Council of the European Union

Brussels, 5 March 2024

6867/24

Interinstitutional File: 2020/0266 (COD)

JUR 121
EF 77
ECOFIN 227
TELECOM 79
CYBER 56
CODEC 573

LEGISLATIVE ACTS AND OTHER INSTRUMENTS: CORRIGENDUM/RECTIFICATIF

Subject:	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 *(Official Journal of the European Union L 333 of 27 December 2022)*

LANGUAGE concerned: **PL**

PROCEDURE APPLICABLE (according to Council document R/2521/75):

— Procedure 2(b) (obvious errors in one language version)

This text has also been transmitted to the European Parliament.

TIME LIMIT for the observations by Member States: 3 days

OBSERVATIONS to be notified to: dql.rectificatifs@consilium.europa.eu

(DQL RECTIFICATIFS (JUR 7), Directorate Quality of Legislation, Legal Service)

ZAŁĄCZNIK

SPROSTOWANIE

do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011

(Dziennik Urzędowy Unii Europejskiej L 333 z dnia 27 grudnia 2022 r.)

1. Strona 5, motyw 21, zdanie drugie

zamiast:

„Podmioty finansowe powinny również dysponować strategiami na potrzeby testowania systemów, kontroli i procesów ICT, a także zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT.”

powinno być:

„Podmioty finansowe powinny również dysponować strategiami na potrzeby testowania systemów, mechanizmów kontrolnych i procesów ICT, a także zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT.”.

2. Strony 10-11, motyw 43

zamiast:

„(43) (…) poddawania ich przeglądowi co najmniej raz w roku; do ich regularnego poddawania audytowi wewnętrznemu; do przeprowadzania dogłębnych ocen po istotnych zmianach w ich infrastrukturze sieci i systemów informatycznych oraz powiązanych procedurach, do regularnego przeprowadzania analiz ryzyka w odniesieniu do dotychczasowych systemów ICT, (…) Dodatkowo mikroprzedsiębiorstwa powinny być zobowiązane do oceny potrzeby utrzymywania takich nadmiarowych zdolności w zakresie ICT wyłącznie w oparciu o ich profil ryzyka. Mikroprzedsiębiorstwa powinny korzystać z bardziej elastycznego systemu w odniesieniu do programów testowania operacyjnej odporności cyfrowej. Rozważając rodzaj i częstotliwość przeprowadzanych testów, mikroprzedsiębiorstwa powinny odpowiednio wyważyć cel polegający na utrzymaniu wysokiej operacyjnej odporności cyfrowej, dostępne zasoby i ich ogólny profil ryzyka. Mikroprzedsiębiorstwa i podmioty finansowe objęte uproszczonymi ramami zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia powinny być zwolnione z obowiązku przeprowadzania zaawansowanego testowania narzędzi, systemów i procesów ICT z wykorzystaniem testów penetracyjnych pod kątem wyszukiwania zagrożeń (TLPT), jako że (…)”

powinno być:

„(43) (…) poddawania ich przeglądowi co najmniej raz w roku; do ich regularnego poddawania audytowi wewnętrznemu; do przeprowadzania dogłębnych ocen po istotnych zmianach w ich infrastrukturze sieci i systemów informatycznych oraz powiązanych procedurach, do regularnego przeprowadzania analiz ryzyka w odniesieniu do przestarzałych systemów ICT, (…) Dodatkowo mikroprzedsiębiorstwa powinny być zobowiązane do oceny potrzeby utrzymywania takich nadmiarowych zdolności w zakresie ICT w oparciu o ich profil ryzyka. Mikroprzedsiębiorstwa powinny korzystać z bardziej elastycznego systemu w odniesieniu do programów testowania operacyjnej odporności cyfrowej. Rozważając rodzaj i częstotliwość przeprowadzanych testów, mikroprzedsiębiorstwa powinny odpowiednio wyważyć cel polegający na utrzymaniu wysokiej operacyjnej odporności cyfrowej, dostępne zasoby i ich ogólny profil ryzyka. Mikroprzedsiębiorstwa i podmioty finansowe objęte uproszczonymi ramami zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia powinny być zwolnione z obowiązku przeprowadzania zaawansowanego testowania narzędzi, systemów i procesów ICT z wykorzystaniem testów penetracyjnych ukierunkowanych przez analizę zagrożeń (TLPT), jako że (…)”.

3. Strona 11, motyw 44

zamiast:

„(44) Ponieważ jedynie od podmiotów finansowych objętych zaawansowanym testowaniem odporności cyfrowej powinno wymagać się przeprowadzenia testów penetracyjnych pod kątem wyszukiwania zagrożeń, procesy administracyjne i koszty finansowe związane z przeprowadzeniem takich testów powinny być ponoszone przez niewielki odsetek podmiotów finansowych.”

powinno być:

„(44) Ponieważ jedynie od podmiotów finansowych objętych zaawansowanym testowaniem odporności cyfrowej powinno wymagać się przeprowadzenia testów penetracyjnych ukierunkowanych przez analizę zagrożeń, procesy administracyjne i koszty finansowe związane z przeprowadzeniem takich testów powinny być ponoszone przez niewielki odsetek podmiotów finansowych.”.

4. Strona 12, motyw 49

zamiast:

„(49) Aby umożliwić podmiotom finansowym szybkie i sprawne rozwiązywanie incydentów związanych z ICT, w szczególności cyberataków, poprzez ograniczenie szkód i priorytetowe traktowanie wznowienia działalności i działań naprawczych, konieczne jest opracowanie skutecznych planów ciągłości działania i planów przywracania sprawności zgodnie z ich politykami tworzenia kopii zapasowych. Takie wznowienie działalności nie powinno jednak w żaden sposób zagrażać integralności i bezpieczeństwu sieci i systemów informatycznych lub dostępności, autentyczności, integralności czy poufności danych.”

powinno być:

„(49) Skuteczne plany ciągłości działania i plany przywracania sprawności są konieczne, aby umożliwić podmiotom finansowym szybkie i sprawne rozwiązywanie incydentów związanych z ICT, w szczególności cyberataków, poprzez ograniczenie szkód i priorytetowe traktowanie wznowienia działalności i działań naprawczych zgodnie z ich politykami dotyczącymi zarządzania kopiami zapasowymi. Takie wznowienie działalności nie powinno jednak w żaden sposób zagrażać integralności i bezpieczeństwu sieci i systemów informatycznych lub dostępności, autentyczności, integralności czy poufności danych.”.

