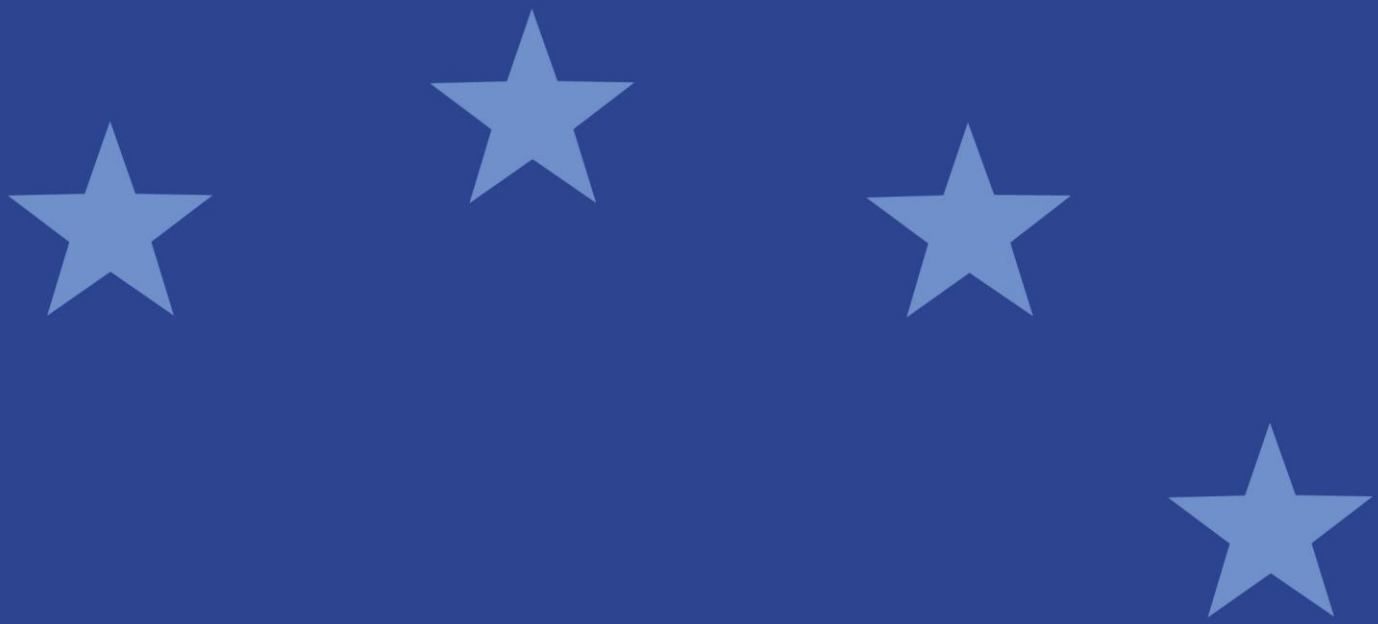
esma European Securities and Markets Authority

Wytyczne

dotyczące outsourcingu do dostawców usług chmury



10/05/2021 | ESMA50-164-4285 PL

Spis treści

I. Zakres stosowania

Kto?

1. Niniejsze wytyczne mają zastosowanie do właściwych organów oraz (i) zarządzających alternatywnymi funduszami inwestycyjnymi (ZAFI) i depozytariuszy alternatywnych funduszy inwestycyjnych (AFI), (ii) przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS), spółek zarządzających i depozytariuszy UCITS oraz spółek inwestycyjnych, które nie wyznaczyły spółki zarządzającej posiadającej zezwolenie na działalność zgodnie z dyrektywą w sprawie UCITS, (iii) kontrahentów centralnych (CCP), w tym CCP Tier II z państw trzecich, którzy spełniają odpowiednie wymogi przewidziane w rozporządzeniu w sprawie infrastruktury rynku europejskiego (EMIR), (iv) repozytoriów transakcji, (v) firm inwestycyjnych i instytucji kredytowych świadczących usługi inwestycyjne i prowadzących działalność inwestycyjną, dostawców usług w zakresie udostępniania informacji i operatorów rynku prowadzących system obrotu, (vi) centralnych depozytów papierów wartościowych, (vii) agencji ratingowych, (viii) repozytoriów sekurytyzacji oraz (ix) administratorów kluczowych wskaźników referencyjnych.

2. ESMA uwzględni niniejsze wytyczne również przy ocenie stopnia, w jakim CCP Tier II z państw trzecich spełniają odpowiednie wymogi EMIR, spełniając jednocześnie porównywalne wymogi w państwie trzecim zgodnie z art. 25 ust. 2b lit. a) EMIR.

Co?

3. Niniejsze wytyczne mają zastosowanie w odniesieniu do następujących przepisów:

   a) art. 15, 18, 20 i art. 21 ust. 8 dyrektywy w sprawie ZAFI; art. 13, 22, 38, 39, 40, 44, 45, art. 57 ust. 1 lit. d), art. 57 ust. 2 i 3, art. 58, 75, 76, 77, 79, 81, 82 i 98 rozporządzenia delegowanego Komisji (UE) 2013/231;
   b) art. 12 ust. 1 lit. a), art. 13, art. 14 ust. 1 lit. c), art. 22, 22a, art. 23 ust. 2, art. 30 i 31 dyrektywy w sprawie UCITS; art. 4 ust. 1–3 i 5, art. 5 ust. 2, art. 7, 9, art. 23 ust. 4, art. 32, 38, 39 i 40 dyrektywy Komisji 2010/43/UE; art. 2 ust. 2 lit. j), art. 3 ust. 1, art. 13 ust. 2, art. 15, 16 i 22 rozporządzenia delegowanego Komisji (UE) 2016/438;
   c) art. 25, art. 26 ust. 1, 3 i 6, art. 34, 35 i 78–81 EMIR; art. 5 i 12 rozporządzenia w sprawie transakcji finansowanych z użyciem papierów wartościowych (SFTR); art. 3 ust. lit. f), art. 3 ust. 2, art. 4, art. 7 ust. 2 lit. d) i f), art. 9 i 17 rozporządzenia delegowanego Komisji (UE) nr 150/2013; art. 16 i 21 rozporządzenia delegowanego Komisji (UE) nr 150/2013; art. 16 i 21 rozporządzenia delegowanego Komisji (UE) 2019/359;

d) art. 16 ust. 2, 4 i 5, art. 18 ust. 1, art. 19 ust. 3 lit. a), art. 47 ust. 1 lit. b) i c), art. 48 ust. 1, art. 64 ust. 4, art. 65 ust. 5 i art. 66 ust. 31 MiFID II; art. 21 ust. 1–3, art. 23, art. 29 ust. 5, art. 30, 31 i 32 rozporządzenia delegowanego Komisji (UE) 2017/565; art. 6, 15 i art. 16 ust. 6 rozporządzenia delegowanego Komisji (UE) 2017/584; art. 6, 7, 8 i 9 rozporządzenia delegowanego Komisji (UE) 2017/571;
e) art. 22, 26, 30, 42, 44 i 45 rozporządzenia w sprawie rozrachunku papierów wartościowych i centralnych depozytów papierów wartościowych (CSDR) oraz art. 33, 47, art. 50 ust. 1, art. 57 ust. 2 lit. i), art. 66, 68, 75, 76, 78 i 80 rozporządzenia delegowanego Komisji (UE) 2017/392;
f) art. 9 i załącznika I, sekcji A pkt 4 i 8 oraz pkt 17 załącznika II do rozporządzenia w sprawie agencji ratingowych (CRA), a także art. 11 i 25 rozporządzenia delegowanego Komisji (UE) 2012/449;
g) art. 10 ust. 2 rozporządzenia w sprawie ustanowienia ogólnych ram dla sekurytyzacji oraz utworzenia szczególnych ram dla prostych, przejrzystych i standardowych sekurytyzacji (SECR);
h) art. 6 ust. 3 i art. 10 rozporządzenia o wskaźnikach referencyjnych i pkt 7 załącznika I do rozporządzenia delegowanego Komisji (UE) 2018/1646.

Kiedy?

