Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/301

20.2.2025

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2025/301

z dnia 23 października 2024 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających treść i terminy przedłożenia wstępnego powiadomienia, sprawozdania śródokresowego i sprawozdania końcowego dotyczących poważnych incydentów związanych z ICT, a także treść dobrowolnego powiadomienia o znaczących cyberzagrożeniach

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 ([1]), a w szczególności jego art. 20 akapit trzeci,

a także mając na uwadze, co następuje:

(1) Aby zapewnić harmonizację i uproszczenie wymogów dotyczących przedkładania powiadomień i sprawozdań w odniesieniu do poważnych incydentów związanych z ICT, o których to powiadomieniach i sprawozdaniach mowa w art. 19 ust. 4 rozporządzenia (UE) 2022/2554, terminy zgłaszania poważnych incydentów związanych z ICT powinny być spójne dla wszystkich rodzajów podmiotów finansowych. Z tych względów terminy te powinny być również, w jak największym stopniu, spójne z wymogami określonymi w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555, a przynajmniej być im równoważne ([2]).

(2) Aby uniknąć nakładania nadmiernych obciążeń sprawozdawczych na podmioty finansowe w czasie, gdy obsługują one incydent związany z ICT, treść wstępnego powiadomienia powinna być ograniczona do najistotniejszych informacji. Aby móc podjąć odpowiednie działania nadzorcze, właściwe organy muszą otrzymywać informacje o poważnych incydentach związanych z ICT jak najszybciej po sklasyfikowaniu incydentu związanego z ICT przez podmiot finansowy jako poważny. W związku z tym termin przedłożenia wstępnego powiadomienia, o którym mowa w art. 19 ust. 4 lit. a) rozporządzenia (UE) 2022/2554, powinien być jak najkrótszy, licząc od momentu sklasyfikowania incydentu związanego z ICT jako poważny, przy jednoczesnym zapewnieniu elastyczności – zwłaszcza w przypadku usługowych modeli biznesowych, w których czas nie jest szczególnie krytyczny – na wypadek gdyby podmioty finansowe potrzebowały więcej czasu na obsługę incydentu związanego z ICT po dowiedzeniu się o nim.

(3) Po otrzymaniu wstępnego powiadomienia właściwe organy powinny otrzymać bardziej szczegółowe informacje na temat incydentu związanego z ICT w sprawozdaniu śródokresowym oraz wszystkie istotne informacje w sprawozdaniu końcowym. Informacje zawarte w tych sprawozdaniach powinny umożliwić właściwym organom dalszą ocenę incydentu związanego z ICT oraz analizę działań nadzorczych, które mogą chcieć podjąć.

(4) W terminach zgłaszania, o których mowa w art. 20 akapit pierwszy lit. a) pkt (ii) rozporządzenia (UE) 2022/2554, należy zatem zrównoważyć potrzebę szybkiego otrzymywania informacji przez właściwe organy z potrzebą zapewnienia podmiotom finansowym wystarczającego czasu na uzyskanie pełnych i dokładnych informacji.

(5) Biorąc pod uwagę kryteria określone w art. 20 akapit pierwszy lit. a) rozporządzenia (UE) 2022/2554, terminy zgłaszania nie powinny stanowić nieproporcjonalnego obciążenia dla mikroprzedsiębiorstw i innych podmiotów finansowych, które nie są istotne. Ponadto, aby uniknąć nieproporcjonalnego obciążenia podmiotów finansowych, terminy zgłaszania powinny uwzględniać weekendy i dni wolne od pracy.

([1]) Dz.U. L 333 z 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Ponieważ powiadamianie o znaczących cyberzagrożeniach ma odbywać się na zasadzie dobrowolności, treść takich powiadomień nie powinna nakładać obciążeń na podmioty finansowe i powinna być bardziej ograniczona niż informacje wymagane w przypadku poważnych incydentów związanych z ICT.

(7) Podstawę niniejszego rozporządzenia stanowi projekt regulacyjnych standardów technicznych przedłożony Komisji przez Europejskie Urzędy Nadzoru.