5. Strona 13, motyw 56 zdania pierwsze i drugie

zamiast:

„(56) W celu osiągnięcia wysokiego poziomu operacyjnej odporności cyfrowej oraz zgodnie zarówno z odpowiednimi standardami międzynarodowymi (np. określonymi przez G-7 podstawowymi elementami dotyczącymi testów penetracyjnych pod kątem wyszukiwania zagrożeń), jak i ramami stosowanymi w Unii, takimi jak TIBER–EU, podmioty finansowe powinny regularnie testować swoje systemy ICT i personel wykonujący obowiązki związane z ICT pod kątem skuteczności ich zdolności w zakresie zapobiegania, wykrywania, reagowania i przywracania sprawności, aby wykrywać i eliminować potencjalne podatności w zakresie ICT. Aby odzwierciedlić różnice istniejące między różnymi podsektorami finansowymi i w ramach tych podsektorów w zakresie gotowości podmiotów finansowych do reagowania w obszarze cyberbezpieczeństwa, testowanie powinno obejmować szeroki zakres narzędzi i działań, począwszy od oceny podstawowych wymogów (np. oceny podatności i skanowanie pod tym kątem, analizy otwartego oprogramowania, oceny bezpieczeństwa sieci, analizy braków, fizyczne kontrole bezpieczeństwa, kwestionariusze i rozwiązania w zakresie oprogramowania skanującego, w miarę możliwości przeglądy kodu źródłowego, testy scenariuszowe, testy kompatybilności, testy wydajności lub testy kompleksowe) aż po bardziej zaawansowane testowanie przy użyciu TLPT.”

powinno być:

„(56) W celu osiągnięcia wysokiego poziomu operacyjnej odporności cyfrowej oraz zgodnie zarówno z odpowiednimi standardami międzynarodowymi (np. określonymi przez G-7 podstawowymi elementami dotyczącymi testów penetracyjnych ukierunkowanych przez analizę zagrożeń), jak i ramami stosowanymi w Unii, takimi jak TIBER–EU, podmioty finansowe powinny regularnie testować swoje systemy ICT i personel wykonujący obowiązki związane z ICT pod kątem skuteczności ich zdolności w zakresie zapobiegania, wykrywania, reagowania i przywracania sprawności, aby wykrywać i eliminować potencjalne podatności w zakresie ICT. Aby odzwierciedlić różnice istniejące między różnymi podsektorami finansowymi i w ramach tych podsektorów w zakresie gotowości podmiotów finansowych do reagowania w obszarze cyberbezpieczeństwa, testowanie powinno obejmować szeroki zakres narzędzi i działań, począwszy od oceny podstawowych wymogów (np. oceny podatności i skanowanie pod tym kątem, analizy otwartych źródeł informacji, oceny bezpieczeństwa sieci, analizy luk, kontrole bezpieczeństwa fizycznego, kwestionariusze i rozwiązania w zakresie oprogramowania skanującego, w miarę możliwości przeglądy kodu źródłowego, testy scenariuszowe, testy kompatybilności, testy wydajności lub testy kompleksowe) aż po bardziej zaawansowane testowanie przy użyciu TLPT.”.

6. Strona 13, motyw 59

zamiast:

„(59) Z uwagi na to, że niniejsze rozporządzenie nie nakłada na podmioty finansowe wymogu objęcia wszystkich krytycznych lub istotnych funkcji pojedynczym testem penetracyjnym pod kątem wyszukiwania zagrożeń, podmioty te powinny mieć możliwość określenia, które z tych funkcji i jaką ich liczbę należy objąć zakresem takiego testu.”

powinno być:

„(59) Z uwagi na to, że niniejsze rozporządzenie nie nakłada na podmioty finansowe wymogu objęcia wszystkich krytycznych lub istotnych funkcji pojedynczym testem penetracyjnym ukierunkowanym przez analizę zagrożeń, podmioty te powinny mieć możliwość określenia, które z tych funkcji i jaką ich liczbę należy objąć zakresem takiego testu.”.

7. Strona 23, art. 1 ust. 3

zamiast:

„3. Niniejsze rozporządzenie pozostaje bez uszczerbku dla odpowiedzialności państw członkowskich w zakresie podstawowych funkcji państwa dotyczących bezpieczeństwa publicznego, obronności i bezpieczeństwa narodowego zgodnie prawem Unii”

powinno być:

„3. Niniejsze rozporządzenie pozostaje bez uszczerbku dla odpowiedzialności państw członkowskich w zakresie podstawowych funkcji państwa dotyczących bezpieczeństwa publicznego, obronności i bezpieczeństwa narodowego zgodnie z prawem Unii”.

8. Strona 25, art. 3 pkt 3

zamiast:

„3) »dotychczasowy system ICT« oznacza system ICT, którego cykl życia dobiegł końca (koniec okresu użytkowania), którego ze względów technologicznych i komercyjnych nie można zmodernizować ani naprawić, lub który nie jest już obsługiwany przez dostawcę lub zewnętrznego dostawcę usług ICT, ale który nadal jest wykorzystywany i wspiera funkcje danego podmiotu finansowego;”

powinno być:

„3) »przestarzały system ICT« oznacza system ICT, którego cykl życia dobiegł końca (koniec okresu użytkowania), który ze względów technologicznych lub komercyjnych nie kwalifikuje się do modernizacji lub naprawy, lub który nie jest już obsługiwany przez dostawcę lub zewnętrznego dostawcę usług ICT, ale który nadal jest wykorzystywany i wspiera funkcje danego podmiotu finansowego;”.

9. Strona 25, art. 3 pkt 5

zamiast:

„5) »ryzyko związane z ICT« oznacza każdą dającą się racjonalnie określić okoliczność związaną z użytkowaniem sieci i systemów informatycznych, która – jeżeli dojdzie do jej urzeczywistnienia – może zagrozić bezpieczeństwu sieci i systemów informatycznych, dowolnego narzędzia lub procesu zależnego od technologii, bezpieczeństwu operacji i procesów lub świadczeniu usług poprzez wywoływanie negatywnych skutków w środowisku cyfrowym lub fizycznym;”

powinno być:

„5) »ryzyko związane z ICT« oznacza każdą dającą się racjonalnie określić okoliczność związaną z użytkowaniem sieci i systemów informatycznych, która – jeżeli dojdzie do jej urzeczywistnienia – może naruszyć bezpieczeństwo sieci i systemów informatycznych, dowolnego narzędzia lub procesu zależnego od technologii, bezpieczeństwo operacji i procesów lub świadczenie usług poprzez wywoływanie negatywnych skutków w środowisku cyfrowym lub fizycznym;”.

