EIOPA-BoS-20-002

Wytyczne dotyczące outsourcingu do dostawców usług chmury obliczeniowej

Spis treści

Wprowadzenie

1. Zgodnie z art. 16 rozporządzenia (UE) nr 1094/2010[1] EIOPA wydaje wytyczne, aby zapewnić zakładom ubezpieczeń i reasekuracji wskazówki dotyczące sposobu stosowania przepisów dotyczących outsourcingu określonych w dyrektywie 2009/138/WE[2] („dyrektywa Wypłacalność II") oraz w rozporządzeniu delegowanym Komisji (UE) 2015/35[3] („rozporządzenie delegowane") w przypadku outsourcingu do dostawców usług chmury obliczeniowej.
2. Niniejsze wytyczne opierają się na art. 13 ust. 28, art. 38 i 49 dyrektywy Wypłacalność II oraz art. 274 rozporządzenia delegowanego. Ponadto niniejsze wytyczne opierają się na wytycznych zawartych w wytycznych EIOPA dotyczących systemu zarządzania (EIOPA-BoS-14/253).
3. Niniejsze wytyczne skierowane są do właściwych organów w celu zapewnienia wskazówek dotyczących sposobu, w jaki zakłady ubezpieczeń i reasekuracji (zwane dalej łącznie „zakładem" lub „zakładami") powinny stosować wymogi w zakresie outsourcingu przewidziane w wyżej wymienionych aktach prawnych w kontekście outsourcingu do dostawców usług chmury obliczeniowej.
4. Wytyczne mają zastosowanie zarówno do poszczególnych zakładów, jak i odpowiednio do grup[4].

   Podmioty podlegające innym wymogom sektorowym, które wchodzą w skład grupy, są wyłączone z zakresu stosowania niniejszych wytycznych na poziomie indywidualnym, ponieważ zobowiązane są przestrzegać szczególnych wymogów sektorowych, a także odpowiednich wytycznych wydanych przez Europejski Urząd Nadzoru Giełd i Papierów Wartościowych oraz Europejski Urząd Nadzoru Bankowego.
5. W przypadku outsourcingu wewnątrzgrupowego i podoutsourcingu do dostawców usług chmury obliczeniowej niniejsze wytyczne powinno się stosować w połączeniu z postanowieniami wytycznych EIOPA dotyczących systemu zarządzania w zakresie outsourcingu wewnątrzgrupowego.
6. Zakłady i właściwe organy powinny, przestrzegając niniejszych wytycznych lub nadzorując ich przestrzeganie, brać pod uwagę zasadę proporcjonalności[5] oraz krytyczność lub wagę usługi zleconej na zasadzie outsourcingu dostawcom usług chmury obliczeniowej. Zasada proporcjonalności zapewnia, aby zasady zarządzania, w tym te związane z outsourcingiem do dostawców usług chmury obliczeniowej, były proporcjonalne do charakteru, skali i złożoności podstawowego ryzyka.
7. Niniejsze wytyczne należy czytać w powiązaniu z wytycznymi EIOPA dotyczącymi systemu zarządzania oraz bez uszczerbku dla tych wytycznych i dla obowiązków regulacyjnych wymienionych w ust. 1.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1094/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/79/WE (Dz.U. L 331 z 15.12.2010, s. 48).

[2] Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.U. L 335 z 17.12.2009, s. 1).

[3] Rozporządzenie delegowane Komisji (UE) 2015/35 z dnia 10 października 2014 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2009/138/WE w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.U. L 12 z 17.1.2015, s. 1).

[4] Artykuł 212 ust. 1 dyrektywy Wypłacalność II.

[5] Artykuł 29 ust. 3 dyrektywy Wypłacalność II.

Definicje

8. Jeżeli terminy nie zostały zdefiniowane w niniejszych wytycznych, uznaje się, że mają one znaczenie nadane im w aktach prawnych przywołanych we wprowadzeniu.

9. Ponadto do celów niniejszych wytycznych stosuje się następujące definicje.

Dostawca usług	oznacza podmiot zewnętrzny, który realizuje proces, usługę lub czynność lub ich części na podstawie ustalenia dotyczącego outsourcingu.
Dostawca usługchmury obliczeniowej	oznacza dostawcę usług, zgodnie z powyższą definicją, odpowiedzialnego za świadczenie usług chmury obliczeniowej na podstawie ustalenia dotyczącego outsourcingu.
Usługi chmury obliczeniowej	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 przez ogół społeczeństwa.
Chmura prywatna	oznacza infrastrukturę chmury dostępną do wyłącznego użytku jednego zakładu.
Chmura społecznościowa	oznacza infrastrukturę chmury dostępną do wyłącznego użytku konkretnej wspólnoty zakładów, np. kilku zakładów z jednej grupy.
Chmura hybrydowa	oznacza infrastrukturę chmury złożoną z dwóch lub więcej odrębnych infrastruktur chmury.

Data rozpoczęcia stosowania

10. Niniejsze wytyczne mają zastosowanie od dnia 1 stycznia 2021 r. do wszystkich ustaleń dotyczących outsourcingu do chmury obliczeniowej zawartych lub zmienionych tego dnia lub po tym dniu.

11. Zakłady, aby zapewnić zgodność z niniejszymi wytycznymi do dnia 31 grudnia 2022 r., powinny dokonać przeglądu istniejących ustaleń dotyczących outsourcingu do chmury obliczeniowej związanych z krytycznymi lub istotnymi funkcjami lub czynnościami operacyjnymi i odpowiednio je zmienić.

12. Jeżeli przegląd ustaleń dotyczących outsourcingu do chmury obliczeniowej związanych z krytycznymi lub istotnymi funkcjami lub czynnościami operacyjnymi nie zakończy się do dnia 31 grudnia 2022 r., zakład powinien powiadomić właściwy organ nadzoru[6] o tym fakcie, w tym o działaniach, które zaplanował w celu zakończenia przeglądu, lub o potencjalnej strategii wyjścia. W stosownych przypadkach organ nadzoru może uzgodnić z zakładem przedłużony termin zakończenia tego przeglądu.

13. Aktualizacji (w razie potrzeby) strategii i procesów wewnętrznych zakładu należy dokonać do dnia 1 stycznia 2021 r., natomiast wymogi w zakresie dokumentacji na

[6] Artykuł 13 ust. 10 dyrektywy Wypłacalność II.

potrzeby ustaleń dotyczących outsourcingu dochmury obliczeniowej związanych z krytycznymi lub istotnymi funkcjami lub czynnościami operacyjnymi należy wdrożyć do dnia 31 grudnia 2022 r.