4. Niniejsze wytyczne mają zastosowanie od dnia 31 lipca 2021 r. do wszystkich umów dotyczących outsourcingu do chmury zawartych, odnowionych lub zmienionych tego dnia lub po tym dniu. Firmy powinny dokonać przeglądu i odpowiednio zmienić istniejące umowy dotyczące outsourcingu do chmury w celu zapewnienia, aby uwzględniały one niniejsze wytyczne do dnia 31 grudnia 2022 r. Jeżeli przegląd umów dotyczących outsourcingu do chmury krytycznych lub istotnych funkcji nie zakończy się do 31 grudnia 2022 r., firmy powinny powiadomić właściwy organ o tym fakcie, w tym o działaniach, które planuje się w celu zakończenia przeglądu lub potencjalnej strategii wyjścia z chmury.

II. Odniesienia do przepisów prawa, skróty i definicje

Odniesienia do przepisów prawa

rozporządzenie w sprawie ustanowienia ESMA	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1095/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/77/WE[2].
dyrektywa w sprawie ZAFI	Dyrektywa Parlamentu Europejskiego i Rady 2011/61/UE z dnia 8 czerwca 2011 r. w sprawie zarządzających

[1] Od dnia 1 stycznia 2022 r. odniesienia do art. 64 ust. 4, art. 65 ust. 5 i art. 66 ust. 3 MiFID II należy rozumieć jako odniesienia do art. 27g ust. 4, art. 27h ust. 5 i art. 27i ust.3 MiFIR.
[2] Dz.U. L 331 z 15.12.2010, s. 84.

	alternatywnymi funduszami inwestycyjnymi i zmiany dyrektyw 2003/41/WE i 2009/65/WE oraz rozporządzeń (WE) nr 1060/2009 i (UE) nr 1095/2010[3]
rozporządzenie delegowane Komisji (UE) 2013/231	Rozporządzenie delegowane Komisji (UE) 2013/231 z dnia 19 grudnia 2012 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2011/61/UE w odniesieniu do zwolnień, ogólnych warunków dotyczących prowadzenia działalności, depozytariuszy, dźwigni finansowej, przejrzystości i nadzoru[4]
dyrektywa w sprawie UCITS	Dyrektywa Parlamentu Europejskiego i Rady 2009/65/WE z dnia 13 lipca 2009 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS)[5]
dyrektywa Komisji 2010/43/UE	Dyrektywa Komisji 2010/43/UE z dnia 1 lipca 2010 r. w sprawie wykonania dyrektywy Parlamentu Europejskiego i Rady 2009/65/WE w zakresie wymogów organizacyjnych, konfliktów interesów, prowadzenia działalności, zarządzania ryzykiem i treści umowy pomiędzy depozytariuszem a spółką zarządzającą[6]
rozporządzenie delegowane Komisji (UE) 2016/438	Rozporządzenie delegowane Komisji (UE) 2016/438 z dnia 17 grudnia 2015 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2009/65/WE w odniesieniu do obowiązków depozytariuszy[7]
rozporządzenie w sprawie infrastruktury rynku europejskiego (EMIR)	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji[8]
SFTR	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2365 z dnia 25 listopada 2015 r. w sprawie przejrzystości transakcji finansowanych z użyciem papierów wartościowych i ponownego wykorzystania oraz zmiany rozporządzenia (UE) nr 648/2012[9]
rozporządzenie delegowane Komisji (UE) nr 153/2013	Rozporządzenie delegowane Komisji (UE) nr 153/2013 z dnia 19 grudnia 2012 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 w

[3] Dz.U. L 174 z 1.7.2011, s. 1.
[4] Dz.U. L 83 z 22.3.2013, s. 1.
[5] Dz.U. L 302 z 17.11.2009, s. 32.
[6] Dz.U. L 176 z 10.7.2010, s. 42.
[7] Dz.U. L 78 z 24.3.2016, s. 11.
[8] Dz.U. L 201 z 27.7.2012, s. 1.
[9] Dz.U. L 337 z 23.12.2015, s. 1.

	odniesieniu do regulacyjnych standardów technicznych dotyczących wymogów obowiązujących kontrahentów centralnych[10]
rozporządzenie delegowane Komisji (UE) nr 150/2013	Rozporządzenie delegowane Komisji(UE) nr 150/2013 z dnia 19 grudnia 2012 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji w odniesieniu do regulacyjnych standardów technicznych określających minimalny poziom szczegółowości informacji podlegających zgłoszeniu repozytoriom transakcji[11]
rozporządzenie delegowane Komisji (UE) 2019/359	Rozporządzenie delegowane Komisji (UE) 2019/359 z dnia 13 grudnia 2018 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2365 w odniesieniu do regulacyjnych standardów technicznych określających szczegóły dotyczące wniosku o rejestrację i o rozszerzenie rejestracji jako repozytorium transakcji[12]
MiFID II	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[13]
MiFIR	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (EU) nr 648/2012 ([14])
rozporządzenie delegowane Komisji (UE) nr 2017/565	Rozporządzenie delegowane Komisji (UE) 2017/565 z dnia 25 kwietnia 2016 r. uzupełniające 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[15]
rozporządzenie delegowane Komisji (UE) nr 2017/584	Rozporządzenie delegowane Komisji (UE) nr 2017/584 z dnia 14 lipca 2016 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do regulacyjnych standardów technicznych określających wymogi organizacyjne w zakresie systemów obrotu[16]

[10] Dz.U. L 52 z 23.2.2013, s. 41.
[11] Dz.U. L 52 z 23.2.2013, s. 25.
[12] Dz.U. L 81 z 22.3.2019, s. 45.
[13] Dz.U. L 173 z 12.6.2014, s. 349.
[14] Dz.U. L 173 z 12.6.2014, s. 84.
[15] Dz.U. L 87 z 31.3.2017, s. 1.
[16] Dz.U. L 87 z 31.3.2017, s. 350.

rozporządzenie delegowane Komisji (UE) nr 2017/571	Rozporządzenie delegowane Komisji (UE) 2017/571 z dnia 2 czerwca 2016 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do regulacyjnych standardów technicznych dotyczących zezwoleń, wymogów organizacyjnych i publikacji transakcji dla dostawców usług w zakresie udostępniania informacji[17]
rozporządzenie w sprawie rozrachunku papierów wartościowych i centralnych depozytów papierów wartościowych (CSDR)	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012[18]
rozporządzenie delegowane Komisji (UE) 2017/392	Rozporządzenie delegowane Komisji (UE) 2017/392 z dnia 11 listopada 2016 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 w odniesieniu do regulacyjnych standardów technicznych dotyczących wymogów w zakresie udzielania zezwoleń oraz wymogów nadzorczych i operacyjnych dla centralnych depozytów papierów wartościowych[19]
rozporządzenie w sprawie agencji ratingowych (CRA)	Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1060/2009 z dnia 16 września 2009 r. w sprawie agencji ratingowych[20]
rozporządzenie delegowane Komisji (UE) 2012/449	Rozporządzenie delegowane Komisji (UE) nr 449/2012 z dnia 21 marca 2012 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1060/2009 w odniesieniu do regulacyjnych standardów technicznych dotyczących informacji do celów rejestracji i certyfikacji agencji ratingowych[21]
rozporządzenie w sprawie ustanowienia ogólnych ram dla sekurytyzacji oraz utworzenia szczególnych ram dla prostych, przejrzystych i standardowych sekurytyzacji (SECR)	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2402 z dnia 12 grudnia 2017 r. w sprawie ustanowienia ogólnych ram sekurytyzacji oraz utworzenia szczególnych ram dla prostych, przejrzystych i standardowych sekurytyzacji, a także zmieniające dyrektywy 2009/65/WE, 2009/138/WE i 2011/61/UE oraz rozporządzenia (WE) nr 1060/2009 i (UE) nr 648/2012[22]

[17] Dz.U. L 87 z 31.3.2017, s. 126.
[18] Dz.U. L 257 z 28.8.2014, s. 1.
[19] Dz.U. L 65 z 10.3.2017, s. 48.
[20] Dz.U. L 302 z 17.11.2009, s. 1.
[21] Dz.U. L 140 z 30.5.2012, s. 32.
[22] Dz.U. L 347 z 28.12.2017, s. 35.