(8) Europejskie Urzędy Nadzoru przeprowadziły otwarte konsultacje społeczne na temat projektu regulacyjnych standardów technicznych stanowiących podstawę niniejszego rozporządzenia, dokonały analizy kosztów i korzyści, które są z nimi potencjalnie związane, oraz zasięgnęły porady grup interesariuszy ustanowionych zgodnie z art. 37 rozporządzeń Parlamentu Europejskiego i Rady (UE) nr 1093/2010 ([3]), (UE) nr 1094/2010 ([4]) i (UE) nr 1095/2010 ([5]).

(9) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([6]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który w dniu 22 lipca 2024 r. wydał pozytywną opinię. Wszelkie przetwarzanie danych osobowych w ramach niniejszego rozporządzenia powinno odbywać się zgodnie z mającymi zastosowanie zasadami i przepisami dotyczącymi ochrony danych określonymi w rozporządzeniu (UE) 2018/1725,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Informacje ogólne przekazywane we wstępnych powiadomieniach oraz sprawozdaniach śródokresowych i końcowych dotyczących poważnych incydentów związanych z ICT

Podmioty finansowe zamieszczają we wstępnym powiadomieniu, sprawozdaniu śródokresowym i sprawozdaniu końcowym, o których mowa w art. 19 ust. 4 rozporządzenia (UE) 2022/2554, następujące informacje ogólne:

a) rodzaj zgłoszenia (wstępne powiadomienie, sprawozdanie śródokresowe lub sprawozdanie końcowe);

b) nazwę podmiotu finansowego, jego kod LEI oraz rodzaj podmiotu finansowego, zgodnie z art. 2 ust. 1 rozporządzenia (UE) 2022/2554;

c) nazwę i kod identyfikacyjny podmiotu, który przedkłada w imieniu podmiotu finansowego wstępne powiadomienie lub sprawozdanie śródokresowe lub sprawozdanie końcowe;

d) w stosownych przypadkach nazwy i kody LEI wszystkich podmiotów finansowych objętych zbiorczym wstępnym powiadomieniem lub zbiorczym sprawozdaniem śródokresowym lub zbiorczym sprawozdaniem końcowym;

e) dane kontaktowe osób odpowiedzialnych za komunikację z właściwym organem w sprawie poważnego incydentu związanego z ICT;

f) w stosownych przypadkach dane identyfikacyjne jednostki dominującej grupy, do której należy dany podmiot finansowy;

g) w przypadku skutków pieniężnych – waluta, na której opierają się kwoty.

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

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

([5]) 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 (Dz.U. L 331 z 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artykuł 2

Szczegółowe informacje przekazywane we wstępnych powiadomieniach

Wstępne powiadomienia, o których mowa w art. 19 ust. 4 lit. a) rozporządzenia (UE) 2022/2554, zawierają co najmniej wszystkie następujące szczegółowe informacje:

a) kod referencyjny incydentu nadany przez podmiot finansowy;

b) datę wykrycia, godzinę wykrycia i klasyfikację incydentu zgodnie z art. 8 rozporządzenia delegowanego Komisji (UE) 2024/1772 ([7]);

c) opis incydentu związanego z ICT;

d) kryteria określone w art. 1–8 rozporządzenia delegowanego (UE) 2024/1772, na podstawie których podmiot finansowy sklasyfikował incydent związany z ICT jako poważny;

e) państwa członkowskie, na które incydent związany z ICT ma wpływ;

f) informacje o tym, w jaki sposób incydent związany z ICT został wykryty;

g) informacje o pochodzeniu incydentu związanego z ICT, o ile są dostępne;

h) informacje o tym, czy podmiot finansowy uruchomił plan ciągłości działania;

i) w stosownych przypadkach informacje na temat zmiany klasyfikacji incydentu związanego z ICT z poważnego na inny niż poważny;

j) wszelkie inne istotne informacje, jeżeli są dostępne.

