsourcingu („prawa do audytu”), aby umożliwić im monitorowanie umowy outsourcingu oraz zapewnić zgodność ze wszystkimi obowiązującymi wymogami prawnymi i umownymi.
88. W odniesieniu do outsourcingu funkcji, które nie są krytyczne lub istotne, instytucje i instytucje płatnicze powinny zapewnić prawa do dostępu i audytu określone w ust. 87 lit. a) i b) oraz w

sekcji 13.3, w oparciu o podejście oparte na analizie ryzyka, z uwzględnieniem charakteru funkcji zleconej na zasadzie outsourcingu oraz związanego z nią ryzyka operacyjnego i ryzyka utraty reputacji, ich skalowalności, potencjalnego wpływu na ciągłość prowadzenia działalności i na okres objęty umową. Instytucje i instytucje płatnicze powinny wziąć pod uwagę, że funkcje mogą z czasem stać się krytyczne lub istotne.

89. Instytucje i instytucje płatnicze dopilnowują, aby umowa outsourcingu lub inne ustalenia umowne nie utrudniały ani nie ograniczały skutecznego korzystania z praw do dostępu i audytu przez te instytucje, właściwe organy lub osoby trzecie wyznaczone przez te instytucje do wykonywania takich praw.
90. Instytucje i instytucje płatnicze powinny korzystać ze swoich praw do dostępu i audytu, określać częstotliwość audytów i obszary podlegające kontroli stosując podejście oparte na analizie ryzyka oraz stosować się do odpowiednich, powszechnie przyjętych krajowych i międzynarodowych standardów audytu³⁵.
91. Z zastrzeżeniem spoczywającej na nich ostatecznej odpowiedzialności za umowy outsourcingu instytucje i instytucje płatnicze mogą stosować:
- a. zbiorcze audyty organizowane wspólnie z innymi klientami tego samego dostawcy usług i przeprowadzane przez instytucje i tych samych klientów lub wyznaczoną przez nich osobą trzecią w celu bardziej efektywnego wykorzystania zasobów audytowych oraz zmniejszenia obciążenia organizacyjnego zarówno po stronie klientów, jak i dostawcy usług;
 - b. certyfikaty osoby trzeciej oraz sprawozdania osoby trzeciej lub sprawozdania z audytu wewnętrznego udostępnione przez dostawcę usług.
92. W przypadku outsourcingu krytycznych lub istotnych funkcji instytucje i instytucje płatnicze powinny ocenić, czy certyfikaty i sprawozdania osób trzecich, o których mowa w ust. 91 lit. b), są odpowiednie i wystarczające do spełnienia ich obowiązków regulacyjnych i na przestrzeni czasu nie powinny opierać się wyłącznie na tych sprawozdaniach.
93. Instytucje i instytucje płatnicze powinny stosować metodę, o której mowa w ust. 91 lit. b), tylko wtedy, gdy:
- a. są zadowolone z planu audytu dotyczącego funkcji zleconej na podstawie outsourcingu;
 - b. zapewniają, aby zakres certyfikatu lub sprawozdania z audytu obejmowały systemy (tj. procesy, aplikacje, infrastrukturę, centra danych itd.) oraz kluczowe mechanizmy kontroli określone przez instytucję lub instytucję płatniczą oraz sprawdzenie zgodności z odpowiednimi wymogami regulacyjnymi;

³⁵W przypadku instytucji proszę zapoznać się z sekcją 22 wytycznych EUNB dotyczących zarządzania wewnętrznego: https://eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29_PL.pdf/1c4d2b82-b044-42fa-8efa-e0867c0335aa