rozporządzenie o wskaźnikach referencyjnych	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1011 z dnia 8 czerwca 2016 r. w sprawie indeksów stosowanych jako wskaźniki referencyjne w instrumentach finansowych i umowach finansowych lub do pomiaru wyników funduszy inwestycyjnych i zmieniające dyrektywy 2008/48/WE i 2014/17/UE oraz rozporządzenie (UE) nr 596/2014[23]
rozporządzenie delegowane Komisji (UE) 2018/1646	Rozporządzenie delegowane Komisji (UE) 2018/1646 z dnia 13 lipca 2018 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1011 w odniesieniu do regulacyjnych standardów technicznych dotyczących informacji, które należy zawrzeć we wniosku o udzielenie zezwolenia i we wniosku o rejestrację[24]
RODO	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[25]

Skróty

CSP	Dostawca usług chmury
ESMA	Europejski Urząd Nadzoru Giełd i Papierów Wartościowych
UE	Unia Europejska

Definicje

funkcja	oznacza wszelkie procesy, usługi lub działania;
funkcja krytyczna lub istotna	oznacza każdą funkcję, której niewłaściwe wykonanie lub brak wykonania mogłyby poważnie zagrozić: a) spełnianiu przez firmę jej obowiązków wynikających z mających zastosowanie przepisów; b) wynikom finansowym firmy; lub c) solidności lub ciągłości świadczenia głównych usług i prowadzenia głównej działalności firmy;
usługi w chmurze	oznaczają usługi świadczone z wykorzystaniem chmury obliczeniowej;

[23] Dz.U. L 171 z 29.6.2016, s. 1.
[24] Dz.U. L 274 z 5.11.2018, s. 43.
[25] Dz.U. L 119 z 4.5.2016, s. 1–88.

chmura obliczeniowa lub chmura[26]	oznacza paradygmat umożliwiający dostęp sieci do skalowalnego i elastycznego zbioru współdzielonych zasobów fizycznych lub wirtualnych (np. serwerów, systemów operacyjnych, sieci, oprogramowania, aplikacji i sprzętu do magazynowania danych) z samoobsługowym dostępem do zasobów i administrowaniem na żądanie;
dostawca usług chmury	oznacza osobę trzecią świadczącą usługi w chmurze w ramach umowy dotyczącej outsourcingu do chmury;
umowa dotycząca outsourcingu do chmury	oznacza dowolną umowę, w tym ustalenia dotyczące delegowania, między: (i) firmą a dostawcą usług chmury, na mocy których dostawca usług chmury pełni funkcję, która w przeciwnym razie byłaby wykonywana przez samą firmę; lub (ii) firmą a stroną trzecią, która nie jest dostawcą usług chmury, lecz która w znacznym stopniu polega na dostawcy usług chmury w zakresie pełnienia funkcji, która w przeciwnym razie byłaby wykonywana przez samą firmę. W takim przypadku odniesienie do „dostawcy usługchmury" w niniejszych wytycznych należy rozumieć jako odniesienie do takiej osoby trzeciej.
podoutsourcing	oznacza sytuację, w której dostawca usługchmury przekazuje dalej funkcję zleconą na zasadzie outsourcingu (lub jej część) innemu usługodawcy na podstawie umowy outsourcingu;
model wdrażania chmury obliczeniowej	oznacza sposób, w jaki chmura może być zorganizowana na zasadzie kontroli i współdzielenia zasobów fizycznych lub wirtualnych. Modele wdrażania chmury obliczeniowej obejmują chmury społecznościowe [27], hybrydowe [28], prywatne[29] i publiczne[30];

[26] „Chmura obliczeniowa" często funkcjonuje jako skrót „chmura". W celu ułatwienia odniesienia w dalszej części niniejszego dokumentu stosuje się pojęcie „chmury".
[27] Model wdrażania chmury obliczeniowej, w którym usługi w chmurze wspierają wyłącznie konkretną grupę klientów korzystających z usług w chmurze, których łączą te same wymogi i relacje, i są przez nich współdzielone, oraz w którym zasoby kontrolowane są przez co najmniej jednego członka tej grupy.
[28] Model wdrażania chmury obliczeniowej, w ramach którego wykorzystuje się co najmniej dwa różne modele wdrażania chmury obliczeniowej.
[29] Model wdrażania chmury obliczeniowej, w którym usługi w chmurze stosowane są wyłącznie przez jednego klienta korzystającego z usług w chmurze, a zasoby kontrolowane są przez tego klienta.
[30] Model wdrażania chmury obliczeniowej, w którym usługi w chmurze są potencjalnie dostępne dla każdego klienta korzystającego z usług w chmurze, a zasoby kontrolowane są przez dostawcę usług w chmurze.

firmy

a) zarządzający alternatywnymi funduszami inwestycyjnymi lub „ZAFI” w rozumieniu art. 4 ust. 1 lit. b) dyrektywy w sprawie ZAFI oraz depozytariusze, o których mowa w art. 21 ust. 3 dyrektywy w sprawie ZAFI („depozytariusze alternatywnych funduszy inwestycyjnych (AFI)”);

b) spółki zarządzające w rozumieniu art. 2 ust. 1 lit. b) dyrektywy w sprawie UCITS („spółki zarządzające UCITS”) i depozytariusze w rozumieniu art. 2 ust. 1 lit. a) dyrektywy w sprawie UCITS („depozytariusze UCITS”);

c) kontrahenci centralni określeni w art. 2 ust. 1 EMIR oraz CCP Tier II z państw trzecich w rozumieniu art. 25 ust. 2a EMIR, którzy spełniają odpowiednie wymogi EMIR zgodnie z art. 25 ust. 2b lit. a) EMIR;

d) repozytoria transakcji określone w art. 2 ust. 2 EMIR i w art. 3 ust. 1 rozporządzenia w sprawie transakcji finansowanych z użyciem papierów wartościowych (SFTR);

e) firmy inwestycyjne określone w art. 4 ust. 1 pkt 1 MiFID II i instytucje kredytowe określone w art. 4 ust. 1 pkt 27 MiFID II świadczące usługi inwestycyjne oraz prowadzące działalność inwestycyjną w rozumieniu art. 4 ust. 1 pkt 2 MiFID II;

f) dostawcy usług w zakresie udostępniania informacji określeni w art. 4 ust. 1 pkt 63 MiFID II[31];

[31] Od dnia 1 stycznia 2022 r. odniesienia do niniejszego przepisu należy rozumieć jako odniesienia do art. 2 ust. 1 pkt 36 lit. a) MiFIR.

g) operatorzy rynku prowadzący system obrotu w rozumieniu art. 4 ust. 1 pkt 24 MiFID II;

h) centralne depozyty papierów wartościowych określone w art. 2 ust. 1 pkt 1 rozporządzenia w sprawie rozrachunku papierów wartościowych i centralnych depozytów papierów wartościowych (CSDR);

i) agencje ratingowe określone w art. 3 ust. 1 lit. b) dyrektywy w sprawie agencji ratingowych (CRA);

j) repozytoria sekurytyzacji określone w art. 2 ust. 23 rozporządzenia w sprawie ustanowienia ogólnych ram dla sekurytyzacji oraz utworzenia szczególnych ram dla prostych, przejrzystych i standardowych sekurytyzacji (SECR);

k) administratorzy kluczowych wskaźników referencyjnych określeni w art. 3 ust. 1 pkt 25 rozporządzenia o wskaźnikach referencyjnych.

III. Cel

5. Niniejsze wytyczne są oparte na art. 16 ust. 1 rozporządzenia w sprawie ustanowienia ESMA. Cele niniejszych wytycznych obejmują ustanowienie spójnych, wydajnych i skutecznych praktyk nadzorczych w ramach Europejskiego Systemu Nadzoru Finansowego (ESNF) oraz zapewnienie wspólnego, jednolitego i spójnego stosowania wymogów, o których mowa w sekcji 1.1 pod nagłówkiem „Co?”, w przypadku gdy firmy zlecają wykonanie zadań dostawcom usługchmury. Niniejsze wytyczne mają w szczególności pomóc firmom i właściwym organom w identyfikowaniu, uwzględnianiu i monitorowaniu zagrożeń i wyzwań wynikających z umów dotyczących outsourcingu do chmury – od podejmowania decyzji w sprawie outsourcingu, wyboru dostawcy usług chmury, monitorowania działań zleconych na zasadzie outsourcingu po zapewnienie strategii wyjścia.