Wytyczna nr 1 – Usługi chmury obliczeniowej i outsourcing

14. Zakład powinien określić, czy ustalenie dotyczące outsourcingu dokonane z dostawcą usług chmury obliczeniowej wchodzi w zakres definicji outsourcingu zgodnie z dyrektywą Wypłacalność II. W ramach oceny należy wziąć pod uwagę:

a. czy funkcja lub czynność operacyjna (lub ich część) zlecane na podstawie outsourcingu są wykonywane w sposób powtarzalny lub ciągły; oraz

b. czy funkcja lub czynność operacyjna (lub ich część) wchodziłyby normalnie w zakres funkcji lub czynności operacyjnych, które byłyby lub mogłyby być realizowane przez zakład w ramach jego zwykłej działalności gospodarczej, nawet jeżeli zakład nie wykonywał takiej funkcji lub czynności operacyjnej w przeszłości.

15. W przypadku gdy ustalenie z dostawcą usług obejmuje wiele funkcji lub czynności operacyjnych, zakład powinien uwzględnić w swojej ocenie wszystkie aspekty ustalenia.

16. W przypadku gdy zakład zleca wykonywanie funkcji lub czynnośći operacyjnych na zasadzie outsourcingu dostawcom usług, którzy nie są dostawcami usług chmury obliczeniowej, ale w znacznym stopniu polegają na infrastrukturze chmury obliczeniowej w celu świadczenia swoich usług (na przykład gdy dostawca usług chmury oblicznioewej jest częścią łańcucha podoutsourcingu), ustalenie dotyczące takiego outsourcingu wchodzi w zakres stosowania niniejszych wytycznych.

Wytyczna nr 2 – Ogólne zasady zarządzania w odniesieniu do outsourcingu do chmury obliczeniowej

17. Z zastrzeżeniem przepisów art. 274 ust. 3 rozporządzenia delegowanego organ administrujący, zarządzający lub nadzorczy zakładu powinien zapewnić, aby każda decyzja o zleceniu na zasadzie outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych dostawcom usług chmury obliczeniowej była podejmowana na podstawie dokładnej oceny ryzyka, obejmującej wszystkie istotne rodzaje ryzyka wynikające ze stosownegoustalenia, takie jak ryzyko związane z technologią informacyjno-komunikacyjną („ICT”), ciągłością działania, prawem i zgodnością z przepisami, koncentracją, i inne rodzaje ryzyk operacyjnych oraz tych związanych z migracją danych lub fazą wdrażania, w stosownych przypadkach.

18. W przypadku outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych do dostawców usług chmury obliczeniowej zakład, w stosownych przypadkach, uwzględnia zmiany w profilu ryzyka wynikające z ustaleń dotyczących outsourcingu do chmury obliczeniowej w ramach własnej oceny ryzyka i wypłacalności („ORSA”).

19. Korzystanie z usług chmury obliczeniowej powinno być spójne ze strategiami danego zakładu (na przykład strategią ICT, strategią bezpieczeństwa informacji, strategią zarządzania ryzykiem operacyjnym) oraz wewnętrzną polityką i procesami, które w razie potrzeby należy aktualizować.

Wytyczna nr 3 – Aktualizacja pisemnej polityki outsourcingu

20. W przypadku outsourcingu do dostawców usług chmury obliczeniowejzakład powinien zaktualizować pisemną politykę outsourcingu (np. poprzez jej przegląd, dodanie oddzielnego załącznika lub opracowanie nowych specjalnych strategii) oraz inne odpowiednie strategie wewnętrzne (np. w zakresie bezpieczeństwa informacji), uwzględniając specyfikę outsourcingu do chmury obliczeniowej przynajmniej w następujących obszarach:

a. role i zakres odpowiedzialności zaangażowanych funkcji zakładu, w szczególności organu administrującego, zarządzającego lub nadzorczego, oraz funkcji odpowiedzialnych za ICT, bezpieczeństwo informacji, zgodność, zarządzanie ryzykiem i audyt wewnętrzny;

b. procesy i procedury sprawozdawcze wymagane do zatwierdzenia, wdrożenia, monitorowania i odnawiania, w stosownych przypadkach, ustaleń dotyczących outsourcingu do chmury obliczeniowej oraz zarządzania takimi ustaleniami, związanymi z krytycznymi lub istotnymi funkcjami lub czynnościami operacyjnymi;

c. nadzór nad usługami chmury obliczeniowej proporcjonalny do charakteru, skali i złożoności ryzyka właściwego dla świadczonych usług, w tym (i) ocena ryzyka w odniesieniu do ustaleń dotyczących outsourcingu do chmury obliczeniowej i analiza due diligence w odniesieniu do dostawców usług chmury obliczeniowej, w tym częstotliwość oceny ryzyka; (ii) monitorowanie i kontrole zarządzania (np. weryfikacji umowy o gwarantowanym poziomie świadczenia usług); (iii) normy i kontrole bezpieczeństwa;

d. w odniesieniu do outsourcingu do chmury obliczeniowej krytycznych lub istotnych funkcji lub czynności operacyjnych należy odnieść się do wymogów dotyczących umowy opisanych w wytycznej nr 10;

e. wymogi dotyczące dokumentacji i pisemne powiadomienie organu nadzoru o outsourcingu do chmury obliczeniowej krytycznych lub istotnych funkcji lub czynności operacyjnych;

f. w odniesieniu do każdego ustalenia dotyczącego outsourcingu do chmury obliczeniowej obejmującego krytyczne lub istotne funkcje lub czynności operacyjne wymóg udokumentowanej i, w stosownych przypadkach, odpowiednio sprawdzonej „strategii wyjścia" proporcjonalnej do charakteru, skali i złożoności ryzyka właściwego dla świadczonych usług; strategia wyjścia może obejmować szereg procedur zakończenia, w tym między innymi zaprzestanie świadczenia, reintegrację lub przeniesienie usług objętych ustaleniem dotyczącym outsourcingu do chmury obliczeniowej.