10. Strona 25, ar. 3 pkt 8 i 9

zamiast:

„8) »incydent związany z ICT« oznacza pojedyncze zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, które zagrażają bezpieczeństwu sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy;

9) »incydent operacyjny lub incydent w zakresie bezpieczeństwa związany z płatnościami« oznacza zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez podmioty finansowe, o których mowa w art. 2 ust. 1 lit. a)–d), związanych z ICT lub nie, które mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych związanych z płatnościami lub świadczonych usług związanych z płatnościami realizowanymi przez dany podmiot finansowy;”

powinno być:

„8) »incydent związany z ICT« oznacza pojedyncze zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, <u>które naruszają bezpieczeństwo sieci</u> i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy;

9) »incydent operacyjny lub incydent w zakresie bezpieczeństwa związany z płatnościami« oznacza zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez podmioty finansowe, o których mowa w art. 2 ust. 1 lit. a)–d), związanych z ICT lub nie, które mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych związanych z płatnościami <u>lub na świadczone przez dany podmiot finansowy usługi związane z płatnościami;</u>”.

11. Strona 25, art. 3 pkt 14

zamiast:

„14) »cyberatak« oznacza złośliwy incydent związany z ICT wywołany przez próbę zniszczenia, ujawnienia, zmiany, dezaktywacji, kradzieży lub uzyskania nieuprawnionego dostępu do składnika aktywów lub jego nieuprawnionego wykorzystania przez jakiegokolwiek agresora;”

powinno być:

„14) »cyberatak« oznacza złośliwy incydent związany z ICT wywołany przez próbę zniszczenia, ujawnienia, zmiany, dezaktywacji, kradzieży lub uzyskania nieuprawnionego dostępu do zasobu lub jego nieuprawnionego wykorzystania przez jakiegokolwiek agresora;”.

12. Strona 26, art. 3 pkt 16 i 17

zamiast:

„16) »podatność« oznacza słabość, wrażliwość lub wadę zasobu, systemu, procesu lub kontroli, które można wykorzystać;

17) »testy penetracyjne pod kątem wyszukiwania zagrożeń (TLPT)« oznaczają ramy naśladujące taktykę, techniki i procedury stosowane w rzeczywistości przez agresorów uznanych za stanowiących rzeczywiste cyberzagrożenie, które zapewniają kontrolowane, dostosowane do konkretnych zagrożeń, oparte na analizie zagrożeń (red team) testy działających na bieżąco krytycznych systemów produkcji podmiotu finansowego;”

powinno być:

„16) »podatność« oznacza słabość, wrażliwość lub wadę zasobu, systemu, procesu lub mechanizmu kontrolnego, które można wykorzystać;

17) »testy penetracyjne ukierunkowane przez analizę zagrożeń (TLPT)« oznaczają ramy naśladujące taktykę, techniki i procedury stosowane w rzeczywistości przez agresorów uznanych za stanowiących rzeczywiste cyberzagrożenie, które zapewniają dostarczenie kontrolowanych, dostosowanych do podmiotu, wynikających z analizy zebranych danych (*red team*) testów działających na bieżąco krytycznych systemów produkcyjnych podmiotu finansowego;”.

13. Strona 26, art. 3 pkt 22

zamiast:

„22) »krytyczna lub istotna funkcja« oznacza funkcję, której zakłócenie w sposób istotny wpłynęłoby na wyniki finansowe podmiotu finansowego, na bezpieczeństwo lub ciągłość usług i działalności tego podmiotu lub której zaprzestanie lub wadliwe lub zakończone niepowodzeniem działanie w sposób istotny wpłynęłoby na dalsze wypełnianie przez podmiot finansowy warunków i obowiązków wynikających z udzielonego mu zezwolenia lub jego innych obowiązków wynikających z obowiązujących przepisów dotyczących usług finansowych;”

powinno być:

„22) »krytyczna lub istotna funkcja« oznacza funkcję, której zakłócenie w sposób istotny niekorzystnie wpłynęłoby na wyniki finansowe podmiotu finansowego, na bezpieczeństwo lub ciągłość usług i działalności tego podmiotu lub której zaprzestanie lub wadliwe bądź zakończone niepowodzeniem działanie w sposób istotny niekorzystnie wpłynęłoby na dalsze wypełnianie przez podmiot finansowy warunków i obowiązków wynikających z udzielonego mu zezwolenia lub jego innych obowiązków wynikających z obowiązujących przepisów dotyczących usług finansowych;”.

14. Strona 28, art. 3 pkt 53

zamiast:

„53) »mała instytucja pracowniczych programów emerytalnych« oznacza instytucję pracowniczych programów emerytalnych, która obsługuje programy emerytalne liczące łącznie nie więcej niż 100 uczestników”

powinno być:

„53) »mała instytucja pracowniczych programów emerytalnych« oznacza instytucję pracowniczych programów emerytalnych, która obsługuje programy emerytalne liczące łącznie mniej niż 100 uczestników”.

15. Strona 28, art. 3 pkt 57

zamiast:

„57) »administrator kluczowych wskaźników referencyjnych« oznacza administratora kluczowych wskaźników referencyjnych zdefiniowanych w art. 3 pkt 25 rozporządzenia (UE) 2016/1011;”

powinno być:

„57) »administrator kluczowych wskaźników referencyjnych« oznacza administratora kluczowych wskaźników referencyjnych zdefiniowanych w art. 3 ust. 1 pkt 25 rozporządzenia (UE) 2016/1011;”.

16. Strona 30, art. 6 ust. 2

zamiast:

„2. Ramy zarządzania ryzykiem związanym z ICT obejmują co najmniej strategie, polityki, procedury, protokoły i narzędzia ICT niezbędne do należytej i odpowiedniej ochrony wszystkich odpowiednich zasobów informacyjnych i zasobów ICT, (…)”

powinno być:

„2. Ramy zarządzania ryzykiem związanym z ICT obejmują co najmniej strategie, polityki, procedury, protokoły i narzędzia ICT niezbędne do należytej i odpowiedniej ochrony wszystkich zasobów informacyjnych i zasobów ICT, (…)”.

17. Strona 31, art. 6 ust. 8 lit. c)

zamiast:

„c) określenie jasnych celów w zakresie bezpieczeństwa informacji, w tym najważniejszych wskaźników efektywności i kluczowych wskaźników ryzyka;”

powinno być:

„c) określenie jasnych celów w zakresie bezpieczeństwa informacji, w tym kluczowych wskaźników efektywności i kluczowych wskaźników ryzyka;”.