IV. Obowiązki w zakresie zgodności i powiadamiania

Status wytycznych

6. Zgodnie z art. 16 ust. 3 rozporządzenia w sprawie ustanowienia ESMA właściwe organy i firmy dokładają wszelkich starań, aby zastosować się do niniejszych wytycznych.

7. Właściwe organy, do których odnoszą się niniejsze wytyczne, powinny zastosować się do nich poprzez włączenie ich do swoich odpowiednich krajowych ram prawnych lub nadzorczych, również w przypadku, gdy poszczególne wytyczne są skierowane głównie do firm. W takim przypadku właściwe organy powinny w ramach sprawowanego nadzoru zadbać o to, aby firmy przestrzegały wytycznych.

8. W ramach sprawowanego bezpośredniego nadzoru bieżącego ESMA oceni stosowanie niniejszych wytycznych przez agencje ratingowe, repozytoria transakcji, repozytoria sekurytyzacji, CCP Tier II z państw trzecich oraz – od dnia 1 stycznia 2022 r. – dostawców usług w zakresie udostępniania informacji i administratorów unijnych kluczowych wskaźników referencyjnych.

Wymogi w zakresie powiadamiania

9. W terminie dwóch miesięcy od daty publikacji niniejszych wytycznych na stronie ESMA we wszystkich językach urzędowych UE właściwe organy, do których niniejsze wytyczne mają zastosowanie, muszą zawiadomić ESMA, czy (i) stosują wytyczne, (ii) nie stosują wytycznych, ale zamierzają zastosować się do nich lub (iii) nie stosują wytycznych i nie zamierzają się do nich zastosować.

10. W przypadku niezastosowania się do wytycznych właściwe organy muszą również przekazać ESMA w terminie dwóch miesięcy od daty publikacji wytycznych na stronie ESMA we wszystkich językach urzędowych UE informację o powodach niestosowania się do wytycznych. Szablon zawiadomienia jest dostępny na stronie internetowej ESMA. Po wypełnieniu szablonu należy przekazać go ESMA.

11. Firmy nie mają obowiązku zawiadamiania, czy stosują się do niniejszych wytycznych.

V. Wytyczne dotyczące outsourcingu do dostawców usług chmury

Wytyczna 1. Zarządzanie, nadzór i dokumentacja

12. Firma powinna posiadać określoną i aktualną strategię outsourcingu do chmury, która jest spójna z odpowiednimi strategiami oraz wewnętrznymi politykami i procesami firmy, w tym w odniesieniu do technologii informacyjno-komunikacyjnych, bezpieczeństwa informacji i zarządzania ryzykiem operacyjnym.

13. Firma powinna:

    a) w ramach swojej organizacji – jednoznacznie przydzielić obowiązki w zakresie dokumentowania umów dotyczących outsourcingu do chmury, zarządzania nimi i kontroli nad takimi umowami;
    b) przeznaczyć wystarczające zasoby na zapewnienie zgodności z niniejszymi wytycznymi i wszystkimi wymogami prawnymi mającymi zastosowanie do umów dotyczących outsourcingu do chmury;
    c) ustanowić funkcję nadzorczą względem outsourcingu do chmury lub wyznaczyć pracowników wyższego szczebla, którzy są bezpośrednio odpowiedzialni przed organem zarządzającym i odpowiadają za zarządzanie ryzykiem związanym z umowami dotyczącymi outsourcingu do chmury i sprawowanie nadzoru nad tym ryzykiem. Stosując się do niniejszej wytycznej firmy powinny uwzględnić charakter, skalę i złożoność swojej działalności, w tym pod względem ryzyka dla systemu finansowego oraz ryzyka nieodłącznie związanego z funkcjami zleconymi na zasadzie outsourcingu, a także upewnić się, że ich organ zarządzający posiada odpowiednie umiejętności techniczne pozwalające zrozumieć ryzyko związane z umowami dotyczącymi outsourcingu do chmury[32]. Małe i mniej złożone firmy powinny przynajmniej zapewnić jasny podział zadań i obowiązków w zakresie zarządzania umowami dotyczącymi outsourcingu do chmury i nadzoru nad nimi.

14. Firma powinna monitorować realizację działań, środki bezpieczeństwa i przestrzeganie uzgodnionych gwarantowanych poziomów usług przez swoich dostawców usług chmury. Monitorowanie to powinno opierać się na analizie ryzyka i skupiać się przede wszystkim na krytycznych lub istotnych funkcjach, które zostały zlecone na zasadzie outsourcingu.

15. Firma powinna okresowo dokonywać ponownej oceny tego, czy jej umowy dotyczące outsourcingu do chmury dotyczą funkcji krytycznej lub istotnej oraz w każdym przypadku gdy ryzyko, charakter lub skala funkcji zleconej na zasadzie outsourcingu uległy istotnej zmianie.

16. Firma powinna prowadzić zaktualizowany rejestr informacji na temat wszystkich swoich umów dotyczących outsourcingu do chmury, dokonując rozróżnienia między outsourcingiem funkcji krytycznych lub istotnych oraz innymi umowami outsourcingu. Dokonując rozróżnienia między outsourcingiem funkcji krytycznych lub istotnych a innymi umowami outsourcingu, firma powinna przedstawić krótkie podsumowanie powodów, dla których funkcja zlecona na zasadzie outsourcingu jest lub nie jest uznawana za krytyczną lub istotną. Zgodnie z prawem krajowym firma powinna również prowadzić rejestr zakończonych umów dotyczących outsourcingu do chmury przez odpowiedni okres.

[32] W przypadku firm inwestycyjnych i instytucji kredytowych zob. „Wspólne wytyczne ESMA i EUNB w sprawie oceny kwalifikacji członków organu zarządzającego i osób pełniących najważniejsze funkcje wydanych na mocy dyrektyw 2013/36/UE oraz 2014/65/UE” (EBA/GL/2017/12).

17. W przypadku umów dotyczących outsourcingu do chmury dotyczących funkcji krytycznych lub istotnych rejestr powinien zawierać co najmniej następujące informacje w odniesieniu do każdej umowy dotyczącej outsourcingu do chmury:

    a) numer referencyjny;
    b) datę rozpoczęcia oraz, w stosownych przypadkach, datę odnowienia umowy, datę zakończenia lub okresy wypowiedzenia obowiązujące dostawcę usług chmury i firmę;
    c) krótki opis funkcji zleconej na zasadzie outsourcingu, w tym dane, które są zlecane na zewnątrz, oraz, czy dane te obejmują dane osobowe (np. poprzez wpisanie „tak" lub „nie" w osobnym polu danych);
    d) kategorię przypisaną przez firmę odzwierciedlającą charakter funkcji zleconej na zasadzie outsourcingu (np. funkcja technologii informacyjnej, funkcja kontroli), co powinno ułatwić identyfikację poszczególnych rodzajów umów dotyczących outsourcingu;
    e) czy funkcja zlecona na zasadzie outsourcingu wspiera działalność, w której czas odgrywa kluczową rolę;
    f) nazwę i ewentualną nazwę marki dostawcy usług do chmury, kraj rejestracji, numer ewidencyjny przedsiębiorstwa, identyfikator podmiotu prawnego (jeżeli jest dostępny), adres i inne stosowne dane kontaktowe oraz nazwę jednostki dominującej (jeżeli istnieje);
    g) prawo właściwe dla umowy dotyczącej outsourcingu do chmury oraz, w stosownych przypadkach, wybór jurysdykcji;
    h) rodzaj usług do chmury i modeli wdrażania oraz szczególny charakter danych, które mają być przechowywane, oraz lokalizacje (tj. regiony lub państwa), w których takie dane mogą być przechowywane;
    i) datę ostatniej oceny krytycznego lub istotnego charakteru funkcji zleconej na zasadzie outsourcingu oraz datę następnej planowanej oceny;
    j) datę ostatniej oceny ryzyka / ostatniego audytu dostawcy usług w chmurze wraz z krótkim podsumowaniem głównych wyników oraz datą następnej planowanej oceny ryzyka / następnego planowanego audytu;
    k) informacje na temat osoby w firmie, która zatwierdziła umowę dotyczącą outsourcingu w chmurze lub organu decyzyjnego w firmie, który zatwierdził umowę dotyczącą outsourcingu do chmury;
    l) w stosownych przypadkach nazwy podmiotów świadczących usługi podoutsourcingu (*sub-outsourcer*), którym zlecane są na zasadzie podoutsourcingu funkcje krytyczne lub istotne (lub ich istotne części), w tym kraje, w których są zarejestrowane podmioty świadczące usługi podoutsourcingu, gdzie wykonywane będą usługi podoutsourcingu oraz lokalizacje (tj. regiony lub państwa), w których przechowywane będą dane;
    m) szacunkowe roczne koszty budżetowe umowy dotyczącej outsourcingu do chmury.

18. W przypadku umów dotyczących outsourcingu do chmury odnoszących się do funkcji niekrytycznych lub nieistotnych firma powinna określić informacje, które mają być zawarte w rejestrze, w oparciu o charakter, skalę i złożoność ryzyka nieodłącznie związanego z funkcją zleconą na zasadzie outsourcingu.

Wytyczna 2. Analiza przed zawarciem umowy dotyczącej outsourcingu i analiza *due diligence*

19. Przed zawarciem jakiejkolwiek umowy dotyczącej outsourcingu do chmury firma powinna:

    a) ocenić, czy umowa dotycząca outsourcingu do chmury dotyczy krytycznej lub istotnej funkcji;
    b) zidentyfikować i ocenić wszystkie istotne ryzyka umowy dotyczącej outsourcingu do chmury;
    c) przeprowadzić odpowiednią analizę *due diligence* w odniesieniu do potencjalnego dostawcy usługchmury;
    d) zidentyfikować i ocenić konflikty interesów, do których może prowadzić outsourcing.

20. Analiza przed zawarciem umowy dotyczącej outsourcingu i analiza *due diligence* odnośnie do potencjalnego dostawcy usług chmury powinny być proporcjonalne do charakteru, skali i złożoności funkcji, którą firma zamierza zlecić na zasadzie outsourcingu oraz do ryzyka nieodłącznie związanego z tą funkcją. Powinny one obejmować co najmniej ocenę potencjalnego wpływu umowy dotyczącej outsourcingu do chmury na ryzyko operacyjne, prawne, ryzyko dla przestrzegania przepisów i ryzyko utraty reputacji firmy.

21. W przypadku gdy umowa dotycząca outsourcingu do chmury dotyczy funkcji krytycznych lub istotnych firma powinna również:

    a) ocenić każde istotne ryzyko, które może powstać w wyniku zawarcia umowy dotyczącej outsourcingu do chmury, w tym ryzyko związane z technologiami informacyjno-komunikacyjnymi, bezpieczeństwem informacji, ciągłością działania, ryzyko prawne i związane z przestrzeganiem przepisów, ryzyko utraty reputacji, ryzyko operacyjne i ewentualne ograniczenia nadzoru dla firmy, wynikające z:
        i. wybranej usługi chmury oraz proponowanych modeli wdrażania;
        ii. procesów migracji lub wdrożenia;
        iii. wrażliwości funkcji i związanych z nią danych, których zlecenie na zasadzie outsourcingu rozważa się, oraz środków bezpieczeństwa, które należałoby podjąć;
        iv. interoperacyjności systemów i aplikacji firmy i dostawcy usług chmury, mianowicie ich zdolności do wymiany informacji i wzajemnego wykorzystywania wymienianych informacji;
        v. możliwości przenoszenia danych firmy, mianowicie zdolności do łatwego przekazywania danych firmy od jednego dostawcy usług chmury do drugiego lub z powrotem do firmy;
        vi. stabilności politycznej, sytuacji w zakresie bezpieczeństwa i systemu prawnego (w tym obowiązujących przepisów dotyczących egzekwowania prawa, przepisów prawa dotyczących niewypłacalności, które miałyby zastosowanie w przypadku upadłości dostawcy usług chmury, obowiązujących przepisów o ochronie danych oraz tego, czy spełnione są

warunki przekazywania danych osobowych do państwa trzeciego na mocy RODO) w państwach (w UE lub poza nią), w których funkcje zlecone na zasadzie outsourcingu byłyby świadczone i w których dane przekazane na zasadzie outsourcingu byłyby przechowywane; w przypadku podoutsourcingu – dodatkowego ryzyka, które może powstać, jeżeli podmiot świadczący usługi podoutsourcingu ma siedzibę w państwie trzecim lub innym niż siedziba dostawcy usług do chmury oraz, w przypadku łańcucha podoutsourcingu, każdego dodatkowego ryzyka, które może powstać, w tym w związku z brakiem bezpośredniej umowy między firmą a podmiotem świadczącym usługi podoutsourcingu wykonującym funkcję zleconą na zasadzie outsourcingu;

vii. możliwej koncentracji w firmie (w tym, w stosownych przypadkach, na poziomie jej grupy), spowodowanej wieloma umowami dotyczącymi outsourcingu do chmury zawieranymi z tym samym dostawcą usług chmury, a także możliwej koncentracji w sektorze finansowym UE, spowodowanej przez wiele firm korzystających z usług tego samego dostawcy usług chmury lub niewielkiej grupy dostawców usług chmury. Dokonując oceny ryzyka koncentracji, firma powinna uwzględnić wszystkie swoje umowy dotyczące outsourcingu do chmury (oraz, w stosownych przypadkach, umowy dotyczące outsourcingu do chmury na poziomie swojej grupy) zawierane z tym dostawcą usług chmury;

b) uwzględnić oczekiwane korzyści i koszty umowy dotyczącej outsourcingu do chmury, w tym zważyć wszelkie istotne ryzyka, które można ograniczyć lub którymi można lepiej zarządzać względem wszelkich znaczących ryzyk, które mogą powstać w wyniku umowy dotyczącej outsourcingu do chmury;

22. W przypadku outsourcingu funkcji krytycznych lub istotnych analiza *due diligence* powinna obejmować ocenę kwalifikacji dostawcy usług chmury. Dokonując oceny kwalifikacji dostawcy usług chmury, firma powinna zapewnić, aby dostawca usług chmury posiadał reputację biznesową, umiejętności, zasoby (w tym zasoby ludzkie, informatyczne i finansowe), strukturę organizacyjną oraz, w stosownych przypadkach, posiadał odpowiednie zezwolenie(-a) lub został zarejestrowany, by wykonywać krytyczną lub istotną funkcję w sposób wiarygodny i profesjonalny i by wywiązać się ze swoich zobowiązań w okresie obowiązywania umowy dotyczącej outsourcingu do chmury. Dodatkowe czynniki, które należy uwzględnić podczas analizy *due diligence* dotyczącej dostawcy usług chmury obejmują między innymi:

a) zarządzanie bezpieczeństwem informacji, w szczególności ochronę danych osobowych, poufnych lub w inny sposób wrażliwych;
b) wsparcie w zakresie świadczonych usług, w tym plany wsparcia i kontakty, oraz procesy zarządzania incydentami;
c) plany ciągłości działania i przywrócenia gotowości do pracy po katastrofie;

23. W stosownych przypadkach i w celu wsparcia analizy *due diligence* firma może również korzystać z certyfikacji opartych na normach międzynarodowych oraz sprawozdaniach z audytu zewnętrznego lub wewnętrznego.

24. Jeżeli firma dowie się o istotnych niedociągnięciach lub istotnych zmianach w zakresie świadczonych usług lub w sytuacji dostawcy usług chmury analiza przed zawarciem umowy outsourcingu i analiza *due diligence* dotyczące dostawcy usług chmury powinny zostać niezwłocznie poddane przeglądowi lub, w razie potrzeby, przeprowadzone ponownie.

25. W przypadku gdy firma zawiera nową umowę lub odnawia istniejącą umowę z dostawcą usług chmury, który został już oceniony, firma powinna określić, przyjmując podejście oparte na analizie ryzyka, czy konieczne jest przeprowadzenie nowej analizy *due diligence*.

Wytyczna 3. Kluczowe elementy umowy

26. Odpowiednie prawa i obowiązki firmy i dostawcy usług chmury powinny być jasno określone w pisemnej umowie.

27. Pisemna umowa powinna wyraźnie umożliwiać firmie rozwiązanie umowy, jeżeli jest to konieczne.

28. W przypadku outsourcingu funkcji krytycznych lub istotnych pisemna umowa powinna zawierać co najmniej:

    a) jasny opis funkcji zleconej na zasadzie outsourcingu;

    b) datę rozpoczęcia i zakończenia, w stosownych przypadkach, umowy i okresy wypowiedzenia dla dostawcy usług chmury oraz firmy;

    c) prawo właściwe dla umowy oraz, w stosownych przypadkach, wybór jurysdykcji;

    d) zobowiązania finansowe firmy i dostawcy usług chmury;

    e) informację, czy podoutsourcing jest dozwolony, a jeżeli tak, na jakich warunkach, z uwzględnieniem wytycznej 7;

    f) lokalizacje (tj. regiony lub państwa), w których wykonywana będzie funkcja zlecona na zasadzie outsourcingu i gdzie będą przechowywane i przetwarzane dane oraz warunki, jakie należy spełnić, w tym wymóg dotyczący powiadamiania firmy, jeżeli dostawca usług chmury zaproponuje zmianę lokalizacji;

    g) postanowienia dotyczące bezpieczeństwa informacji i ochrony danych osobowych, z uwzględnieniem wytycznej 4;

    h) prawo firmy do regularnego monitorowania działalności dostawcy usług chmury w ramach umowy dotyczącej outsourcingu do chmury, z uwzględnieniem wytycznej 6;

    i) uzgodnione gwarantowane poziomy usług, które powinny obejmować 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 dostawcy usług chmury w zakresie powiadamiania względem firmy oraz, w stosownych przypadkach, obowiązki dotyczące składania sprawozdań istotnych dla funkcji bezpieczeństwa firmy oraz kluczowych funkcji, takich jak sprawozdania z funkcji audytu wewnętrznego dostawcy usług chmury;

k) postanowienia dotyczące zarządzania incydentami przez dostawcę usług chmury, w tym obowiązek dostawcy usług chmury dotyczący bezzwłocznego zgłaszania firmie incydentów, które mają wpływ na świadczenie usług zleconych przez firmę;

l) informację, czy dostawca usług chmury powinien wykupić obowiązkowe ubezpieczenie od określonych rodzajów ryzyka oraz, w stosownych przypadkach, wymagany poziom ochrony;

m) wymogi nałożone na dostawcę usług chmury w zakresie wdrażania i testowania planów ciągłości działania i planów przywrócenia gotowości do pracy po katastrofie;

n) wymóg nałożony na dostawcę usług chmury w zakresie przyznania firmie, jej właściwym organom i każdej innej osobie wyznaczonej przez firmę lub właściwe organy prawa dostępu do („prawa dostępu") oraz kontroli („prawa do audytu") odpowiednich informacji, pomieszczeń, systemów i urządzeń dostawcy usług chmury w zakresie niezbędnym do monitorowania działalności dostawcy usług chmury w ramach umowy dotyczącej outsourcingu do chmury oraz przestrzegania przez niego zgodności z mającymi zastosowanie wymogami regulacyjnymi i umownymi, z uwzględnieniem wytycznej 6;

o) przepisy zapewniające, aby dane przetwarzane lub przechowywane przez dostawcę usług chmury w imieniu firmy były w razie potrzeby dostępne, możliwe do odzyskania i zwrócone firmie, z uwzględnieniem wytycznej 5.

Wytyczna 4. Bezpieczeństwo informacji

29. Firma powinna określić wymogi w zakresie bezpieczeństwa informacji w swoich wewnętrznych strategiach i procedurach oraz w pisemnej umowie dotyczącej outsourcingu do chmury oraz na bieżąco monitorować przestrzeganie tych wymogów, w tym w celu ochrony danych poufnych, osobowych lub w inny sposób wrażliwych. Wymogi te powinny być proporcjonalne do charakteru, skali i złożoności funkcji, którą firma zamierza zlecić dostawcy usług chmury na zasadzie outsourcingu oraz do ryzyka nieodłącznie związanego z tą funkcją.

30. W tym celu, w przypadku outsourcingu funkcji krytycznych lub istotnych oraz bez uszczerbku dla mających zastosowanie wymogów przewidzianych w RODO, firma stosująca podejście oparte na analizie ryzyka powinna co najmniej:

a) *organizacja bezpieczeństwa informacji:* zapewnić jasny podział ról i obowiązków w zakresie bezpieczeństwa informacji między firmą a dostawcą usług chmury, w tym w odniesieniu do wykrywania zagrożeń, zarządzania incydentami i wprowadzania poprawek oraz zapewnić, aby dostawca usług chmury był w stanie skutecznie wypełniać swoje role i obowiązki;

b) *zarządzanie tożsamością i dostępem*: zapewnić wprowadzenie wzmocnionych mechanizmów uwierzytelniania (np. uwierzytelniania wieloskładnikowego) i kontroli dostępu w celu zapobiegania nieuprawnionemu dostępowi do danych firmy i wewnętrznych zasobów chmury;
c) *szyfrowanie i zarządzanie kluczami*: zapewnić stosowanie, w razie potrzeby, odpowiednich technologii szyfrowania w odniesieniu do danych w tranzycie, danych w pamięci, danych odłożonych i kopii zapasowych danych, w połączeniu z odpowiednimi rozwiązaniami w zakresie zarządzania kluczami w celu ograniczenia ryzyka niedozwolonego dostępu do kluczy kryptograficznych; przy wyborze rozwiązania w zakresie zarządzania kluczami firma powinna w szczególności brać pod uwagę najnowocześniejsze technologie i procesy;
d) *operacje i bezpieczeństwo sieci:* rozważyć odpowiednie poziomy dostępności sieci, izolację sieci (na przykład odizolowanie najemcy we wspólnym środowisku chmury, separację operacyjną w odniesieniu do sieci, logiki aplikacji, systemu operacyjnego, systemu zarządzania bazą danych (DBMS) i warstw przechowywania) oraz środowiska przetwarzania (np. testy, testy przyjęcia przez użytkowników, opracowanie, produkcja)
e) *interfejsy programowania aplikacji*: rozważyć mechanizmy integracji usług przetwarzania w chmurze z systemami firmy w celu zapewnienia bezpieczeństwa interfejsów programowania aplikacji (na przykład ustanowienie i utrzymywanie polityki i procedur w zakresie bezpieczeństwa informacji odnośnie do interfejsów programowania aplikacji w różnych interfejsach systemowych, jurysdykcjach i funkcjach biznesowych w celu zapobiegania nieuprawnionemu ujawnianiu, zmienianiu lub niszczeniu danych);
f) *ciągłość działania i przywrócenie gotowości do pracy po katastrofie*: zapewnić skuteczne kontrole ciągłości działania i przywrócenia gotowości do pracy po katastrofie (na przykład poprzez ustanowienie minimalnych wymogów w zakresie pojemności, wybór opcji hostingu, które są odpowiednio rozłożone geograficznie, z możliwością przejścia z jednej opcji do drugiej, lub poprzez żądanie i przegląd dokumentacji wskazującej trasę migracji danych firmy w ramach systemów dostawcy usług chmury, a także rozważenie możliwości kopiowania obrazów maszynowych do niezależnego miejsca przechowywania, które jest wystarczająco odizolowane od sieci lub działa offline);
g) *lokalizacja danych*: przyjąć podejście oparte na analizie ryzyka w odniesieniu do lokalizacji przechowywania i przetwarzania danych (tj. regionów lub państw);
h) *przestrzeganie przepisów i monitorowanie*: sprawdzić, czy dostawca usług chmury przestrzega norm bezpieczeństwa informacji uznanych na szczeblu międzynarodowym oraz czy wdrożył odpowiednie środki kontroli bezpieczeństwa informacji (na przykład poprzez zwrócenie się do dostawcy usług chmury o przedstawienie dowodów na to, że przeprowadza on odpowiednie przeglądy bezpieczeństwa informacji oraz poprzez przeprowadzanie regularnych ocen i testów rozwiązań dostawcy usług chmury w zakresie bezpieczeństwa informacji).