Wytyczna nr 4 – Pisemne powiadomienie organu nadzoru

21. Wymogi dotyczące pisemnego powiadamiania określone w art. 49 ust. 3 dyrektywy Wypłacalność II i uszczegółowione w wytycznych EIOPA dotyczących systemu zarządzania mają zastosowanie do outsourcingu krytycznych lub istotnych funkcji i czynności operacyjnych do dostawcówusług chmury obliczeniowej. W przypadku gdy dana funkcja lub czynność operacyjna zlecona na zasadzie outsourcingu uprzednio sklasyfikowana jako niekrytyczna lub nieistotna stanie się krytyczna lub istotna, zakład powinien powiadomić o tym organ nadzoru.

22. Sporządzane przez zakład pisemne powiadomienie powinno zawierać, przy uwzględnieniu zasady proporcjonalności, co najmniej następujące informacje:

a. krótki opis funkcji lub czynności operacyjnej zlecanej na zasadzie outsourcingu;

b. termin rozpoczęcia oraz, w zależności od przypadku, datę odnowienia umowy, datę zakończenia lub okresy wypowiedzenia obowiązujące dostawcę usług chmury obliczeniowej i zakład;

c. prawo właściwe dla umowy outsourcingu do chmury obliczeniowej;

d. nazwę dostawcy usług chmury obliczeniowej, numer ewidencyjny przedsiębiorstwa, identyfikator podmiotu prawnego (jeżeli jest dostępny), adres i inne stosowne dane kontaktowe oraz nazwę jednostki dominującej (jeżeli istnieje); w przypadku grup – niezależnie od tego, czy dostawca usług chmury obliczeniowej stanowi część grupy;

e. usługi chmury obliczeniowej i modele wdrażania (tj. publiczny/prywatny/hybrydowy/społecznościowy) oraz specyfikę danych, które mają być przechowywane, oraz lokalizację (tj. kraje lub regiony), gdzie dane będą przechowywane;

f. krótkie podsumowanie powodów, dla których zlecona na zasadzie outsourcingu funkcja lub czynność operacyjna jest uważana za krytyczną lub istotną;

g. datę ostatniej oceny krytycznego lub istotnego znaczenia funkcji lub czynności operacyjnej zleconej na zasadzie outsourcingu.

Wytyczna nr 5 – Wymogi dotyczące dokumentacji

23. W ramach swojego systemu zarządzania i zarządzania ryzykiem zakład powinien prowadzić ewidencję swoich ustaleń dotyczących outsourcingu do chmury obliczeniowej, na przykład w formie specjalnego, aktualizowanego z czasem rejestru. Zakład powinien również prowadzić rejestr wypowierdzianych ustaleń dotyczących outsourcingu do chmury obliczeniowej przez odpowiedni okres przechowywania, podlegający regulacji krajowej.

24. W przypadku outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych zakład powinien rejestrować wszystkie poniższe informacje:

a. informacje, które należy przekazać organowi nadzoru, o których mowa w wytycznej nr 4;

b. w przypadku grup, informacje na temat zakładów ubezpieczeń lub reasekuracji i innych zakładów objętych zakresem konsolidacji ostrożnościowej, które korzystają z usług chmury obliczeniowej;

c. datę ostatniej oceny ryzyka i krótkie streszczenie ogólnych wyników;

d. informacje na temat osoby fizycznej lub organu decyzyjnego (np. organu administrującego, zarządzającego lub nadzorczego) w zakładzie, którzy zatwierdzili ustalenie dotyczące outsourcingu do chmury obliczeniowej;

e. daty ostatnich i kolejnych zaplanowanych audytów, w stosownych przypadkach;

f. nazwy podwykonawców, którym zlecane są na zasadzie outsourcingu istotne części krytycznych i istotnych funkcji lub czynności operacyjnych, w tym kraje, gdzie są zarejestrowani, gdzie wykonywana będzie usługa oraz, jeżeli dotyczy, lokalizacje (tj. kraje lub regiony) przechowywania danych;

g. wynik oceny substytucyjności dostawcy usług chmury obliczeniowej (np. łatwa, trudna lub niemożliwa);

h. czy krytyczna lub istotna funkcja lub czynność operacyjna zlecona na zasadzie outsourcingu wspiera działalność, która jest zależna od czasu;

i. szacowane roczne koszty budżetowe;

j. informacje o posiadaniu przez zakład strategii wyjścia na wypadek zakończenia współpracy przez którąkolwiek ze stron lub zakłócenia świadczenia usług przez dostawcę usług chmury obliczeniowej.

25. W przypadku powierzania na zasadzie outsourcingu niekrytycznych lub nieistotnych funkcji lub czynności operacyjnych zakład powinien określić informacje, które należy zarejestrować, na podstawie charakteru, skali i złożoności ryzyk właściwych dla usług świadczonych przez dostawcę usług chmury obliczeniowej.

26. Zakład powinien udostępnić organowi nadzoru, na jego wniosek, wszelkie informacje niezbędne do umożliwienia organowi nadzoru sprawowanie nadzoru nad zakładem, w tym kopię ustalenia dotyczącego outsourcingu.

Wytyczna nr 6 – Analiza poprzedzająca outsourcing

27. Przed dokonaniem jakiegokolwiek ustalenia z dostawcami usług chmury obliczeniowej zakład powinien:

a. ocenić, czy ustalenie dotyczące outsourcingu do chmury obliczeniowej dotyczy krytycznej lub istotnej funkcji lub czynności operacyjnej, zgodnie z wytyczną nr 7;

b. zidentyfikować i ocenić wszystkie istotne ryzyka ustalenia dotyczącego outsourcingu do chmury obliczeniowej, zgodnie z wytyczną nr 8;

c. przeprowadzić odpowiednią analizę due diligence dotyczącą przyszłego dostawcy usług chmury obliczeniowej, zgodnie z wytyczną nr 9;

d. zidentyfikować i ocenić konflikty interesów, które może spowodować outsourcing, zgodnie z wymogami określonymi w art. 274 ust. 3 lit. b) rozporządzenia delegowanego.

Wytyczna nr 7 – Ocena krytycznych lub istotnych funkcji i czynności operacyjnych

28. Przed dokonaniem jakiegokolwiek ustalelenia dotyczącego outsourcingu z dostawcami usług chmury obliczeniowej zakład powinien ocenić, czy ustalenie dotyczące outsourcingu do chmury obliczeniowej dotyczy funkcji operacyjnej lub czynności operacyjnej, które są krytyczne lub istotne. Dokonując takiej oceny, zakład powinien, w stosownych przypadkach, rozważyć, czy dane ustalenie może stać się w przyszłości krytyczne lub istotne. Zakład powinien również dokonać ponownej oceny krytycznego lub istotnego znaczenia funkcji operacyjnej lub czynności operacyjnej, które wcześniej były zlecane na zasadzie outsourcingu dostawcom usług chmury obliczeniowej, jeżeli charakter, skala i złożoność ryzyka wynikającego z umowy istotnie się zmienią.