Artykuł 3

Szczegółowe informacje przekazywane w sprawozdaniach śródokresowych

Sprawozdania śródokresowe, o których mowa w art. 19 ust. 4 lit. b) rozporządzenia (UE) 2022/2554, zawierają co najmniej wszystkie następujące szczegółowe informacje:

a) w stosownych przypadkach kod referencyjny incydentu przekazany przez właściwy organ;

b) datę i godzinę wystąpienia incydentu związanego z ICT;

c) w stosownych przypadkach datę i godzinę odzyskania przez podmiot finansowy sprawności w zakresie regularnej działalności;

d) informacje, w jaki sposób zostały spełnione kryteria określone w art. 1–8 rozporządzenia delegowanego (UE) 2024/1772, na podstawie których podmiot finansowy sklasyfikował incydent związany z ITC jako poważny;

e) rodzaj incydentu związanego z ICT;

f) w stosownych przypadkach zagrożenia i techniki stosowane przez agresora;

g) obszary funkcjonalne i procesy biznesowe, których dotyczy incydent związany z ICT;

h) wspierające procesy biznesowe elementy infrastruktury, których dotyczy incydent związany z ICT;

i) wpływ na interesy finansowe klientów;

j) informacje na temat zgłoszenia incydentu związanego z ICT innym organom;

k) tymczasowe działania lub środki wprowadzone lub planowane przez podmiot finansowy w celu przywrócenia sprawności po incydencie związanym z ICT;

l) w stosownych przypadkach informacje na temat oznak naruszenia integralności systemu.

([7]) Rozporządzenie delegowane Komisji (UE) 2024/1772 z dnia 13 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria klasyfikacji incydentów związanych z ICT i cyberzagrożeń, progi istotności i szczegółowe informacje dotyczące zgłaszania poważnych incydentów (Dz.U. L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

Artykuł 4

Szczegółowe informacje przekazywane w sprawozdaniach końcowych

Sprawozdania końcowe, o których mowa w art. 19 ust. 4 lit. c) rozporządzenia (UE) 2022/2554, zawierają wszystkie następujące szczegółowe informacje:

a) informacje na temat podstawowych przyczyn incydentu związanego z ICT;

b) daty i godziny rozwiązania incydentu związanego z ICT oraz wyeliminowania podstawowych przyczyn;

c) informacje na temat rozwiązania incydentu związanego z ICT;

d) w stosownych przypadkach informacje istotne dla organów ds. restrukturyzacji i uporządkowanej likwidacji;

e) informacje na temat bezpośrednich i pośrednich kosztów i strat wynikających z incydentu związanego z ICT oraz informacje o odzyskanych środkach finansowych;

f) w stosownych przypadkach informacje o powtarzających się incydentach związanych z ICT.

Artykuł 5

Terminy przedłożenia wstępnego powiadomienia oraz sprawozdania śródokresowego i końcowego

1. Podmioty finansowe przedkładają wstępne powiadomienie oraz sprawozdanie śródokresowe i sprawozdanie końcowe, o których mowa w art. 19 ust. 4 lit. a), b) i c) rozporządzenia (UE) 2022/2554, w następujących terminach:

a) w przypadku wstępnego powiadomienia: tak szybko, jak to możliwe, ale w każdym razie w ciągu czterech godzin od sklasyfikowania incydentu związanego z ICT jako poważny incydent związany z ICT i nie później niż 24 godziny od momentu, w którym podmiot finansowy dowiedział się o incydencie związanym z ICT;

b) w przypadku sprawozdania śródokresowego: najpóźniej w ciągu 72 godzin od przedłożenia wstępnego powiadomienia, nawet jeżeli status incydentu lub obsługa incydentu nie uległy zmianie, jak określono w art. 19 ust. 4 lit. b) rozporządzenia (UE) 2022/2554. Podmioty finansowe przedkładają zaktualizowane sprawozdanie śródokresowe bez zbędnej zwłoki, a w każdym razie po odzyskaniu sprawności w zakresie regularnej działalności;

c) w przypadku sprawozdania końcowego: nie później niż miesiąc po przedłożeniu sprawozdania śródokresowego lub, w stosownych przypadkach, po ostatniej aktualizacji sprawozdania śródokresowego.