18. Strona 32, art. 8 ust. 2

zamiast:

„2. Podmioty finansowe na bieżąco identyfikują wszystkie źródła ryzyka związanego z ICT, w szczególności ekspozycję na ryzyko w odniesieniu do innych podmiotów finansowych i pochodzące od tych podmiotów, oraz oceniają cyberzagrożenia i podatności w obszarze ICT istotne dla ich funkcji biznesowych wspieranych przez ICT, zasobów informacyjnych i zasobów ICT. Podmioty finansowe dokonują regularnie, a co najmniej raz w roku, przeglądu scenariuszy ryzyka, które mają na nie wpływ.”

powinno być:

„2. Podmioty finansowe na bieżąco identyfikują wszystkie źródła ryzyka związanego z ICT, w szczególności ekspozycję na ryzyko w odniesieniu do innych podmiotów finansowych i pochodzące od tych podmiotów, oraz oceniają cyberzagrożenia i podatności w obszarze ICT mające znaczenie dla ich funkcji biznesowych wspieranych przez ICT, zasobów informacyjnych i zasobów ICT. Podmioty finansowe dokonują regularnie, a co najmniej raz w roku, przeglądu scenariuszy ryzyka, które mają na nie wpływ.”.

19. Strona 32, art. 8 ust. 7

zamiast:

„7. Podmioty finansowe inne niż mikroprzedsiębiorstwa regularnie, a co najmniej raz w roku, przeprowadzają szczegółową ocenę ryzyka związanego z ICT w odniesieniu do wszystkich dotychczasowych systemów ICT, i w każdym przypadku przed połączeniem i po połączeniu technologii, aplikacji lub systemów”

powinno być:

„7. Podmioty finansowe inne niż mikroprzedsiębiorstwa regularnie, a co najmniej raz w roku, przeprowadzają szczegółową ocenę ryzyka związanego z ICT w odniesieniu do wszystkich przestarzałych systemów ICT, i w każdym przypadku przed połączeniem i po połączeniu technologii, aplikacji lub systemów”.

20. Strona 33, art. 9 ust. 4 lit. c)

zamiast:

„c) wdrażają polityki ograniczające fizyczny lub logiczny dostęp do zasobów informacyjnych i zasobów ICT do tego, co jest wymagane jedynie do uzasadnionych i zatwierdzonych funkcji i działań, oraz ustanawiają w tym celu zestaw polityk, procedur i kontroli dotyczących praw zarządzania dostępem i zapewniających należyte zarządzanie tymi prawami;”

powinno być:

„c) wdrażają polityki ograniczające fizyczny lub logiczny dostęp do zasobów informacyjnych i zasobów ICT do tego, co jest wymagane jedynie do uzasadnionych i zatwierdzonych funkcji i działań, oraz ustanawiają w tym celu zestaw polityk, procedur <u>i mechanizmów kontrolnych dotyczących praw dostępu i</u> zapewniających należyte zarządzanie tymi prawami;”.

21. Strona 33, art. 9 ust. 4 lit. e)

zamiast:

„e) wdrażają udokumentowane polityki, procedury i kontrole w zakresie zarządzania zmianą w systemach ICT, (…)”

powinno być:

„e) wdrażają udokumentowane polityki, procedury <u>i mechanizmy kontrolne w</u> zakresie zarządzania zmianą w systemach ICT, (…)”.

22. Strona 34, art. 11 ust. 2 lit. b) i c)

zamiast:

„b) szybkie, właściwe i skuteczne reagowanie na wszystkie incydenty związane z ICT i ich rozwiązywanie w sposób ograniczający szkody i nadający priorytet wznowieniu działań i działaniom mającym na celu przywrócenie systemów;

c) bezzwłoczne uruchamianie specjalnych planów umożliwiających zastosowanie środków, procesów i technologii ograniczających rozprzestrzenianie się, dostosowanych do każdego rodzaju incydentu związanego z ICT i zapobiegających dalszym szkodom, jak również dostosowanych do potrzeb procedur reagowania i przywracania sprawności, które to procedury zostały ustanowione zgodnie z art. 12”

powinno być:

„b) szybkie, właściwe i skuteczne reagowanie na wszystkie incydenty związane z ICT i ich rozwiązywanie w sposób ograniczający szkody i nadający priorytet wznowieniu działań i działaniom odtworzeniowym;

c) bezzwłoczne uruchamianie specjalnych planów umożliwiających zastosowanie środków, procesów i technologii ograniczających rozprzestrzenianie się, dostosowanych do każdego rodzaju incydentu związanego z ICT i zapobiegających dalszym szkodom, jak również bezzwłoczne uruchamianie dostosowanych do potrzeb procedur reagowania i przywracania sprawności, które to procedury zostały ustanowione zgodnie z art. 12”.

23. Strona 34, art. 11 ust. 3

zamiast:

„3. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 ust. 1, podmioty finansowe wdrażają powiązane z ich działalnością plany reagowania i przywracania sprawności ICT, (…)”

powinno być:

„3. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 ust. 1, podmioty finansowe wdrażają powiązane plany reagowania i przywracania sprawności ICT, (…)”.

24. Strona 34, art. 11 ust. 6 akapit trzeci

zamiast:

„Podmioty finansowe dokonują regularnych przeglądów swojej strategii na rzecz ciągłości działania w zakresie ICT oraz planów przywracania sprawności ICT, uwzględniając wyniki testów przeprowadzonych zgodnie z akapitem pierwszym oraz zalecenia wynikające z kontroli audytowych lub przeglądów nadzorczych.”

powinno być:

„Podmioty finansowe dokonują regularnych przeglądów swojej strategii na rzecz ciągłości działania w zakresie ICT oraz planów reagowania i przywracania sprawności ICT, uwzględniając wyniki testów przeprowadzonych zgodnie z akapitem pierwszym oraz zalecenia wynikające z kontroli audytowych lub przeglądów nadzorczych.”.

25. Strona 35, art. 11 ust. 7

zamiast:

„7. Podmioty finansowe inne niż mikroprzedsiębiorstwa posiadają funkcję zarządzania w sytuacji kryzysowej, w której – w przypadku uruchomienia ich planów ciągłości działania w zakresie ICT lub planów reagowania i przywracania sprawności ICT – określono między innymi. jasne procedury zarządzania wewnętrznymi i zewnętrznymi działaniami informacyjnymi na wypadek wystąpienia sytuacji kryzysowej zgodnie z art. 14.”

powinno być:

„7. Podmioty finansowe inne niż mikroprzedsiębiorstwa posiadają funkcję zarządzania w sytuacji kryzysowej, która – w przypadku uruchomienia ich planów ciągłości działania w zakresie ICT lub planów reagowania i przywracania sprawności ICT – określa między innymi jasne procedury zarządzania wewnętrznymi i zewnętrznymi działaniami informacyjnymi na wypadek wystąpienia sytuacji kryzysowej zgodnie z art. 14.”.