29. W swojej ocenie zakład powinien uwzględnić, wraz z wynikiem oceny ryzyka, co najmniej następujące czynniki:

a. potencjalny wpływ istotnego zakłócenia na funkcję lub czynność operacyjną zleconą na zasadzie outsourcingu lub niewykonania przez dostawcę usługi chmury obliczeniowej usługi na uzgodnionym, gwarantowanym poziomie usług na:

   i. wypełnianie przez zakład w sposób ciągły jego obowiązków regulacyjnych;

   ii. krótko- i długoterminową odporność finansową zakładu i jego wypłacalność oraz rentowność;

   iii. ciągłość działania i odporność operacyjną zakładu;

iv. ryzyko operacyjne zakładu, w tym prowadzenie działalności, ICT i ryzyko prawne;

v. ryzyko utraty reputacji zakładu;

b. potencjalny wpływ ustalenia dotyczącego outsourcingu do dostawcy usług chmury ubliczeniowej na zdolność zakładu do:

i. identyfikacji wszelkiego ryzyka, zarządzania ryzykiem i jego monitorowania;

ii. spełnienia wszystkich wymogów prawnych i regulacyjnych;

iii. przeprowadzania odpowiednich kontroli w odniesieniu do funkcji lub czynności operacyjnej zleconych na zasadzie outsourcingu;

c. łączną ekspozycję zakładu (lub w stosownych przypadkach grupy) na tego samego dostawcę usług chmury obliczeniowej oraz potencjalny łączny wpływ ustaleń dotyczących outsourcingu w tym samym obszarze działalności;

d. rozmiar i złożoność obszarów działalności zakładu, na które wpływ ma ustalenie dotyczące outsourcingu do chmury obliczeniowej;

e. jeżeli jest to konieczne lub pożądane – możliwość przeniesienia proponowanego ustalenia dotyczącego outsourcingu do chmury obliczeniowej na innego dostawcę usług chmury obliczeniowej lub możliwość reintegracji usług („substytucyjność");

f. ochronę danych osobowych i nieosobowych oraz potencjalny wpływ naruszenia poufności lub niezapewnienia dostępności i integralności danych na zakład, ubezpieczających lub inne istotne podmioty na podstawie m.in. rozporządzenia (UE) 2016/679[7]; zakład uwzględnia w szczególności dane stanowiące tajemnicę handlową lub dane szczególnie chronione (np. dane dotyczące zdrowia ubezpieczających).

Wytyczna nr 8 – Ocena ryzyka outsourcingu do chmury obliczeniowej

30. Co do zasady zakład powinien przyjąć podejście proporcjonalne do charakteru, skali i złożoności ryzyka właściwego dla usług zlecanych na zasadzie outsourcingu dostawcom usług chmury obliczeniowej. Obejmuje to ocenę potencjalnego wpływu outsourcingu do chmury obliczeniowej, w szczególności na ryzyko operacyjne i ryzyko utraty reputacji.

31. W przypadku outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych do dostawców usług chmury obliczeniowej zakład powinien:

a. uwzględnić oczekiwane korzyści i koszty proponowanego ustalenia dotyczącego outsourcingu do chmury obliczeniowej, w tym zważyć wszelkie istotne ryzyka, które można ograniczyć lub którymi można lepiej zarządzać względem wszelkich znaczących ryzyk, które mogą powstać w wyniku proponowanego ustalenia dotyczącego outsourcingu do chmury obliczeniowej;

b. ocenić, w stosownych przypadkach i w razie potrzeby, ryzyko, w tym prawne, ryzyko związane z ICT, ryzyko braku zgodności i ryzyko utraty reputacji, a także ograniczenia w zakresie nadzoru wynikające z:

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

i. wybranej usługi chmury obliczeniowej oraz proponowanego modelu wdrożenia
(tj. publicznego/prywatnego/hybrydowego/społecznościowego);

ii. migracji lub wdrożenia;

iii. czynności i powiązanych danych i systemów, które mają zostać zlecone (lub zostały zlecone) na zasadzie outsourcingu oraz ich wrażliwości i wymaganych środków bezpieczeństwa;

iv. stabilności politycznej i sytuacji w zakresie bezpieczeństwa państw (w obrębie UE lub poza nią), w których usługi te są lub mogą być świadczone i w których dane są lub mogą być przechowywane; w ocenie należy uwzględnić:

1. obowiązujące przepisy, w tym przepisy prawa w zakresie ochrony danych;

2. obowiązujące przepisy w zakresie egzekwowania prawa;

3. 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 zakładu;

v. podoutsourcing, w tym dodatkowe ryzyka, które mogą powstać, jeżeli podwykonawca ma siedzibę w państwie trzecim lub w kraju innym niż dostawca usług chmury obliczeniowej, oraz ryzyko, że długie i złożone łańcuchy podoutsourcingu zmniejszają zdolność zakładu do nadzorowania jego krytycznych lub istotnych funkcji lub czynności operacyjnych oraz zdolność organów nadzoru do sprawowania nad nimi skutecznego nadzoru;

vi. faktu, iż zakłady ponoszą ogólne ryzyko koncentracji w stosunku do tego samego dostawcy usług chmury obliczeniowej, w tym ryzyka wynikającego z outsourcingu do dostawcy usług chmury obliczeniowej, którego nie jest łatwo zastąpić, lub dokonania wielu ustaleń dotyczących outsourcingu z tym samym dostawcą usług chmury obliczeniowej; oceniając ryzyko koncentracji, zakład (lub w stosownych przypadkach grupa) powinien wziąć pod uwagę wszystkie swoje ustalenia dotyczące outsourcingu do chmury obliczeniowej z takim dostawcą usług chmury obliczeniowej.

32. Ocenę ryzyka należy przeprowadzić przed rozpoczęciem outsourcingu do chmury obliczeniowej. Jeżeli zakład dowie się o istotnych niedociągnięciach lub istotnych zmianach w zakresie świadczonych usług lub w sytuacji dostawcy usług chmury obliczeniowej, powinien niezwłocznie dokonać przeglądu oceny ryzyka lub ponownie ją przeprowadzić. W przypadku odnowienia ustalenia dotyczącego outsourcingu do chmury obliczeniowej odnośnie do jej treści i zakresu (np. rozszerzenie zakresu lub włączenie do zakresu krytycznych lub istotnych funkcji operacyjnych, które wcześniej nie były objęte zakresem ustalenia), należy ponownie przeprowadzić ocenę ryzyka.