Wytyczna 5. Strategie wyjścia

31. W przypadku outsourcingu funkcji krytycznych lub istotnych firma powinna zapewnić sobie możliwość rozwiązania umowy dotyczącej outsourcingu do chmury bez zbędnych zakłóceń w prowadzeniu swojej działalności i świadczeniu usług na rzecz swoich klientów oraz bez uszczerbku dla wypełniania przez nią obowiązków wynikających z mających zastosowanie przepisów, a także bez uszczerbku dla poufności, integralności i dostępności swoich danych. W tym celu firma powinna:

    a) opracować plany wyjścia, które są kompleksowe, dobrze udokumentowane i odpowiednio przetestowane. Plany te należy w razie potrzeby aktualizować, w tym w przypadku zmian w funkcji zleconej na zasadzie outsourcingu;
    b) określić alternatywne rozwiązania i opracować plany przejścia w celu usunięcia funkcji i danych zleconych na zasadzie outsourcingu u dostawcy usług chmury oraz, w stosownych przypadkach, u każdego podmiotu świadczącego usługi podoutsourcingu i przekazać je alternatywnemu dostawcy usług chmury wskazanemu przez firmę lub bezpośrednio do firmy. Rozwiązania te należy określić w odniesieniu do wyzwań, które mogą pojawić się ze względu na lokalizację danych, podejmując niezbędne środki w celu zapewnienia ciągłości działania w fazie przejściowej;
    c) zapewnić, aby pisemna umowa dotycząca outsourcingu do chmury zawierała zobowiązanie dostawcy usług chmury do wspierania należytego przekazywania funkcji zleconej na zasadzie outsourcingu i związanego z tym przetwarzania danych od dostawcy usług chmury i każdego podmiotu świadczącego usługi podoutsourcingu do innego dostawcy usług chmury wskazanego przez firmę lub bezpośrednio do firmy, w przypadku gdy firma rozpocznie wdrażanie strategii wyjścia. Obowiązek wspierania należytego przekazywania funkcji zleconej na zasadzie outsourcingu i związanego z tym przetwarzania danych powinien obejmować, w stosownych przypadkach, bezpieczne usunięcie danych z systemów dostawcy usług chmury i każdego podmiotu świadczącego usługi podoutsourcingu.

32. Opracowując plany wyjścia i rozwiązania, o których mowa w lit. a) i b) powyżej („strategia wyjścia”), firma powinna uwzględnić:

    a) określenie celów strategii wyjścia;
    b) określenie zdarzeń inicjujących, które mogłyby przyczynić się do wdrożenia strategii wyjścia. Powinny one obejmować co najmniej rozwiązanie umowy dotyczącej outsourcingu do chmury z inicjatywy firmy lub dostawcy usług chmury oraz zakończenie lub inne poważne zakłócenie działalności gospodarczej dostawcy usług chmury;
    c) przeprowadzenie analizy wpływu na działalność współmiernej do funkcji zleconej na zasadzie outsourcingu w celu określenia, jakie zasoby ludzkie i inne byłyby wymagane do wdrożenia strategii wyjścia;
    d) przypisanie ról i obowiązków w celu zarządzania strategią wyjścia;
    e) przetestowanie stosowności strategii wyjścia, stosując podejście oparte na analizie ryzyka (np. poprzez przeprowadzenie analizy potencjalnych kosztów,

oddziaływania, zasobów i skutków czasowych przeniesienia usługi zleconej na zasadzie outsourcingu na rzecz alternatywnego dostawcy);

f) określenie kryteriów dotyczących pomyślnego przeniesienia.

33. Firma powinna uwzględnić oznaki zdarzeń inicjujących strategię wyjścia w ramach bieżącego monitorowania i nadzoru nad usługami świadczonymi przez dostawcę usług chmury w ramach umowy dotyczącej outsourcingu do chmury.

Wytyczna 6. Prawa dostępu i prawa do audytu

34. Firma powinna dopilnować, aby pisemna umowa dotycząca outsourcingu do chmury nie ograniczała skutecznego wykonywania przez firmę i właściwy organ praw dostępu i praw do audytu oraz możliwości nadzoru nad dostawcą usług chmury.

35. Firma powinna dopilnować, aby wykonywanie praw dostępu i praw do audytu (na przykład częstotliwość audytu oraz obszary i usługi podlegające audytowi) uwzględniało to, czy outsourcing jest związany z funkcją krytyczną lub istotną, a także charakter i zakres ryzyka i wpływu umowy dotyczącej outsourcingu do chmury na firmę.

36. W przypadku gdy korzystanie z praw dostępu lub praw do audytu lub stosowanie określonych technik audytu stwarza ryzyko dla środowiska dostawcy usług chmury lub klienta dostawcy usług chmury (na przykład poprzez wpływanie na gwarantowane poziomy usług, poufność, integralność i dostępność danych) dostawca usług chmury powinien przedstawić firmie wyraźne uzasadnienie, dlaczego doprowadziłoby to do powstania ryzyka, a dostawca usług chmury powinien uzgodnić z firmą alternatywne sposoby osiągnięcia podobnego rezultatu (np. wprowadzenie szczególnych kontroli, które mają zostać zbadane w ramach konkretnego sprawozdania/certyfikatu przygotowanego przez dostawcę usług chmury).

37. Firmy, z zastrzeżeniem ich ostatecznej odpowiedzialności odnośnie do umów dotyczących outsourcingu do chmury, w celu efektywniejszego wykorzystania zasobów audytowych i zmniejszenia obciążenia organizacyjnego dostawcy usług chmury i jego klientów, mogą stosować:

a) certyfikaty osoby trzeciej oraz sprawozdania z audytu wewnętrznego lub zewnętrznego udostępnione przez dostawcę usług chmury;
b) połączone audyty przeprowadzone wspólnie z innymi klientami tego samego dostawcy usług chmury lub połączone audyty przeprowadzone przez audytora zewnętrznego wyznaczonego przez wielu klientów tego samego dostawcy usług chmury.

38. W przypadku outsourcingu funkcji krytycznych lub istotnych firma powinna ocenić, czy certyfikaty osoby trzeciej oraz sprawozdania z audytu zewnętrznego lub wewnętrznego, o których mowa w ust. 37 lit. a), są odpowiednie i wystarczające do wypełnienia przez nią obowiązków wynikających z mających zastosowanie przepisów oraz nie powinna dążyć do polegania wyłącznie na tych certyfikatach i sprawozdaniach w przyszłości.

39. W przypadku outsourcingu funkcji krytycznych lub istotnych firma powinna korzystać z certyfikatów osoby trzeciej oraz sprawozdań z audytu zewnętrznego lub wewnętrznego, o których mowa w ust. 37 lit. a), wyłącznie w przypadku gdy:

    a) jest przekonana, że zakres certyfikatów lub sprawozdań z audytu obejmuje kluczowe systemy dostawcy usług chmury (np. procesy, aplikacje, infrastrukturę, centra danych), kluczowe kontrole określone przez firmę oraz przestrzeganie odpowiednich mających zastosowanie przepisów;
    b) dokonuje dokładnej regularnej oceny treści nowych certyfikatów lub sprawozdań z audytu i weryfikacji, czy certyfikaty lub sprawozdania nie są nieaktualne;
    c) zapewnia objęcie kluczowych systemów i kontroli przyszłymi wersjami certyfikatów lub sprawozdań z audytu;
    d) ma pewność co do strony dokonującej certyfikacji lub audytu (na przykład w odniesieniu do jej kwalifikacji, wiedzy fachowej, ponownego przeprowadzenia / weryfikacji dowodów w podstawowej dokumentacji audytowej, jak również rotacji przedsiębiorstwa dokonującego certyfikacji lub audytu);
    e) upewniła się, że certyfikaty są wydawane, a audyty przeprowadzone zgodnie z odpowiednimi standardami i obejmują badanie skuteczności operacyjnej kluczowych kontroli prowadzonych na miejscu;
    f) ma wynikające z umowy prawo zwrócić się o rozszerzenie zakresu certyfikatów lub sprawozdań z audytu na inne odpowiednie systemy i mechanizmy kontroli dostawcy usług chmury; liczba i częstotliwość takich wniosków o zmianę zakresu powinny być uzasadnione i zgodne z prawem z perspektywy zarządzania ryzykiem;
    g) zachowuje wynikające z umowy prawo do przeprowadzania indywidualnych audytów na miejscu według swojego uznania w odniesieniu do funkcji zleconej na zasadzie outsourcingu.