26. Strona 35, art. 11 ust. 9

zamiast:

„9. Centralne depozyty papierów wartościowych dostarczają właściwym organom kopie wyników testów ciągłości działania w zakresie ICT lub podobnych testów.”

powinno być:

„9. Centralne depozyty papierów wartościowych dostarczają właściwym organom kopie wyników testów ciągłości działania w zakresie ICT lub podobnych ćwiczeń.”.

27. Strona 35, art. 12, tytuł i ust. 1–4

zamiast:

„*Artykuł 12*

Polityki i procedury tworzenia kopii zapasowych oraz metody i procedury przywracania i odzyskiwania danych

„1. (…):

a) polityki i procedury tworzenia kopii zapasowych, w których określono (…);

b) procedury i metody przywracania i odzyskiwania danych.

2. Podmioty finansowe ustanawiają systemy tworzenia kopii zapasowych, które mogą być uruchamiane zgodnie z politykami i procedurami tworzenia kopii zapasowych oraz procedurami i metodami przywracania i odzyskiwania danych. Uruchomienie systemów tworzenia kopii zapasowych nie może zagrażać bezpieczeństwu sieci i systemów informatycznych ani dostępności, autentyczności, integralności ani poufności danych. Procedury tworzenia kopii zapasowych a także procedury i metody przywracania i odzyskiwania danych są testowane okresowo.

3. Przywracając dane z kopii zapasowych przy użyciu własnych systemów, podmioty finansowe korzystają z systemów ICT, które są oddzielone fizycznie i logicznie od ich głównego systemu ICT. Systemy ICT są zabezpieczone przed wszelkim nieupoważnionym dostępem lub uszkodzeniem w zakresie ICT i umożliwiają terminowe przywrócenie usług w razie potrzeby przy wykorzystaniu kopii zapasowych danych i systemów.
W przypadku kontrahentów centralnych plany przywracania sprawności umożliwiają odzyskanie wszystkich transakcji realizowanych w chwili wystąpienia zakłócenia, tak aby umożliwić kontrahentowi centralnemu dalsze niezawodne prowadzenie działalności oraz ukończenie rozrachunku w wyznaczonym terminie.
Dostawcy usług w zakresie udostępniania informacji dodatkowo utrzymują odpowiednie zasoby i dysponują urządzeniami służącymi do tworzenia kopii zapasowych i przywracania danych, by móc przez cały czas oferować i utrzymywać swoje usługi.

4. Podmioty finansowe inne niż mikroprzedsiębiorstwa utrzymują nadmiarowe zdolności w zakresie ICT posiadające zasoby, zdolności i funkcje, które są odpowiednie do zaspokojenia potrzeb biznesowych. Mikroprzedsiębiorstwa oceniają potrzebę utrzymywania takich nadmiarowych zdolności w zakresie ICT wyłącznie w oparciu o swój profil ryzyka.”

powinno być:

„*Artykuł 12*

Polityki i procedury zarządzania kopiami zapasowymi oraz procedury i metody odtwarzania i przywracania sprawności

„1. (…):

a) polityki i procedury zarządzania kopiami zapasowymi, w których określono (…);

b) procedury i metody odtwarzania i przywracania sprawności.

2. Podmioty finansowe ustanawiają systemy tworzenia kopii zapasowych, które mogą być uruchamiane zgodnie z politykami i procedurami zarządzania kopiami zapasowymi oraz procedurami i metodami odtwarzania i przywracania sprawności. Uruchomienie systemów tworzenia kopii zapasowych nie może zagrażać bezpieczeństwu sieci i systemów informatycznych ani dostępności, autentyczności, integralności ani poufności danych. Procedury zarządzania kopiami zapasowymi a także procedury i metody odtwarzania i przywracania sprawności są testowane okresowo.

3. Przywracając dane z kopii zapasowych przy użyciu własnych systemów, podmioty finansowe korzystają z systemów ICT, które są oddzielone fizycznie i logicznie od źródłowego systemu ICT. Systemy ICT są zabezpieczone przed wszelkim nieupoważnionym dostępem lub uszkodzeniem w zakresie ICT i umożliwiają terminowe przywrócenie usług w razie potrzeby przy wykorzystaniu kopii zapasowych danych i systemów.

W przypadku kontrahentów centralnych plany przywracania sprawności umożliwiają odtworzenie wszystkich transakcji w chwili wystąpienia zakłócenia, tak aby umożliwić kontrahentowi centralnemu dalsze niezawodne prowadzenie działalności oraz ukończenie rozrachunku w wyznaczonym terminie.

Dostawcy usług w zakresie udostępniania informacji dodatkowo utrzymują odpowiednie zasoby i dysponują obiektami i urządzeniami służącymi do tworzenia kopii zapasowych i odtwarzania, by móc przez cały czas oferować i utrzymywać swoje usługi.

4. Podmioty finansowe inne niż mikroprzedsiębiorstwa utrzymują nadmiarowe zdolności w zakresie ICT posiadające zasoby, zdolności i funkcje, które są odpowiednie do zaspokojenia potrzeb biznesowych. Mikroprzedsiębiorstwa oceniają potrzebę utrzymywania takich nadmiarowych zdolności w zakresie ICT w oparciu o swój profil ryzyka.”.

28. Strona 36, art. 13 ust. 1 i 2

zamiast:

„1. Podmioty finansowe dysponują zdolnościami i personelem umożliwiającymi im gromadzenie informacji na temat podatności oraz cyberzagrożeń, incydentów związanych z ICT, w szczególności cyberataków, oraz analizę ich prawdopodobnego wpływu na operacyjną odporność cyfrową podmiotów finansowych.

2. Podmioty finansowe przeprowadzają przeglądy incydentów związanych z ICT przeprowadzonych po ich wystąpieniu, gdy taki poważny incydent (…).
Podmioty finansowe inne niż mikroprzedsiębiorstwa informują właściwe organy, na żądanie, o zmianach wprowadzonych w następstwie przeglądów incydentów związanych z ICT przeprowadzonych po ich wystąpieniu, o których mowa w akapicie pierwszym.
W ramach przeglądów incydentów związanych z ICT, przeprowadzanych po ich wystąpieniu, o których mowa w akapicie pierwszym, (…)”

powinno być:

„1. Podmioty finansowe dysponują zdolnościami i personelem umożliwiającymi im gromadzenie informacji na temat podatności oraz cyberzagrożeń, incydentów związanych z ICT, w szczególności cyberataków, oraz analizę ich prawdopodobnego wpływu na ich operacyjną odporność cyfrową.

2. Podmioty finansowe przeprowadzają przeglądy po wystąpieniu incydentów związanych z ICT, gdy taki poważny incydent (…).
Podmioty finansowe inne niż mikroprzedsiębiorstwa informują właściwe organy, na żądanie, o zmianach wprowadzonych w następstwie przeglądów po wystąpieniu incydentów związanych z ICT, o których mowa w akapicie pierwszym.
W ramach przeglądów po wystąpieniu incydentów związanych z ICT, o których mowa w akapicie pierwszym, …”.

29. Strona 38, art. 16 ust. 1 lit. e) i f)

zamiast:

„e) określają najważniejsze zależności od zewnętrznych dostawców usług ICT;
f) zapewniają ciągłość krytycznych lub istotnych funkcji poprzez plany ciągłości działania oraz środki reagowania i przywracania sprawności, które obejmują co najmniej środki tworzenia kopii zapasowych i środki przywracania danych;”

powinno być:

„e) określają kluczowe zależności od zewnętrznych dostawców usług ICT;
f) zapewniają ciągłość krytycznych lub istotnych funkcji poprzez plany ciągłości działania oraz środki reagowania i przywracania sprawności, które obejmują co najmniej środki zarządzania kopiami zapasowymi i środki odtwarzania;”.

30. Strona 39, art. 17 ust. 2

zamiast:

„2. Podmioty finansowe rejestrują wszystkie incydenty związane z ICT i znaczące cyberzagrożenia. Podmioty finansowe ustanawiają odpowiednie procedury i procesy mające zapewnić spójne i zintegrowane monitorowanie incydentów związanych z ICT i obsługa takich incydentów oraz działania następcze w związku z takimi incydentami, aby zapewnić zidentyfikowanie, udokumentowanie i wyeliminowanie podstawowych przyczyn, co ma zapobiec występowaniu takich incydentów.”

powinno być:

„2. Podmioty finansowe rejestrują wszystkie incydenty związane z ICT i znaczące cyberzagrożenia. Podmioty finansowe ustanawiają odpowiednie procedury i procesy mające zapewnić spójne i zintegrowane monitorowanie incydentów związanych z ICT i obsługę takich incydentów oraz działania następcze w związku z takimi incydentami, aby zapewnić zidentyfikowanie, udokumentowanie i wyeliminowanie przyczyn źródłowych, co ma zapobiec występowaniu takich incydentów.”.

31. Strona 40, art. 17 ust. 3 lit. e) i f)

zamiast:

„e) zapewnienie zgłaszania co najmniej poważnych incydentów związanych z ICT właściwej kadrze kierowniczej wyższego szczebla oraz informowanie organu zarządzającego co najmniej o poważnych incydentach związanych z ICT wraz z wyjaśnieniem wpływu, reakcji i dodatkowych kontroli, które należy ustanowić w wyniku takich incydentów związanych z ICT;

f) ustanowienie procedur reagowania na incydenty związane z ICT w celu złagodzenia wpływu i zapewnienia przywrócenia operacyjności i bezpieczeństwa usług w rozsądnym terminie.”

powinno być:

„e) zapewnienie zgłaszania co najmniej poważnych incydentów związanych z ICT właściwej kadrze kierowniczej wyższego szczebla oraz informowanie organu zarządzającego co najmniej o poważnych incydentach związanych z ICT wraz z wyjaśnieniem wpływu, reakcji i dodatkowych mechanizmów kontrolnych, które należy ustanowić w wyniku takich incydentów związanych z ICT;

f) ustanowienie procedur reagowania na incydenty związane z ICT w celu złagodzenia wpływu i zapewnienia przywrócenia operacyjności i bezpieczeństwa usług w odpowiednim terminie.”.

32. Strona 41, art. 19 ust. 2 akapit pierwszy, zdanie pierwsze

zamiast:

„2. Podmioty finansowe mogą dobrowolnie powiadomić odpowiedni właściwy organ o znaczących cyberzagrożeniach, jeżeli uznają dane zagrożenie za istotne dla systemu finansowego, użytkowników usług lub klientów.”

powinno być:

„2. Podmioty finansowe mogą dobrowolnie powiadomić odpowiedni właściwy organ o znaczących cyberzagrożeniach, jeżeli uznają, że dane zagrożenie ma znaczenie dla systemu finansowego, użytkowników usług lub klientów.”.

33. Strona 42, art. 19 ust. 3 akapit pierwszy

zamiast:

„3. W przypadku gdy wystąpi poważny incydent związany z ICT, który ma istotny wpływ na interesy finansowe klientów, podmioty finansowe bez zbędnej zwłoki, gdy tylko się o nim dowiedzą, informują swoich klientów o poważnym incydencie związanym z ICT oraz o środkach, które podjęto w celu złagodzenia negatywnych skutków takiego incydentu.”

powinno być:

„3. W przypadku gdy wystąpi poważny incydent związany z ICT, który ma wpływ na interesy finansowe klientów, podmioty finansowe bez zbędnej zwłoki, gdy tylko się o nim dowiedzą, informują swoich klientów o poważnym incydencie związanym z ICT oraz o środkach, które podjęto w celu złagodzenia negatywnych skutków takiego incydentu.”.

34. Strona 42, art. 19 ust. 4 lit. b) i c)

zamiast:

„b) sprawozdanie śródokresowe po wstępnym powiadomieniu, o którym mowa w lit. a), jak tylko status pierwotnego incydentu ulegnie istotnej zmianie lub gdy w oparciu o nowe informacje zmienia się obsługa danego poważnego incydentu związanego z ICT; po tym sprawozdaniu, w stosownych przypadkach, składa się uaktualnione powiadomienia za każdym razem, gdy dostępna jest odpowiednia aktualizacja statusu, jak również na specjalny wniosek właściwego organu;

c) sprawozdanie końcowe, po zakończeniu analizy podstawowych przyczyn, niezależnie od tego, czy wdrożono już środki łagodzące skutki incydentu, oraz po udostępnieniu danych dotyczących rzeczywistego wpływu zastępujących dane szacunkowe.”

powinno być:

„b) sprawozdanie śródokresowe po wstępnym powiadomieniu, o którym mowa w lit. a), jak tylko status pierwotnego incydentu ulegnie istotnej zmianie lub gdy w oparciu o nowe informacje zmienia się obsługa danego poważnego incydentu związanego z ICT; po tym sprawozdaniu, w stosownych przypadkach, składa się uaktualnione powiadomienia za każdym razem, gdy dostępna jest odpowiednia aktualizacja statusu, jak również na wyraźne żądanie właściwego organu;

c) sprawozdanie końcowe, po zakończeniu analizy przyczyn źródłowych, niezależnie od tego, czy wdrożono już środki łagodzące skutki incydentu, oraz gdy dostępne są dane dotyczące rzeczywistego wpływu zastępujące dane szacunkowe.”.

35. Strona 42, art. 19 ust. 6

zamiast:

„6. Po otrzymaniu wstępnego powiadomienia i poszczególnych sprawozdań, o których mowa w ust. 4, (…)”

powinno być:

„6. Po otrzymaniu wstępnego powiadomienia i każdego ze sprawozdań, o których mowa w ust. 4, (…)”.

36. Strona 45, art. 25 ust. 1

zamiast:

„1. Program testowania operacyjnej odporności cyfrowej, o którym mowa w art. 24, przewiduje, zgodnie z kryteriami określonymi w art. 4 ust. 2, przeprowadzenie odpowiednich testów, takich jak oceny podatności i skanowanie pod tym kątem, analizy otwartego oprogramowania, oceny bezpieczeństwa sieci, analizy braków, fizycznych kontroli bezpieczeństwa, kwestionariusze i rozwiązania w zakresie oprogramowania skanującego, przeglądy kodu źródłowego, gdy jest to wykonalne, testy scenariuszowe, testy kompatybilności, testy wydajności, testy kompleksowe i testy penetracyjne.”

powinno być:

„1. Program testowania operacyjnej odporności cyfrowej, o którym mowa w art. 24, przewiduje, zgodnie z kryteriami określonymi w art. 4 ust. 2, przeprowadzenie odpowiednich testów, takich jak oceny podatności i skanowanie pod tym kątem, analizy otwartych źródeł informacji, oceny bezpieczeństwa sieci, analizy luk, kontrole bezpieczeństwa fizycznego, kwestionariusze i rozwiązania w zakresie oprogramowania skanującego, przeglądy kodu źródłowego, gdy jest to wykonalne, testy scenariuszowe, testy kompatybilności, testy wydajności, testy kompleksowe i testy penetracyjne.”.

37. Strona 46, art. 26 ust. 2

zamiast:

„2. Każdy test penetracyjny pod kątem wyszukiwania zagrożeń obejmuje kilka krytycznych lub istotnych funkcji podmiotu finansowego lub wszystkie te funkcje i jest przeprowadzany na działających systemach produkcyjnych wspierających takie funkcje.
Podmioty finansowe określają wszystkie istotne bazowe systemy, procesy i technologie ICT (…)”

powinno być:

„2. Każdy test penetracyjny ukierunkowany przez analizę zagrożeń obejmuje kilka krytycznych lub istotnych funkcji podmiotu finansowego lub wszystkie te funkcje i jest przeprowadzany na działających systemach produkcyjnych wspierających takie funkcje.
Podmioty finansowe określają wszystkie stosowne bazowe systemy, procesy i technologie ICT (…)”.

38. Strona 46, art. 26 ust. 6

zamiast:

„6. Na koniec testowania, po uzgodnieniu sprawozdań i planów naprawczych, podmiot finansowy i, w stosownych przypadkach, testerzy zewnętrzni przedstawiają organowi wyznaczonemu zgodnie z ust. 9 lub 10 podsumowanie najbardziej istotnych ustaleń, plany naprawcze i dokumentację wykazującą, że TLPT przeprowadzono zgodnie z wymogami.”

powinno być:

„6. Na koniec testowania, po uzgodnieniu sprawozdań i planów naprawczych, podmiot finansowy i, w stosownych przypadkach, testerzy zewnętrzni przedstawiają organowi wyznaczonemu zgodnie z ust. 9 lub 10 podsumowanie odpowiednich ustaleń, plany naprawcze i dokumentację wykazującą, że TLPT przeprowadzono zgodnie z wymogami.”.

39. Strona 46, art. 26 ust. 7 akapit pierwszy

zamiast:

„7. Organy przekazują podmiotom finansowym poświadczenie, że test został przeprowadzony zgodnie z wymogami potwierdzonymi w dokumentacji, aby umożliwić właściwym organom wzajemne uznawanie testów penetracyjnych pod kątem wyszukiwania zagrożeń. Podmiot finansowy powiadamia odpowiedni właściwy organ o poświadczeniu, podsumowaniu najbardziej istotnych ustaleń i planach naprawczych.”

powinno być:

„7. Organy przekazują podmiotom finansowym poświadczenie, że test został przeprowadzony zgodnie z wymogami potwierdzonymi w dokumentacji, aby umożliwić właściwym organom wzajemne uznawanie testów penetracyjnych ukierunkowanych przez analizę zagrożeń. Podmiot finansowy powiadamia odpowiedni właściwy organ o poświadczeniu, podsumowaniu odpowiednich ustaleń i planach naprawczych.”.

40. Strona 47, art. 26 ust. 10

zamiast:

„10. W przypadku niewyznaczenia takiego organu zgodnie z ust. 9 niniejszego artykułu i bez uszczerbku dla uprawnienia do określenia podmiotów finansowych, które są zobowiązane do przeprowadzania TLPT, właściwy organ może przekazać wykonywanie niektórych lub wszystkich zadań, o których mowa w niniejszym artykule i w art. 26 i 27, innemu organowi krajowemu w sektorze finansowym.”

powinno być:

„10. W przypadku niewyznaczenia takiego organu zgodnie z ust. 9 niniejszego artykułu i bez uszczerbku dla uprawnienia do określenia podmiotów finansowych, które są zobowiązane do przeprowadzania TLPT, właściwy organ może przekazać wykonywanie niektórych lub wszystkich zadań, o których mowa w niniejszym artykule i w art. 27, innemu organowi krajowemu w sektorze finansowym.”.

41. Strona 48, art. 27 ust. 1 lit. d)

zamiast:

„d) przedstawiają niezależne zapewnienie lub sprawozdanie z audytu dotyczące należytego zarządzania ryzykiem związanym z przeprowadzaniem TLPT, w tym należytej ochrony poufnych informacji podmiotu finansowego i dochodzenia roszczeń z tytułu ryzyka biznesowego podmiotu finansowego;”

powinno być:

„d) przedstawiają niezależne zapewnienie lub sprawozdanie z audytu dotyczące należytego zarządzania ryzykiem związanym z przeprowadzaniem TLPT, w tym należytej ochrony poufnych informacji podmiotu finansowego i mitygacji ryzyka biznesowego podmiotu finansowego;”.

42. Strona 48, art. 28 ust. 1

zamiast:

„1. Podmioty finansowe zarządzają ryzykiem ze strony zewnętrznych dostawców usług ICT integralnym elementem ryzyka związanego z ICT (…)”

powinno być:

„1. Podmioty finansowe zarządzają ryzykiem ze strony zewnętrznych dostawców usług ICT jako integralnym elementem ryzyka związanego z ICT (…)”.

43. Strona 49, art. 28 ust. 4 lit. c) i d)

zamiast:

„c) określają i oceniają wszystkie rodzaje istotnego ryzyka związane z ustaleniem umownym, w tym możliwość, że takie ustalenie umowne może przyczynić się do zwiększenia ryzyka koncentracji w obszarze ICT, o czym mowa w art. 29;

d) dokładają należytej staranności w stosunku do potencjalnych zewnętrznych dostawców usług ICT i zapewniają, aby w trakcie całego procesu wyboru i oceny zewnętrzny dostawca usług ICT był odpowiedni;”

powinno być:

„c) określają i oceniają wszystkie stosowne rodzaje ryzyka związane z ustaleniem umownym, w tym możliwość, że takie ustalenie umowne może przyczynić się do zwiększenia ryzyka koncentracji w obszarze ICT, o czym mowa w art. 29;

d) dokładają należytej staranności w stosunku do potencjalnych zewnętrznych dostawców usług ICT i zapewniają w trakcie całego procesu wyboru i oceny, aby zewnętrzny dostawca usług ICT był odpowiedni;”.

44. Strona 57, art. 33 ust. 3 lit. g)

zamiast:

„g) testowanie systemów, infrastruktury i kontroli ICT;”

powinno być:

„g) testowanie systemów, infrastruktury i mechanizmów kontrolnych ICT;”.

45. Strona 58, art. 35 ust. 1 lit. d) ppkt (i) i (ii)

zamiast:

„(i) stosowania szczególnych wymogów lub procesów z zakresu bezpieczeństwa i jakości ICT, w szczególności w związku z wprowadzaniem poprawek, aktualizacji, szyfrowania i innych środków bezpieczeństwa, które wiodący organ nadzorczy uważa za istotne dla zapewnienia bezpieczeństwa ICT usług świadczonych na rzecz podmiotów finansowych;

(ii) korzystania z warunków i zasad, w tym ich technicznego wdrożenia, zgodnie z którymi kluczowi zewnętrzni dostawcy usług ICT świadczą usługi ICT na rzecz podmiotów finansowych, które wiodący organ nadzorczy uważa za istotne dla zapobiegania powstawaniu pojedynczych punktów awarii lub ich nasileniu lub dla minimalizowania potencjalnego wpływu systemowego na cały sektor finansowy Unii w przypadku ryzyka koncentracji w obszarze ICT;”

powinno być:

„(i) stosowania szczególnych wymogów lub procesów z zakresu bezpieczeństwa i jakości ICT, w szczególności w związku z wprowadzaniem poprawek, aktualizacji, szyfrowania i innych środków bezpieczeństwa, które wiodący organ nadzorczy uważa za stosowne dla zapewnienia bezpieczeństwa ICT usług świadczonych na rzecz podmiotów finansowych;

(ii) korzystania z warunków i zasad, w tym ich technicznego wdrożenia, zgodnie z którymi kluczowi zewnętrzni dostawcy usług ICT świadczą usługi ICT na rzecz podmiotów finansowych, które wiodący organ nadzorczy uważa za stosowne dla zapobiegania powstawaniu pojedynczych punktów awarii lub ich nasileniu lub dla minimalizowania potencjalnego wpływu systemowego na cały sektor finansowy Unii w przypadku ryzyka koncentracji w obszarze ICT;”.

46. Strona 65, art. 42 ust. 1

zamiast:

„1. W terminie 60 dni kalendarzowych od otrzymania zaleceń wydanych przez wiodący organ nadzorczy zgodnie z art. 31 ust. 1 lit. d) kluczowi zewnętrzni dostawcy usług ICT (…)”

powinno być:

„1. W terminie 60 dni kalendarzowych od otrzymania zaleceń wydanych przez wiodący organ nadzorczy zgodnie z art. 35 ust. 1 lit. d) kluczowi zewnętrzni dostawcy usług ICT (…)”.

47. Strona 66, art. 42 ust. 8 lit. b)

zamiast:

„b) kwestię, czy brak zgodności ujawnił poważne słabości w procedurach, systemach zarządzania, zarządzaniu ryzykiem i kontrolach wewnętrznych kluczowego zewnętrznego dostawcy usług ICT;”

powinno być:

„b) kwestię, czy brak zgodności ujawnił poważne słabości w procedurach, systemach zarządzania, zarządzaniu ryzykiem i wewnętrznych mechanizmach kontrolnych kluczowego zewnętrznego dostawcy usług ICT;”.

48. Strona 69, art. 47 ust. 3

zamiast:

„3. W stosownych przypadkach właściwe organy mogą zwrócić się o wszelkie istotne zalecenia techniczne (…).”

powinno być:

„3. W stosownych przypadkach właściwe organy mogą zwrócić się o wszelkie stosowne zalecenia techniczne (…).”.

49. Strona 77, art. 60 pkt 7 lit. b), dotyczy zmiany załącznika III sekcja III lit. a) do rozporządzenia (UE) nr 648/2012

zamiast:

„a) CCP Tier II narusza art. 34 ust. 1, jeżeli nie ustanawia, nie wprowadza ani nie utrzymuje odpowiedniej strategii na rzecz ciągłości działania lub planu reagowania i przywracania sprawności utworzonych zgodnie z rozprowadzeniem (UE) 2022/2554, które służą zapewnieniu zachowania pełnionych funkcji, szybkiego przywrócenia działalności i wywiązywania się z obowiązków CCP, przy czym taki plan musi pozwalać co najmniej na odzyskanie wszystkich transakcji realizowanych w chwili wystąpienia zakłócenia, tak aby umożliwić CCP dalsze niezawodne prowadzenie działalności oraz ukończenie rozrachunku w wyznaczonym terminie;”

powinno być:

„a) CCP Tier II narusza art. 34 ust. 1, jeżeli nie ustanawia, nie wprowadza ani nie utrzymuje odpowiedniej strategii na rzecz ciągłości działania lub planu reagowania i przywracania sprawności utworzonych zgodnie z rozprowadzeniem (UE) 2022/2554, które służą zapewnieniu zachowania pełnionych funkcji, szybkiego przywrócenia działalności i wywiązywania się z obowiązków CCP, przy czym taki plan musi pozwalać co najmniej <u>na odtworzenie wszystkich transakcji w</u> chwili wystąpienia zakłócenia, tak aby umożliwić CCP dalsze niezawodne prowadzenie działalności oraz ukończenie rozrachunku w wyznaczonym terminie;”.