Wytyczna nr 9 – Analiza due diligence dostawcy usług chmury obliczeniowej

33. W swoim procesie wyboru i oceny zakład powinien zapewnić, aby dostawca usług chmury obliczeniowej spełniał kryteria określone w przyjętej przez zakład pisemnej polityce outsourcingu.

34. Analizę due diligence dostawcy usług chmury obliczeniowej należy przeprowadzić przed zleceniem na zasadzie outsourcingu jakiejkolwiek funkcji lub czynności operacyjnej. W przypadku gdy zakład zawiera drugą umowę z dostawcą usług chmury obliczeniowej, który został już oceniony, zakład powinien określić, przyjmując podejście oparte na ocenie ryzyka, czy konieczne jest przeprowadzenie drugiej analizy due diligence. Jeżeli zakład dowie się o istotnych niedociągnięciach lub istotnych zmianach w zakresie świadczonych usług lub w sytuacji dostawcy usług chmury obliczeniowej, powinien niezwłocznie dokonać przeglądu analizy due diligence lub ponownie ją przeprowadzić.

35. W przypadku outsourcingu krytycznych lub istotnych funkcji operacyjnych do chmury obliczeniowej analiza due diligence powinna obejmować ocenę adekwatności dostawcy usług chmury obliczeniowej (np. umiejętności, infrastrukturę, sytuację ekonomiczną, status korporacyjny i regulacyjny). W stosownych przypadkach zakład może wykorzystywać do wsparcia analizy due diligence dowody, certyfikaty oparte na standardach międzynarodowych, sprawozdania z audytu uznanych stron trzecich lub sprawozdania z audytu wewnętrznego.

Wytyczna nr 10 – Wymogi dotyczące umowy

36. Odpowiednie prawa i obowiązki zakładu i dostawcy usług chmury obliczeniowej powinny być w sposób jasny rozdzielone i określone w pisemnej umowie.

37. Z zastrzeżeniem wymogów określonych w art. 274 rozporządzenia delegowanego, w przypadku zlecania na zasadzie outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych dostawcy usług chmury obliczeniowej, pisemna umowa między zakładem a dostawcą usług chmury obliczeniowej powinna określać:

a. jasny opis funkcji zlecanej na zasadzie outsourcingu (usługi chmury obliczeniowej, w tym rodzaj usług wsparcia);

b. datę rozpoczęcia i zakończenia, w stosownych przypadkach, umowy i okresy wypowiedzenia dla dostawcy usług chmury obliczeniowej oraz zakładu;

c. właściwość sądu i prawo właściwe dla umowy;

d. zobowiązania finansowe stron;

e. czy dopuszcza się podoutsourcing krytycznej lub istotnej funkcji lub czynności operacyjnej (lub ich istotnych części), a jeżeli tak – warunki, którym podlega istotny podoutsourcing (zob. wytyczna nr 13);

f. lokalizację (tj. regiony lub państwa), w których będą przechowywane i przetwarzane określone dane (lokalizacja centrów danych) oraz warunki, jakie należy spełnić, w tym wymóg dotyczący powiadamiania zakładu, jeżeli dostawca usług zaproponuje zmianę lokalizacji;

g. postanowienia dotyczące dostępności, integralności, poufności, prywatności i bezpieczeństwa odpowiednich danych, z uwzględnieniem specyfikacji zawartych w wytycznej nr 12;

h. prawo zakładu do regularnego monitorowania działalności dostawcy usług chmury obliczeniowej;

i. uzgodnione gwarantowane poziomy usług, które powinny obejmować dokładne cele ilościowe i jakościowe w celu umożliwienia terminowego monitorowania, tak aby możliwe było bezzwłoczne podjęcie odpowiednich działań naprawczych, jeżeli gwarantowane poziomy usług nie zostaną osiągnięte;

j. obowiązki sprawozdawcze dostawcy usług chmury obliczeniowej względem zakładu, w tym, w stosownych przypadkach, obowiązki dotyczące składania sprawozdań istotnych dla funkcji bezpieczeństwa zakładu oraz kluczowych funkcji, takich jak sprawozdania z funkcji audytu wewnętrznego dostawcy usług chmury obliczeniowej;

k. czy dostawca usług chmury obliczeniowej 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. wymóg, aby dostawca usług chmury obliczeniowej udzielił zakładowi, jego organom nadzoru oraz każdej innej osobie wyznaczonej przez zakład lub organy nadzoru, co następuje:

    i. pełnego dostępu do wszystkich odpowiednich lokali (siedziby firmy i centrów operacyjnych), w tym do pełnego zakresu odpowiednich urządzeń, systemów, sieci, informacji i danych wykorzystywanych do wykonywania funkcji zleconej na zasadzie outsourcingu, w tym do powiązanych informacji finansowych, informacji dotyczących personelu i audytorów zewnętrznych dostawcy usług chmury obliczeniowej („prawa dostępu”);

    ii. nieograniczonych praw w zakresie kontroli i audytu związanych z ustaleniem dotyczącym outsourcingu do chmury obliczeniowej („prawa do audytu”), aby umożliwić im monitorowanie tego ustalenia dotyczącego outsourcingu oraz zapewnić zgodność ze wszystkimi obowiązującymi wymogami prawnymi i dotyczącymi umowy;

n. postanowienia zapewniające natychmiastowy dostęp do danych stanowiących własność zakładu w przypadku niewypłacalności, restrukturyzacji i uporządkowanej likwidacji lub zaprzestania działalności dostawcy usług chmury obliczeniowej.

Wytyczna nr 11 – Prawa dostępu i prawa do audytu

38. Umowa outsourcingu do chmury obliczeniowej nie powinna ograniczać skutecznego wykonywania przez zakład praw dostępu i praw do audytu ani opcji kontroli usług chmury obliczeniowej w celu wypełnienia jego obowiązków regulacyjnych.

39. Zgodnie z sekcją 8 wytycznych EIOPA dotyczących systemu zarządzania zakład powinien korzystać z przysługujących mu praw dostępu i praw do audytu, określać częstotliwość audytu oraz obszary i usługi, które mają być przedmiotem audytu, stosując podejście oparte na ocenie ryzyka.

40. Przy określaniu częstotliwości i zakresu wykonywania praw dostępu lub praw do audytu, zakład powinien rozważyć, czy outsourcing do chmury obliczeniowej jest związany z krytyczną lub istotną funkcją lub czynnością operacyjną, charakter i zakres ryzyka oraz wpływ ustaleń dotyczących outsourcingu do chmury obliczeniowej na zakład.

41. Jeżeli korzystanie z jego praw dostępu lub praw do audytu lub stosowanie pewnych technik audytu stwarza zagrożenie dla środowiska dostawcy usług chmury obliczeniowej lub innego klienta dostawcy usług chmury obliczeniowej (na przykład wpływa na poziom usług, dostępność danych, aspekty poufności), zakład i dostawca usług chmury obliczeniowej powinni uzgodnić inne sposoby zapewnienia zakładowi podobnego poziomu pewności i usług (na przykład włączenie do określonego sprawozdania/certyfikatu sporządzanych przez dostawcę usługi chmury obliczeniowej w ramach określonych kontroli.

42. Zakłady, z zastrzeżeniem ich ostatecznej odpowiedzialności za czynności wykonywane przez ich dostawców usług chmury obliczeniowej, w celu efektywniejszego wykorzystania zasobów audytowych i zmniejszenia obciążenia organizacyjnego dostawcy usług chmury obliczeniowej i jego klientów, mogą stosować:

a. certyfikację trzeciej strony oraz sprawozdania z audytu trzeciej strony lub sprawozdania z audytu wewnętrznego udostępnione przez dostawcę usług chmury obliczeniowej;

b. zbiorcze audyty (tj. audyty przeprowadzane wspólnie z innymi klientami tego samego dostawcy usług chmury obliczeniowej) lub zbiorcze audyty przeprowadzane przez wyznaczoną przez nich stronę trzecią.

43. W przypadku outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych do chmury obliczeniowej zakłady powinny stosować metodę, o której mowa w ust. 42 lit. a), tylko wtedy, gdy:

a. zapewniają, aby zakres certyfikatu lub sprawozdania z audytu obejmował systemy (np. procesy, aplikacje, infrastrukturę, centra danych itd.) oraz mechanizmy kontroli określone przez zakład oraz sprawdzenie zgodności z odpowiednimi wymogami regulacyjnymi;

b. dokonują dokładnej regularnej oceny treści nowych certyfikatów lub sprawozdań z audytu i weryfikacji, czy certyfikaty lub sprawozdania nie są nieaktualne;

c. zapewniają objęcie kluczowych systemów i kontroli przyszłymi wersjami certyfikatu lub sprawozdania z audytu;

d. 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);

e. upewniły się, że certyfikaty są wydawane, a audyty przeprowadzone zgodnie z odpowiednimi standardami i obejmują badanie skuteczności operacyjnej kluczowych kontroli prowadzonych na miejscu;

f. 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;

g. zachowują wynikające z umowy prawo do przeprowadzania indywidualnych audytów na miejscu według własnego uznania w odniesieniu do krytycznych lub istotnych funkcji lub czynności operacyjnych zleconych na zasadzie outsourcingu do chmury obliczeniowej; prawo to powinno być wykonywane w przypadku szczególnych potrzeb, których nie można zaspokoić poprzez innego rodzaju interakcje z dostawcą usługi chmury obliczeniowej.

44. W przypadku outsourcingu krytycznych lub istotnych funkcji operacyjnych do chmury obliczeniowej zakłady powinny ocenić, czy certyfikaty i sprawozdania stron trzecich, o których mowa w ust. 42 lit. a), są odpowiednie i wystarczające do spełnienia ich obowiązków regulacyjnych oraz, stosując podejście oparte na ocenie ryzyka, nie powinny na przestrzeni czasu opierać się wyłącznie na tych sprawozdaniach i certyfikatach.

45. Przed planowaną wizytą na miejscu strona korzystająca z prawa dostępu (zakład, audytor lub strona trzecia działająca w imieniu zakładu (zakładów)) powinna odpowiednio wcześniej powiadomić o tym fakcie, chyba że wcześniejsze powiadomienie nie było możliwe ze względu na sytuację nadzwyczajną lub kryzysową. Takie powiadomienie powinno określać lokalizację i cel wizyty oraz personel, który będzie uczestniczył w wizycie.

46. Biorąc pod uwagę fakt, że rozwiązania „w chmurze" charakteryzują się wysokim stopniem złożoności technicznej, zakład powinien sprawdzić, czy personel prowadzący audyt – tj. audytorzy wewnętrzni lub grupa audytorów działających w jego imieniu lub audytorzy wyznaczeni przez dostawcę usług chmury obliczeniowej – lub, w stosownych przypadkach, personel dokonujący przeglądu certyfikatu strony trzeciej lub sprawozdań z audytu sporządzonych przez dostawcę usług posiada odpowiednie umiejętności i wiedzę do przeprowadzania odpowiednich audytów lub ocen.

Wytyczna nr 12 – Bezpieczeństwo danych i systemów

47. Zakład powinien zapewnić, aby dostawcy usług chmury obliczeniowej przestrzegali europejskich i krajowych przepisów oraz odpowiednich norm bezpieczeństwa ICT.

48. W przypadku outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych do dostawców usług chmury obliczeniowej zakład powinien dodatkowo określić szczegółowe wymogi dotyczące bezpieczeństwa informacji w umowie outsourcingu i regularnie monitorować zgodność z tymi wymogami.