40. Firma powinna dopilnować, aby przed wizytą na miejscu, w tym wizytą osoby trzeciej wyznaczonej przez firmę (na przykład audytora), dostawca usług chmury został o tym powiadomiony z wyprzedzeniem w rozsądnym terminie, chyba że wcześniejsze powiadomienie nie jest możliwe ze względu na sytuację nadzwyczajną lub kryzysową lub prowadziłoby do sytuacji, w której audyt przestałby być skuteczny. Takie powiadomienie powinno określać lokalizację i cel wizyty oraz personel, który będzie uczestniczył w wizycie.

41. Biorąc pod uwagę, że usługi chmury charakteryzują się wysokim poziomem złożoności technicznej i wiążą się ze szczególnymi wyzwaniami jurysdykcyjnymi, pracownicy przeprowadzający audyt – będący audytorami wewnętrznymi firmy lub audytorami działającymi w jej imieniu – powinni posiadać odpowiednie umiejętności i wiedzę umożliwiające właściwą ocenę odpowiednich usług chmury oraz przeprowadzanie skutecznych i odpowiednich audytów. Powinno to mieć również zastosowanie do pracowników firm dokonujących przeglądu certyfikatów lub sprawozdań z audytu dostarczonych przez dostawcę usług chmury.

Wytyczna 7. Podoutsourcing

42. Jeżeli zezwala się na podoutsourcing krytycznych lub istotnych funkcji (lub ich istotnych części) umowa dotycząca outsourcingu do chmury zawarta między firmą a dostawcą usług chmury powinna:

    a) określać jakąkolwiek część lub aspekt funkcji zleconej na zasadzie outsourcingu, które są wyłączone z potencjalnego podoutsourcingu;
    b) określać warunki, które muszą być spełnione w przypadku podoutsourcingu;
    c) wskazywać, że dostawca usług chmury pozostaje odpowiedzialny i jest zobowiązany do nadzorowania tych usług, które zlecił na zasadzie podoutsourcingu w celu zapewnienia, by wszystkie zobowiązania umowne między dostawcą usług chmury a firmą były spełniane w sposób nieprzerwany;
    d) zawierać zobowiązanie dostawcy usług chmury do powiadamiania firmy o jakikolwiek planowanym podoutsourcingu lub istotnych zmianach w tym zakresie, w szczególności w przypadkach, gdy mogłoby to wpłynąć na zdolność dostawcy usług chmury do wypełniania obowiązków wynikających z umowy dotyczącej outsourcingu do chmury zawartej z tą firmą. Okres powiadomienia określony w pisemnej umowie powinien dać firmie wystarczającą ilość czasu przynajmniej na przeprowadzenie oceny ryzyka proponowanego podoutsourcingu lub istotnych zmian w tym zakresie oraz na zgłoszenie sprzeciwu wobec proponowanego podoutsourcingu lub jego wyraźne zatwierdzenie, jak wskazano w lit. e) poniżej;
    e) zapewnić, aby firma miała prawo wniesienia sprzeciwu wobec zamierzonego podoutsourcingu lub istotnych zmian w tym zakresie, lub aby wymagane było wyraźne zatwierdzenie przed wejściem w życie proponowanego podoutsourcingu lub istotnych zmian;
    f) zapewnić, aby firma miała wynikające z umowy prawo do rozwiązania umowy dotyczącej outsourcingu do chmury zawartej z dostawcą usług chmury w przypadku sprzeciwu wobec proponowanego podoutsourcingu lub istotnych zmian w tym zakresie oraz w przypadku nieuzasadnionego podoutsourcingu (na przykład gdydostawca usług chmury rozpoczyna realizację podoutsourcingu bez powiadomienia firmy lub poważnie narusza warunki podoutsourcingu określone w umowie outsourcingu).

43. Firma powinna dopilnować, aby dostawca usług chmury odpowiednio nadzorował podmiot świadczący usługi podoutsourcingu.

Wytyczna 8. Pisemne powiadomienie właściwych organów

44. Firma powinna powiadomić na piśmie swój właściwy organ w odpowiednim czasie o planowanych umowach dotyczących outsourcingu do chmury, które dotyczą funkcji krytycznej lub istotnej. Firma powinna również w odpowiednim czasie i na piśmie powiadomić właściwy organ o tych umowach dotyczących outsourcingu do chmury, które dotyczą funkcji, która została wcześniej zaklasyfikowana jako niekrytyczna lub nieistotna, a następnie stała się krytyczna lub istotna.

45. Pisemnie powiadomienie firmy powinno zawierać, przy uwzględnieniu zasady proporcjonalności, co najmniej następujące informacje:

    a) datę rozpoczęcia oraz, w zależności od przypadku, datę odnowienia umowy, datę zakończenia lub okresy wypowiedzenia obowiązujące dostawcę usług chmury i firmę;
    b) krótki opis funkcji zleconej na zasadzie outsourcingu;
    c) krótkie podsumowanie powodów, dla których zlecona na zasadzie outsourcingu funkcja uważana jest za krytyczną lub istotną;
    d) nazwę i ewentualną nazwę marki dostawcy usług chmury, kraj rejestracji, numer ewidencyjny przedsiębiorstwa, identyfikator podmiotu prawnego (jeżeli jest dostępny), adres i inne stosowne dane kontaktowe oraz nazwę jednostki dominującej (jeżeli istnieje);
    e) prawo właściwe dla umowy dotyczącej outsourcingu do chmury oraz, w stosownych przypadkach, wybór jurysdykcji;
    f) modele wdrażania chmury obliczeniowej oraz szczególny charakter danych, które mają być przechowywane przez dostawcę usług chmury oraz lokalizacje (tj. regiony lub państwa), w których takie dane będą przechowywane;
    g) datę ostatniej oceny krytycznego lub istotnego znaczenia funkcji zleconej na zasadzie outsourcingu;
    h) datę ostatniej oceny ryzyka / ostatniego audytu dostawcy usług chmury wraz z krótkim podsumowaniem głównych wyników oraz datą następnej planowanej oceny ryzyka / następnego planowanego audytu;
    i) informacje na temat osoby fizycznej, która zatwierdziła umowę dotyczącą outsourcingu do chmury lub organu decyzyjnego w firmie, którzy zatwierdzili umowę dotyczącą outsourcingu do chmury;
    j) w stosownych przypadkach nazwy podmiotów świadczących usługi podoutsourcingu, którym na zasadzie podoutsourcingu zlecane są istotne części krytycznych i istotnych funkcji, w tym kraj lub region, w którym podmioty te są zarejestrowane, gdzie wykonywana będzie usługa zlecona na zasadzie podoutsourcingu oraz gdzie przechowywane będą dane;

Wytyczna 9. Nadzór nad umowami dotyczącymi outsourcingu w chmurze

46. W ramach procesu nadzoru właściwe organy powinny oceniać ryzyko dla firm wynikające z umów dotyczących outsourcingu do chmury. Ocena ta powinna dotyczyć w szczególności umów dotyczących outsourcingu funkcji krytycznych lub istotnych.

47. Właściwe organy powinny mieć pewność, że są w stanie sprawować skuteczny nadzór, w szczególności gdy firmy zlecają na zasadzie outsourcingu krytyczne lub istotne funkcje, które są wykonywane poza UE.

48. Właściwe organy powinny ocenić w ramach podejścia opartego na analizie ryzyka, czy firmy:

a) dysponują odpowiednimi mechanizmami zarządzania, zasobami i procesami operacyjnymi umożliwiającymi odpowiednie i skuteczne zawieranie, wdrażanie i nadzorowanie umów dotyczących outsourcingu do chmury;
b) identyfikują wszystkie istotne ryzyka związane z outsourcingiem do chmury i zarządzają nimi;

49. W przypadku stwierdzenia ryzyka koncentracji właściwe organy powinny monitorować rozwój takiego ryzyka i oceniać zarówno jego potencjalny wpływ na inne nadzorowane przez nie firmy, jak i stabilność rynku finansowego.