- c. dokonują dokładnej bieżącej oceny treści certyfikatów lub sprawozdań z audytu i weryfikacji, czy sprawozdania lub certyfikaty nie są nieaktualne;
 - d. zapewniają objęcie kluczowych systemów i kontroli przyszłymi wersjami certyfikatu lub sprawozdania z audytu;
 - e. są zadowolone z umiejętności podmiotu certyfikującego lub podmiotu przeprowadzającego audyt (np. w odniesieniu do rotacji firmy certyfikującej lub audytowej, kwalifikacji, wiedzy fachowej, ponownego przeprowadzenia/weryfikacji dowodów w bazowej dokumentacji audytu);
 - f. upewniły się, że certyfikaty zostaną wydane a audyty przeprowadzone zgodnie z powszechnie uznawanymi odpowiednimi standardami zawodowymi i obejmują badanie skuteczności operacyjnej kluczowych kontroli prowadzonych na miejscu;
 - g. mają wynikające z umowy prawo zwrócić się o rozszerzenie zakresu certyfikatów lub sprawozdań z audytu na inne odpowiednie systemy i mechanizmy kontroli; liczba i częstotliwość takich wniosków o zmianę zakresu powinny być uzasadnione i zgodne z prawem z perspektywy zarządzania ryzykiem; oraz
 - h. zachowują wynikające z umowy prawo do przeprowadzania indywidualnych audytów według ich uznania w odniesieniu do outsourcingu krytycznych lub istotnych funkcji.
94. Zgodnie z wytycznymi EUNB w sprawie oceny ryzyka technologii informacyjno-komunikacyjnych w ramach procesu przeglądu i oceny nadzorczej (SREP) instytucje powinny w stosownych przypadkach zapewniać, by były one w stanie przeprowadzać testy penetracyjne w celu oceny skuteczności wdrożonych środków i procesów z zakresu cybernetycznego i wewnętrznego bezpieczeństwa ICT³⁶. Biorąc pod uwagę tytuł I, instytucje płatnicze powinny również posiadać wewnętrzne mechanizmy kontroli ICT, w tym środki kontroli w zakresie ochrony ICT i środki ograniczające ryzyko.
95. Przed planowaną kontrolą na miejscu, instytucje, instytucje płatnicze, właściwe organy i audytorzy lub osoby trzecie działające w imieniu instytucji, instytucji płatniczej lub właściwych organów powinny przekazać dostawcy usług stosowne zawiadomienie, chyba że jest to niemożliwe ze względu na sytuację nadzwyczajną lub kryzysową lub doprowadziłoby to do sytuacji, w której audyt przestanie być skuteczny.
96. Podczas przeprowadzania audytów w środowiskach wielu klientów należy dołożyć starań w celu uniknięcia powstania zagrożeń dla środowiska innego klienta (np. wpływu na gwarantowane poziomy usług, dostępność danych, aspekty poufności) lub ograniczenia takich zagrożeń.

³⁶ Zobacz również wytyczne EUNB w sprawie oceny ryzyka technologii informacyjno-komunikacyjnych: https://eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_PL.pdf/29a924fe-f97e-48da-90d6-3cfe08284a63

97. W przypadku gdy umowa outsourcingu wiąże się z wysokim poziomem złożoności technicznej, na przykład w przypadku outsourcingu usług w chmurze, instytucja lub instytucja płatnicza powinna sprawdzić, czy podmiot, który przeprowadza audyt, niezależnie od tego, czy są to jej audytorzy wewnętrzni, zespół audytorów lub audytorów zewnętrznych działających w jej imieniu, posiada odpowiednie i istotne umiejętności oraz wiedzę w zakresie skutecznego przeprowadzania odpowiednich audytów lub ocen. To samo dotyczy wszystkich pracowników instytucji lub instytucji płatniczej dokonujących kontroli certyfikatów lub audytów przeprowadzonych przez dostawców usług.

13.4 Prawa do rozwiązania umowy

98. W umowie outsourcingu należy w sposób wyraźny umożliwić instytucji lub instytucji płatniczej rozwiązanie umowy zgodnie z obowiązującymi przepisami prawa, w tym w następujących sytuacjach:

- a. jeżeli dostawca wykonujący funkcje zlecone na zasadzie outsourcingu narusza obowiązujące przepisy prawa, regulacje lub postanowienia umowne;
- b. w przypadku wykrycia przeszkód mogących zakłócić wykonywanie funkcji będącej przedmiotem outsourcingu;
- c. w przypadku istotnych zmian mających wpływ na umowę outsourcingu lub dostawcę usług (np. zmiana dotycząca podoutsourcingu lub zmiany podwykonawców);
- d. w przypadku wystąpienia słabości w zakresie zarządzania danymi lub informacjami poufnymi, osobowymi lub szczególnie chronionymi oraz w zakresie ich bezpieczeństwa; oraz
- e. jeżeli właściwy organ instytucji lub instytucji płatniczej wyda nakaz np. w przypadku gdy właściwy organ, z powodu umowy outsourcingu, nie jest już w stanie skutecznie nadzorować instytucji lub instytucji płatniczej.

99. Umowa outsourcingu powinna ułatwiać przeniesienie funkcji zleconej na zasadzie outsourcingu do innego dostawcy usług lub jej ponowne włączenie do instytucji lub instytucji płatniczej. W tym celu pisemna umowa outsourcingu powinna:

- a. jasno określać obowiązki istniejącego dostawcy usług w przypadku przeniesienia funkcji zleconych na zasadzie outsourcingu do innego dostawcy usług lub z powrotem do instytucji lub instytucji płatniczej, również w zakresie przetwarzania danych;
- b. określać odpowiedni okres przejściowy, w którym dostawca usług, po zakończeniu umowy outsourcingu, będzie w dalszym ciągu wykonywał funkcję zlecaną na zasadzie outsourcingu w celu ograniczenia ryzyka powstania zakłóceń; oraz

- c. obejmować zobowiązanie dostawcy usług do wspierania instytucji lub instytucji płatniczej w prawidłowym przeniesieniu funkcji w przypadku rozwiązania umowy outsourcingu.

14 Nadzór nad funkcjami zleconymi na zasadzie outsourcingu

100. Instytucje i instytucje płatnicze na bieżąco monitorują wyniki działalności dostawców usług w odniesieniu do wszystkich umów outsourcingu stosując podejście oparte na ryzyku, przy czym główny nacisk kładą na outsourcing krytycznych lub istotnych funkcji, w tym na zapewnienie dostępności, integralności i bezpieczeństwa danych i informacji. Jeżeli ryzyko, charakter lub skala funkcji zleconej na zasadzie outsourcingu uległy znacznej zmianie, instytucje i instytucje płatnicze oceniają ponownie krytyczne lub istotne znaczenie danej funkcji zgodnie z sekcją 4.
101. Instytucje i instytucje płatnicze monitorują umowy outsourcingu i zarządzają nimi z należytą wprawą, rozważą i starannością.
102. Instytucje regularnie aktualizują swoją ocenę ryzyka zgodnie z sekcją 12.2 i okresowo składają organowi zarządzającemu sprawozdania na temat zidentyfikowanego ryzyka związanego z outsourcingiem krytycznych lub istotnych funkcji.
103. Instytucje i instytucje płatnicze monitorują swoje wewnętrzne ryzyko koncentracji wynikające z umów outsourcingu i zarządzają nim z uwzględnieniem postanowień sekcji 12.2 niniejszych wytycznych.
104. Instytucje i instytucje płatnicze, kładąc główny nacisk na krytyczne lub istotne funkcje podlegające outsourcingowi, na bieżąco zapewniają, aby umowy outsourcingu spełniały odpowiednie normy w zakresie wyników i jakości zgodnie ze swoimi strategiami:
 - a. dopilnowując, aby otrzymywały odpowiednie sprawozdania od usługodawców;
 - b. oceniając wyniki działalności dostawców za pomocą takich narzędzi jak kluczowe wskaźniki efektywności, kluczowe wskaźniki kontroli, sprawozdania z realizacji usług, certyfikacja własna oraz niezależne weryfikacje;
 - c. przeglądając wszystkie inne istotne informacje otrzymane od dostawcy usług, w tym sprawozdania na temat środków na rzecz zapewnienia ciągłości działania i testowania.
105. Instytucje powinny przedsięwziąć odpowiednie środki, jeżeli stwierdzą niedociągnięcia w zakresie wykonywania funkcji zleconych na zasadzie outsourcingu. W szczególności instytucje i instytucje płatnicze podejmują działania następcze w odniesieniu do wszelkich przesłanek świadczących o tym, że dostawcy usług nie mogą wykonać krytycznej lub istotnej funkcji zleconej na zasadzie outsourcingu w sposób skuteczny lub zgodny z obowiązującymi przepisami prawa i wymogami regulacyjnymi. W przypadku zidentyfikowania niedociągnięć instytucje i instytucje płatnicze podejmują odpowiednie działania naprawcze lub zaradcze. Działania takie

mogą obejmować, w razie potrzeby, rozwiązanie umowy outsourcingu ze skutkiem natychmiastowym.

15 Strategie wyjścia

106. Instytucje i instytucje płatnicze w przypadku outsourcingu krytycznych lub istotnych funkcji powinny posiadać udokumentowaną strategię wyjścia zgodną z ich polityką w zakresie outsourcingu i planami ciągłości działania³⁷, która powinna uwzględniać co najmniej:

- a. możliwość rozwiązania umów outsourcingu;
- b. niewykonanie świadczenia ze strony dostawcy usług;
- c. pogorszenie jakości wykonywanej funkcji oraz rzeczywiste lub potencjalne zakłócenia działalności spowodowane niewłaściwym wykonaniem funkcji lub jej niewykonaniem;
- d. istotne zagrożenia dla odpowiedniego i ciągłego wykonywania danej funkcji.

107. Instytucje i instytucje płatnicze powinny zapewnić sobie możliwość wycofania się z umów outsourcingu w taki sposób, aby nie spowodować zbędnych zakłóceń w ich działalności, bez uszczerbku dla zachowania przez nie zgodności z wymogami regulacyjnymi i bez szkody dla ciągłości i jakości świadczenia usług na rzecz klientów. W tym celu powinny one:

- a. opracować i wdrożyć kompleksowe, udokumentowane i, w stosownych przypadkach, odpowiednio sprawdzone plany wyjścia (np. poprzez przeprowadzenie analizy potencjalnych kosztów, oddziaływania, zasobów i skutków czasowych przeniesienia usługi zleconej na zasadzie outsourcingu na rzecz alternatywnego dostawcy); oraz
- b. określić alternatywne rozwiązania i opracować plany przejściowe, aby umożliwić instytucji lub instytucji płatniczej usunięcie zleconych na zasadzie outsourcingu funkcji i danych od dostawcy usług i przeniesienie ich do alternatywnego dostawcy lub z powrotem do instytucji lub instytucji płatniczej lub przedsięwzięcie innych środków zapewniających ciągłe wykonywanie krytycznych lub istotnych funkcji lub działalności w kontrolowany i odpowiednio przetestowany sposób, uwzględniając wyzwania, jakie mogą pojawić się w związku z lokalizacją danych oraz podejmując niezbędne środki na rzecz zapewnienia ciągłości działania w fazie przejściowej.

108. Opracowując strategię wyjścia instytucje i instytucje płatnicze powinny:

- a. określić cele strategii wyjścia;

³⁷ Instytucje, zgodnie z wymogami określonymi w art. 85 ust. 2 dyrektywy 2013/36/UE oraz tytułem VI wytycznych EUNB w sprawie zarządzania wewnętrznego, oraz instytucje płatnicze powinny dysponować odpowiednimi planami ciągłości działania w odniesieniu do outsourcingu krytycznych lub istotnych funkcji.

- b. przeprowadzić analizę wpływu na działalność proporcjonalną do ryzyka związanego ze zleconymi na zasadzie outsourcingu procesami, usługami lub działaniami w celu ustalenia, jakie zasoby ludzkie i finansowe byłyby niezbędne do wdrożenia planu wyjścia i jak dużo czasu zajęłoby jego wdrożenie;
- c. przydzielić role, obowiązki i odpowiednie zasoby do zarządzania planami wyjścia i działaniami związanymi z przeniesieniem;
- d. określić kryteria powodzenia w zakresie przeniesienia funkcji zleconych na zasadzie outsourcingu i danych; oraz
- e. określić wskaźniki, które należy stosować w celu monitorowania umowy outsourcingu (jak przedstawiono w sekcji 14), w tym wskaźniki na podstawie niedopuszczalnych poziomów usług, osiągnięcie których powinno skutkować wyjściem.

Tytuł V – Wytyczne w sprawie outsourcingu skierowane do właściwych organów

- 109. Ustanawiając odpowiednie metody monitorowania przestrzegania przez instytucje i instytucje płatnicze warunków dotyczących udzielenia pierwszego zezwolenia, właściwe organy powinny dążyć do określenia, czy umowy outsourcingu powodują istotną zmianę warunków i obowiązków wynikających z pierwszego zezwolenia instytucji i instytucji płatniczych.
- 110. Właściwe organy powinny mieć pewność, że są w stanie skutecznie nadzorować instytucje i instytucje płatnicze, w tym że instytucje lub instytucje płatnicze, w ramach umów outsourcingu, dopilnowały, aby dostawcy usług byli zobowiązani do udzielenia właściwemu organowi oraz instytucji praw do audytu i dostępu, zgodnie z sekcją 13.3.
- 111. Analizę ryzyka związanego z outsourcingiem, które ponosi instytucja, przeprowadza się przynajmniej w ramach procesu przeglądu i oceny nadzorczej lub, w odniesieniu do instytucji płatniczych, w ramach innych procesów nadzoru, w tym wniosków na zasadzie ad hoc lub w trakcie kontroli na miejscu.
- 112. W związku z informacjami zapisanymi w rejestrze, o którym mowa w sekcji 11, właściwe organy mogą zwrócić się do instytucji i instytucji płatniczych o dostarczenie dodatkowych informacji, w szczególności w odniesieniu do krytycznych lub istotnych umów outsourcingu, takich jak:
 - a. szczegółowa analiza ryzyka;
 - b. czy dostawca usług posiada plan ciągłości działania, który jest odpowiedni dla usług świadczonych na rzecz instytucji lub instytucji płatniczej korzystającej z outsourcingu;
 - c. strategia wyjścia stosowana w przypadku rozwiązania umowy outsourcingu przez którąkolwiek ze stron lub w przypadku zakłóceń w świadczeniu usług; oraz

- d. zasoby i środki służące odpowiedniemu monitorowaniu działań zleconych na zasadzie outsourcingu.
113. W uzupełnieniu informacji wymaganych na podstawie sekcji 11 właściwe organy mogą wymagać, aby instytucje i instytucje płatnicze przedstawiły szczegółowe informacje na temat wszelkich umów outsourcingu, nawet jeżeli dana funkcja nie jest uznawana za krytyczną lub istotną.
114. Właściwe organy stosując podejście oparte na analizie ryzyka oceniają następujące elementy:
- a. czy instytucje i instytucje płatnicze w odpowiedni sposób monitorują umowy outsourcingu, w szczególności te o znaczeniu krytycznym lub istotnym, i w odpowiedni sposób nimi zarządzają;
 - b. czy instytucje i instytucje płatnicze dysponują odpowiednimi zasobami, aby monitorować umowy outsourcingu i zarządzać nimi;
 - c. czy instytucje i instytucje płatnicze identyfikują wszystkie istotne rodzaje ryzyka i zarządzają nimi; oraz
 - d. czy instytucje i instytucje płatnicze identyfikują konflikty interesów, oceniają je i właściwie nimi zarządzają w odniesieniu do umów outsourcingu, np. w przypadku wewnątrzgrupowego outsourcingu lub outsourcingu w ramach tego samego instytucjonalnego systemu ochrony.
115. Właściwe organy dopilnowują, aby instytucje i instytucje płatnicze UE/EOG nie działały jako „puste struktury”, z uwzględnieniem sytuacji, w których instytucje stosują transakcje typu back to back lub transakcje wewnątrzgrupowe w celu przeniesienia części ryzyka rynkowego i kredytowego na podmiot spoza UE/EOG, oraz aby posiadały odpowiednie zasady zarządzania i mechanizmy zarządzania ryzykiem na potrzeby identyfikacji ryzyka i zarządzania nim.
116. W ramach swojej oceny właściwe organy powinny uwzględnić wszystkie rodzaje ryzyka, w szczególności³⁸:
- a. ryzyko operacyjne³⁹ wynikające z umowy outsourcingu;
 - b. ryzyko utraty reputacji;
 - c. ryzyko związane ze wstąpieniem w prawa i obowiązki, które mogłoby wymagać od instytucji ratowania dostawcy usług w przypadku istotnych instytucji;

³⁸ W przypadku instytucji objętych zakresem dyrektywy 2013/36/UE – zob. również wytyczne EUNB dotyczące SREP: <https://eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2>

³⁹ Zobacz również wytyczne EUNB w sprawie oceny ryzyka technologii informacyjno-komunikacyjnych: https://eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_PL.pdf/29a924fe-f97e-48da-90d6-3cfe08284a63

- d. ryzyko koncentracji w obrębie instytucji, w tym na zasadzie skonsolidowanej, wynikające z wielu umów outsourcingu zawartych z jednym dostawcą usług lub dostawcami usług blisko ze sobą związanymi lub z wielu umów outsourcingu w ramach tego samego obszaru działalności;
 - e. ryzyko koncentracji na poziomie sektora, np. w przypadku gdy wiele instytucji lub instytucji płatniczych korzysta z usług jednego dostawcy usług lub niewielkiej grupy dostawców usług;
 - f. zakres, w jakim instytucja lub instytucja płatnicza zlecająca outsourcing kontroluje dostawcę usług lub ma możliwość wpływania na jego działania, ograniczenie ryzyka, które może wynikać z wyższego poziomu kontroli oraz czy dostawca usług jest objęty skonsolidowanym nadzorem grupy; oraz
 - g. konflikty interesów między instytucją a dostawcą usług.
117. W przypadku zidentyfikowania ryzyka koncentracji właściwe organy monitorują rozwój takiego ryzyka i oceniają zarówno jego potencjalny wpływ na inne instytucje i instytucje płatnicze, jak i na stabilność rynku finansowego; w stosownych przypadkach właściwe organy informują organ ds. restrukturyzacji i uporządkowanej likwidacji o nowych potencjalnie krytycznych funkcjach⁴⁰, które zostały zidentyfikowane w ramach tej oceny.
118. W przypadku stwierdzenia zastrzeżeń, które prowadzą do wniosku, że instytucja lub instytucja płatnicza nie posiada już solidnych zasad zarządzania lub nie spełnia wymogów regulacyjnych, właściwe organy powinny podjąć odpowiednie działania, które mogą obejmować ograniczenie zakresu funkcji zleczanych na zasadzie outsourcingu lub zażądanie wyjścia z jednej umowy outsourcingu lub większej liczby takich umów. W szczególności, biorąc pod uwagę potrzebę działania instytucji lub instytucji płatniczej w sposób ciągły, anulowanie umów może być wymagane w sytuacji gdy nadzoru nad wymogami regulacyjnymi i ich egzekwowania nie można zapewnić za pomocą innych środków.
119. Właściwe organy powinny mieć pewność, że są w stanie sprawować skuteczny nadzór, w szczególności gdy instytucje i instytucje płatnicze zlecają na zasadzie outsourcingu krytyczne lub istotne funkcje, które są wykonywane poza UE/EOG.

⁴⁰ Zgodnie z definicją zawartą w art. 2 ust. 1 pkt. 35 dyrektywy w sprawie naprawy oraz restrukturyzacji i uporządkowanej likwidacji banków.