49. Do celów ust. 48, w przypadku outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych do dostawców usług chmury obliczeniowej, zakład, stosując podejście oparte na ocenie ryzykai uwzględniając swoje obowiązki oraz obowiązki dostawcy usług chmury obliczeniowej, powinien:

a. uzgodnić jasny podział ról i obowiązków między dostawcą usługi chmury obliczeniowej a zakładem w odniesieniu do funkcji operacyjnych lub czynności, na które ma wpływ outsourcing do chmury obliczeniowej, które powinny być wyraźnie podzielone;

b. określić i podjąć decyzję o odpowiednim poziomie ochrony danych poufnych, ciągłości zleconych czynności oraz integralności i identyfikowalności danych i systemów w kontekście zamierzonego outsourcingu do chmury obliczeniowej;

c. uwzględnić szczególne środki, tam gdzie jest to konieczne, w odniesieniu do danych przesyłanych (ang. data in transit), danych zapisanych w pamięci (data in memory) i danych przechowywanych (data at rest), np. wykorzystanie technologii szyfrowania w połączeniu z odpowiednim zarządzaniem kluczami;

d. uwzględnić mechanizmy integracji usług chmury obliczeniowej z systemami zakładów, na przykład interfejsy programowania aplikacji i rzetelny proces zarządzania użytkownikami i dostępem;

e. zapewnić na podstawie umowy, że dostępność ruchu sieciowego i oczekiwana zdolność przepustowa spełniają rygorystyczne wymagania dotyczące ciągłości, tam gdzie ma to zastosowanie i jest wykonalne;

f. określić i podjąć decyzję w sprawie właściwych wymogów dotyczących ciągłości, zapewniających odpowiednie poziomy na każdym szczeblu łańcucha technologicznego, w stosownych przypadkach;

g. posiadać rzetelny i dobrze udokumentowany proces zarządzania incydentami, obejmujący odpowiednie obowiązki, na przykład poprzez zdefiniowanie modelu współpracy w przypadku wystąpienia rzeczywistych lub podejrzewanych incydentów;

h. przyjąć oparte na ocenie ryzyka podejście do przechowywania i przetwarzania danych w miejscu (miejscach) przechowywania i przetwarzania danych (tj. kraj lub region) oraz do kwestii bezpieczeństwa informacji;

i. monitorować spełnianie wymogów związanych ze skutecznością i efektywnością mechanizmów kontroli wdrożonych przez dostawcę usług chmury obliczeniowej, które ograniczyłyby ryzyko związane ze świadczonymi usługami.

Wytyczna nr 13 – Podoutsourcing krytycznych lub istotnych funkcji i czynności operacyjnych

50. Jeżeli zezwala się na podoutsourcing krytycznych lub istotnych funkcji operacyjnych (lub ich części), umowa outsourcingu do chmury obliczeniowej między zakładem a dostawcą usług chmury obliczeniowej powinna:

a. określać rodzaje czynności, które są wyłączone z potencjalnego podoutsourcingu;

b. wskazywać warunki, które należy spełnić w przypadku podoutsourcingu (na przykład, że podwykonawca będzie również w pełni wywiązywał się z obowiązków dostawcy usług chmury obliczeniowej); obowiązki te obejmują prawa do audytu i prawa dostępu oraz bezpieczeństwo danych i systemów;

c. wskazywać, że dostawca usług chmury obliczeniowej zachowuje pełną odpowiedzialność i nadzór nad usługami zleconymi na zasadzie podoutsourcingu;

d. zawierać zobowiązanie dostawcy usług chmury obliczeniowej do informowania zakładu o wszelkich planowanych istotnych zmianach dotyczących podwykonawców lub usług zlecanych na zasadzie podoutsourcingu, które mogą wpłynąć na zdolność dostawcy usług do wywiązania się z obowiązków wynikających z umowy outsourcingu do chmury obliczeniowej; okres powiadamiania o tych zmianach powinien umożliwiać zakładowi przynajmniej przeprowadzenie oceny ryzyka skutków proponowanych zmian przed wprowadzeniem rzeczywistej zmiany dotyczącej podwykonawcy lub usług zlecanych na zasadzie podoutsourcingu;

e. zapewnić, aby w przypadkach, gdy dostawca usług chmury obliczeniowej planuje zmiany dotyczące podwykonawcy lub usług zlecanych na zasadzie podoutsourcingu, które miałyby niekorzystny wpływ na ocenę ryzyka uzgodnionych usług, zakład miał prawo wniesienia sprzeciwu wobec takich zmian lub prawo do wypowiedzenia umowy i odstąpienia od niej.

Wytyczna nr 14 – Monitorowanie ustaleń dotyczących outsourcingu do chmury obliczeniowej i nadzór nad nimi

51. Zakład, stosując podejście oparte na ocenie ryzyka, powinien regularnie monitorować wykonywanie czynności, środki bezpieczeństwa oraz przestrzeganie przez jego dostawców usług chmury obliczeniowej uzgodnionego poziomu usług.

Główny nacisk należy położyć na zlecone na zasadzie outsourcingu do chmury obliczeniowej krytyczne i istotne funkcje operacyjne.

52. W tym celu zakład powinien ustanowić mechanizmy monitorowania i nadzoru, które powinny uwzględniać, o ile jest to wykonalne i właściwe, fakt podoutsourcingu krytycznych lub istotnych funkcji operacyjnych lub ich części.

53. Organ administrujący, zarządzający lub nadzorczy powinien być okresowo informowany o ryzykach zidentyfikowanych w ramach outsourcingu do chmury obliczeniowej krytycznych lub istotnych funkcji lub czynności operacyjnych.

54. Aby zapewnić odpowiednie monitorowanie swoich ustaleń dotyczących outsourcingu do chmury obliczeniowej i nadzór nad nimi, zakład powinien posiadać wystarczające zasoby o odpowiednich umiejętnościach i wiedzy, aby monitorować usługi zlecone na zasadzie outsourcingu do chmury obliczeniowej. Personel zakładu odpowiedzialny za te działania powinien posiadać zarówno wiedzę z zakresu ICT, jak i wiedzę biznesową, jeśli uzna to za konieczne.

Wytyczna nr 15 – Prawa do rozwiązania umowy i strategie wyjścia

55. W przypadku zlecania na zasadzie outsourcingu do chmury obliczeniowej krytycznych lub istotnych funkcji lub czynności operacyjnych, w ramach umowy outsourcingu do chmury obliczeniowej zakład powinien jasno określić klauzulę dotyczącą strategii wyjścia, zapewniającą mu możliwość rozwiązania umowy w razie potrzeby. Rozwiązanie umowy powinno być możliwe bez uszczerbku dla ciągłości i jakości świadczonych przez niego usług na rzecz ubezpieczających. W tym celu zakład powinien:

a. opracować plany wyjścia, które są kompleksowe, oparte na usługach, udokumentowane i odpowiednio przetestowane (np. poprzez przeprowadzenie analizy potencjalnych kosztów, skutków, zasobów i konsekwencji czasowych różnych potencjalnych wariantów wyjścia);

b. określić alternatywne rozwiązania i opracować odpowiednie i wykonalne plany przejścia, aby umożliwić zakładowi usunięcie i przeniesienie dotychczasowych czynności i danych od dostawcy usług chmury obliczeniowej do innych dostawców usług lub z powrotem do zakładu; rozwiązania te należy określić w odniesieniu do wyzwań, które mogą pojawić się ze względu na lokalizację danych, przedsiębiorąc niezbędne środki w celu zapewnienia ciągłości działania w fazie przejściowej;

c. zapewnić, aby dostawca usług chmury obliczeniowej odpowiednio wspierał zakład podczas przenoszenia powierzonych mu danych, systemów lub aplikacji do innego dostawcy usług lub bezpośrednio do zakładu;

d. uzgodnić z dostawcą usług chmury obliczeniowej, że po przeniesieniu do zakładu jego dane zostaną całkowicie i bezpiecznie usunięte przez dostawcę usług chmury obliczeniowej we wszystkich regionach.

56. Opracowując strategie wyjścia, zakład powinien uwzględnić:

a. zdefiniowanie celów strategii wyjścia;

b. zdefiniowanie zdarzeń powodujących (np. kluczowych wskaźników ryzyka informujących o niedopuszczalnym poziomie usług), które mogłyby uruchomić strategię wyjścia;

c. przeprowadzenie analizy wpływu na działalność współmierną do czynności zleconych na zasadzie outsourcingu w celu określenia, jakie zasoby ludzkie i materialne byłyby wymagane do wdrożenia planu wyjścia i jak wiele czasu zajęłoby wdrożenie takiego planu;

d. przydzielenie ról i obowiązków w zakresie zarządzania planami wyjścia i działaniami związanymi z przeniesieniem;

e. określenie kryteriów dotyczących pomyślnego przeniesienia.

Wytyczna nr 16 – Sprawowanie nadzoru nad ustaleniami dotyczącymi outsourcingu do chmury obliczeniowej przez organ nadzoru

57. Organy nadzoru powinny przeprowadzić analizę skutków wynikających z ustaleń zakładu dotyczących outsourcingu do chmury obliczeniowej w ramach prowadzonego przez nie procesu nadzoru. Analiza skutków powinna obejmować przede wszystkim ustalenia dotyczące outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych.

58. Organy nadzoru powinny uwzględnić następujące ryzyka w ramach nadzoru nad ustaleniami zakładów dotyczącymi outsourcingu do chmury obliczeniowej:

a. ryzyko związane z ICT;

b. inne ryzyka operacyjne (w tym ryzyko prawne i ryzyko braku zgodności, ryzyko outsourcingu i ryzyko związane z zarządzaniem przez osoby trzecie);

c. ryzyko utraty reputacji;

d. ryzyko koncentracji, w tym na poziomie kraju/sektora.

59. W ramach swojej oceny organy nadzoru powinny uwzględnić następujące aspekty, stosując podejście oparte na ocenie ryzyka:

a. adekwatność i skuteczność procesów zarządzania i procesów operacyjnych zakładu związanych z zatwierdzaniem, wdrażaniem, monitorowaniem i odnawianiem ustaleń dotyczących outsourcingu do chmury obliczeniowej i zarządzaniem nimi;

b. czy zakład posiada wystarczające zasoby o odpowiednich umiejętnościach i wiedzy do monitorowania usług zlecanych na zasadzie outsourcingu do chmury obliczeniowej;

c. czy zakład identyfikuje wszystkie rodzaje ryzyka wymienione w niniejszych wytycznych i zarządza nimi.

60. W przypadku grup organ sprawujący nadzór nad grupą powinien dopilnować, aby skutki outsourcingu krytycznych lub istotnych funkcji lub czynności operacyjnych do chmury obliczeniowej były odzwierciedlone w ocenie ryzyka w ramach nadzoru nad grupą, z uwzględnieniem wymogów wymienionych w ust. 58-59 oraz indywidualnej charakterystyki zarządzania i działalności grupy.

61. Jeżeli outsourcing krytycznych lub istotnych funkcji lub czynności operacyjnych do chmury obliczeniowej dotyczy więcej niż jednego zakładu w różnych państwach członkowskich i jest zarządzane centralnie przez spółkę dominującą lub przez spółkę zależną należącą do grupy (na przykład zakład lub spółkę usługową należącą do grupy, taką jak dostawca ICT grupy), organ sprawujący nadzór nad grupą lub właściwe organy nadzoru nad zakładami, których outsourcing do chmury obliczeniowej dotyczy, powinny omówić, w stosownych przypadkach, wpływ outsourcingu do chmury obliczeniowej na profil ryzyka grupy w ramach kolegium organów nadzoru.

62. W przypadku stwierdzenia zastrzeżeń, które prowadzą do wniosku, że zakład nie posiada już solidnych zasad zarządzania lub nie spełnia wymogów regulacyjnych, organy nadzoru powinny podjąć odpowiednie działania, które mogą obejmować np. nałożenie na zakład wymogu usprawnienia zarządzania, ograniczenie zakresu funkcji

zlecanych na zasadzie outsourcingu lub zażądanie wycofania się z jednego ustalenia dotyczącego outsourcingu lub większej liczby takich ustaleń. W szczególności, biorąc pod uwagę potrzebę działania zakładu w sposób ciągły, anulowanie umów może być wymagane w sytuacji, gdy nadzoru nad wymogami regulacyjnymi i ich egzekwowania nie można by zapewnić za pomocą innych środków.

Zasady dotyczące zgodności z przepisami i sprawozdawczości

63. Niniejszy dokument zawiera wytyczne wydane zgodnie z art. 16 rozporządzenia (UE) nr 1094/2010. Zgodnie z art. 16 ust. 3 tego rozporządzenia właściwe organy i instytucje finansowe dokładają wszelkich starań, aby zastosować się do wytycznych i zaleceń.

64. Właściwe organy, które stosują się lub zamierzają zastosować się do niniejszych wytycznych, powinny włączyć je w odpowiedni sposób do swoich ram regulacyjnych lub nadzorczych.

65. Właściwe organy muszą poinformować EIOPA, czy stosują się lub zamierzają zastosować się do niniejszych wytycznych, podając powody niezastosowania się do nich, w terminie dwóch miesięcy od daty publikacji ich przetłumaczonych wersji.

66. W przypadku braku odpowiedzi w powyższym terminie właściwe organy zostaną uznane za niestosujące się do wymogów sprawozdawczości i zostanie to zgłoszone.

Postanowienie końcowe dotyczące przeglądu

67. Niniejsze wytyczne będą poddawane przeglądowi przez EIOPA.