2. Jeżeli podmiot finansowy nie sklasyfikował incydentu związanego z ICT jako poważny w ciągu 24 godzin od momentu, w którym podmiot finansowy dowiedział się o nim, ale klasyfikuje ten incydent jako poważny na późniejszym etapie, podmiot ten przedkłada wstępne powiadomienie w terminie czterech godzin od sklasyfikowania incydentu związanego z ICT jako poważny incydent.

3. Podmioty finansowe, które nie są w stanie przedłożyć wstępnego powiadomienia, sprawozdania śródokresowego lub sprawozdania końcowego w terminach określonych w ust. 1, informują o tym właściwy organ bez zbędnej zwłoki, ale nie później niż w odpowiednich terminach przedłożenia powiadomienia lub sprawozdania, i wyjaśniają przyczyny opóźnienia.

4. W przypadku gdy termin złożenia wstępnego powiadomienia, sprawozdania śródokresowego lub sprawozdania końcowego przypada w weekend lub dzień wolny od pracy w państwie członkowskim zgłaszającego podmiotu finansowego, podmiot finansowy może przedłożyć wstępne powiadomienie, sprawozdanie śródokresowe lub sprawozdanie końcowe do południa następnego dnia roboczego.

5. Ust. 4 nie ma zastosowania do przedkładania wstępnego powiadomienia lub sprawozdania śródokresowego przez instytucje kredytowe, kontrahentów centralnych, operatorów systemów obrotu i inne podmioty finansowe uznane za podmioty kluczowe lub podmioty ważne na podstawie art. 3 dyrektywy (UE) 2022/2555.

6. Właściwe organy mogą podjąć decyzję, że ust. 4 nie ma zastosowania do przedkładania wstępnego powiadomienia lub sprawozdania śródokresowego przez podmioty finansowe inne niż te, o których mowa w ust. 5, które są znaczące lub mają charakter systemowy dla sektora finansowego na poziomie krajowym lub unijnym. Właściwe organy powiadamiają o swojej decyzji wskazane podmioty finansowe. Decyzja właściwego organu ma zastosowanie wyłącznie do incydentów zgłaszanych po dacie powiadomienia wskazanych podmiotów finansowych o tej decyzji przez właściwy organ.

Artykuł 6

Treść dobrowolnego powiadomienia o znaczących cyberzagrożeniach

Treść dobrowolnego powiadomienia o znaczących cyberzagrożeniach, o którym mowa w art. 19 ust. 2 rozporządzenia (UE) 2022/2554, obejmuje wszystkie następujące elementy:

a) ogólne informacje o powiadamiającym podmiocie finansowym, jak określono w art. 1;

b) datę i godzinę wykrycia znaczącego cyberzagrożenia oraz wszelkie inne istotne znaczniki czasu związane ze znaczącym cyberzagrożeniem;

c) opis znaczącego cyberzagrożenia;

d) informacje na temat potencjalnego wpływu znaczącego cyberzagrożenia na podmiot finansowy, jego klientów lub kontrahentów finansowych;

e) kryteria klasyfikacji, określone w art. 1–8 rozporządzenia delegowanego (UE) 2024/1772, które – gdyby cyberzagrożenie się urzeczywistniło – spowodowałyby zgłoszenie poważnego incydentu;

f) informacje na temat statusu znaczącego cyberzagrożenia i wszelkich zmian w zagrożeniu;

g) w stosownych przypadkach opis działań podjętych przez podmiot finansowy w celu zapobieżenia urzeczywistnieniu się znaczących cyberzagrożeń;

h) informacje o wszelkich powiadomieniach innych podmiotów lub organów finansowych o znaczącym cyberzagrożeniu;

i) w stosownych przypadkach informacje na temat oznak naruszenia integralności systemu;

j) wszelkie inne istotne informacje, jeżeli są dostępne.

Artykuł 7

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 23 października 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN