ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/302

z dnia 23 października 2024 r.

ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych formularzy, wzorów i procedur stosowanych przez podmioty finansowe do celów zgłaszania poważnych incydentów związanych z ICT i powiadamiania 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]), w szczególności jego art. 20 akapit czwarty,

a także mając na uwadze, co następuje:

(1) W celu zapewnienia, aby podmioty finansowe w spójny sposób zgłaszały poważne incydenty swoim właściwym organom oraz aby przekazywały tym organom dane dobrej jakości, należy określić, które pola danych podmioty te muszą przekazać na różnych etapach zgłaszania, o których mowa w art. 19 ust. 4 rozporządzenia (UE) 2022/2554. Ważne jest, aby informacje te były przedstawiane w sposób umożliwiający jednolity przegląd incydentu. Do tych celów należy zatem ustanowić jednolity wzór sprawozdawczy.

(2) Podmioty finansowe powinny wypełnić te pola danych wzoru sprawozdawczego, które odpowiadają wymogom informacyjnym określonym w odpowiednim powiadomieniu lub sprawozdaniu. Podmioty finansowe, które posiadają już informacje, które mają przekazać na późniejszym etapie sprawozdawczości, tj. w sprawozdaniu śródokresowym lub końcowym, powinny jednak mieć możliwość uprzedniego przedłożenia danych.

(3) Ponieważ liczne lub powtarzające się incydenty mogą stanowić poważny incydent, o którym mowa w art. 8 rozporządzenia delegowanego Komisji (UE) 2024/1772 ([2]), struktura wzoru sprawozdawczego i pól danych powinna umożliwiać podmiotom finansowym zgłaszanie takich powtarzających się incydentów.

(4) Aby zapewnić dokładne i aktualne informacje, wzór sprawozdawczy powinien umożliwiać podmiotom finansowym – przy przedkładaniu sprawozdania śródokresowego i końcowego – aktualizację wszelkich informacji, które zostały wcześniej przedłożone, oraz, w razie potrzeby, zmianę klasyfikacji poważnych incydentów na incydenty inne niż poważne.

(5) Identyfikację prawną podmiotów należy dostosować do identyfikatorów określonych w wykonawczych standardach technicznych przyjętych na podstawie art. 28 ust. 9 rozporządzenia (UE) 2022/2554.

(6) W przypadku gdy podmioty finansowe zlecają w drodze outsourcingu zadania związane z obowiązkami w zakresie zgłaszania poważnych incydentów związanych z ICT osobie trzeciej, właściwe organy powinny znać tożsamość osoby trzeciej dokonującej zgłoszenia w imieniu podmiotu finansowego przed przedłożeniem pierwszego powiadomienia lub pierwszego sprawozdania, aby móc zweryfikować legalność zgłaszającej osoby trzeciej.

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

([2]) 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).

(7) Aby łatwo zidentyfikować skutki incydentu, który miał miejsce u dostawcy będącego osobą trzecią lub został spowodowany przez dostawcę będącego osobą trzecią i który ma wpływ na wiele podmiotów finansowych w jednym państwie członkowskim, oraz aby ograniczyć nakład pracy ponoszony przez podmioty finansowe w związku ze sprawozdawczością, wzór sprawozdawczy powinien umożliwiać przedłożenie zagregowanego sprawozdania obejmującego zagregowane informacje na temat skutków incydentu dla wszystkich podmiotów finansowych, których ten incydent dotyczył i które zaklasyfikowały ten incydent jako poważny.

(8) Wzór sprawozdawczy powinien być opracowany w sposób neutralny pod względem technologicznym, aby umożliwić jego wdrożenie w różnych rozwiązaniach w zakresie zgłaszania incydentów, które już istnieją lub które mogą zostać opracowane na potrzeby wdrożenia wymogów rozporządzenia (UE) 2022/2554.

(9) Struktura wzoru sprawozdawczego i pól danych powinna ułatwiać zgłaszanie poważnych incydentów związanych z ICT przez osoby trzecie, którym podmioty finansowe zleciły na zasadzie outsourcingu zadania związane ze spoczywającym na tych podmiotach obowiązkiem sprawozdawczym zgodnie z art. 19 ust. 5 rozporządzenia (UE) 2022/2554.

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

(11) Europejskie Urzędy Nadzoru przeprowadziły otwarte konsultacje publiczne w zakresie projektu wykonawczych standardów technicznych, który stanowi podstawę niniejszego rozporządzenia, przeanalizowały potencjalne powiązane koszty i korzyści oraz zwróciły się o opinię do 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]).

(12) 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

Wzór na potrzeby zgłaszania poważnych incydentów związanych z ICT

1. Podmioty finansowe korzystają ze wzoru określonego w załączniku I na potrzeby przedłożenia wstępnego powiadomienia, sprawozdania śródokresowego i sprawozdania końcowego, o których mowa w art. 19 ust. 4 rozporządzenia (UE) 2022/2554, w następujący sposób:

a) podmioty finansowe, które przedkładają wstępne powiadomienie, wypełniają pola danych wzoru, które odpowiadają informacjom do przekazania zgodnie z art. 2 rozporządzenia delegowanego Komisji (UE) 2025/301 ([7]), oraz mogą, w przypadku gdy posiadają już te informacje, wypełnić te pola danych, których wypełnienie nie jest wymagane w przypadku wstępnego powiadomienia, lecz których wypełnienie jest wymagane w przypadku sprawozdania śródokresowego lub końcowego;

([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).

([7]) 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 (Dz.U. L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) podmioty finansowe, które przedkładają sprawozdanie śródokresowe, wypełniają pola danych wzoru, które odpowiadają informacjom do przekazania zgodnie z art. 3 rozporządzenia delegowanego (UE) 2025/301, oraz mogą, w przypadku gdy posiadają już stosowne informacje, wypełnić pola danych, których wypełnienie nie jest wymagane w przypadku sprawozdania śródokresowego, lecz których wypełnienie jest wymagane w przypadku sprawozdania końcowego;

c) podmioty finansowe, które przedkładają sprawozdanie końcowe, wypełniają pola danych wzoru, które odpowiadają informacjom do przekazania zgodnie z art. 4 rozporządzenia delegowanego (UE) 2025/301.

2. Podmioty finansowe zapewniają kompletność i dokładność informacji przedstawianych we wstępnym powiadomieniu oraz w sprawozdaniu śródokresowym i końcowym.

3. Podmioty finansowe, w miarę możliwości, przedstawiają szacunkowe wartości oparte na innych dostępnych danych i informacjach, w przypadku gdy dokładne dane nie są dostępne w momencie przedkładania wstępnego powiadomienia lub sprawozdania śródokresowego.

4. Przedkładając sprawozdanie śródokresowe lub końcowe, podmioty finansowe korzystają ze wzoru określonego w załączniku I w celu przekazania wszystkich wymaganych informacji oraz, w stosownych przypadkach, aktualizacji informacji, które zostały wcześniej przedstawione we wstępnym powiadomieniu lub w sprawozdaniu śródokresowym.

5. Wypełniając wzór określony w załączniku I, podmioty finansowe stosują glosariusz danych i instrukcje określone w załączniku II.

Artykuł 2

Łączne przedłożenie wstępnego powiadomienia, sprawozdania śródokresowego i sprawozdania końcowego

Podmioty finansowe mogą połączyć przedłożenie wstępnego powiadomienia oraz sprawozdania śródokresowego i sprawozdania końcowego w celu przekazania dwóch lub wszystkich tych dokumentów w tym samym czasie, w przypadku gdy przywrócono regularne działania lub zakończono analizę przyczyn źródłowych oraz pod warunkiem że dochowano terminów określonych w art. 5 rozporządzenia delegowanego (UE) 2025/301.

Artykuł 3

Powtarzające się incydenty związane z ICT

Podmioty finansowe, które przekazują informacje na temat innych niż poważne, powtarzających się incydentów związanych z ICT, które łącznie spełniają warunki dotyczące jednego poważnego incydentu związanego z ICT określone w art. 8 ust. 2 rozporządzenia delegowanego (UE) 2024/1772, przekazują te informacje w formie zagregowanej.

Artykuł 4

Korzystanie z zabezpieczonych kanałów elektronicznych

1. Podmioty finansowe korzystają z zabezpieczonych kanałów elektronicznych udostępnionych przez ich właściwy organ w celu przedłożenia wstępnego powiadomienia oraz sprawozdania śródokresowego i końcowego.

2. Podmioty finansowe, które nie są w stanie korzystać z zabezpieczonych kanałów elektronicznych udostępnionych przez ich właściwy organ, informują swój właściwy organ o poważnym incydencie związanym z ICT za pomocą innych bezpiecznych środków komunikacji w porozumieniu z właściwym organem. Jeżeli wymaga tego właściwy organ, podmioty finansowe ponownie przedkładają wstępne powiadomienie lub sprawozdanie śródokresowe lub końcowe za pośrednictwem zabezpieczonego kanału elektronicznego udostępnionego przez właściwy organ, gdy tylko będą w stanie tego dokonać.

Artykuł 5

Zmiana klasyfikacji poważnych incydentów związanych z ICT

Jeżeli po przeprowadzeniu dalszej oceny podmiot finansowy stwierdza, że incydent związany z ICT zgłoszony wcześniej jako poważny w żadnym momencie nie spełniał kryteriów klasyfikacji i progów określonych w art. 8 rozporządzenia delegowanego (UE) 2024/1772, podmiot finansowy powiadamia właściwy organ o zmianie klasyfikacji incydentu związanego z ICT z poważnego na inny niż poważny, podając informacje na temat tej zmiany klasyfikacji we wzorze określonym w załączniku II do niniejszego rozporządzenia w polach „rodzaj sprawozdania" i „inne informacje".

Artykuł 6

Powiadomienie o outsourcingu zadań związanych z obowiązkami sprawozdawczymi

1. Podmioty finansowe, które zleciły w drodze outsourcingu zadania związane z obowiązkiem zgłaszania poważnych incydentów związanych z ICT zgodnie z art. 19 ust. 5 rozporządzenia (UE) 2022/2554, informują swój właściwy organ o takim ustaleniu dotyczącym outsourcingu niezwłocznie po jego zawarciu, a najpóźniej przed przedłożeniem pierwszego powiadomienia lub sprawozdania.

2. Podmioty finansowe przekazują właściwemu organowi nazwę, dane kontaktowe i kod identyfikacyjny osoby trzeciej, która będzie przedkładać mu powiadomienia lub sprawozdania dotyczące poważnego incydentu związanego z ICT.

3. Podmioty finansowe informują swój właściwy organ, gdy tylko przestaną zlecać w drodze outsourcingu zadania związane z ich obowiązkami sprawozdawczymi zgodnie z art. 19 ust. 5 rozporządzenia (UE) 2022/2554.

Artykuł 7

Sprawozdawczość zagregowana

1. Dostawca usług będący osobą trzecią, któremu zlecono w drodze outsourcingu zadania związane z obowiązkami sprawozdawczymi zgodnie z art. 19 ust. 5 rozporządzenia (UE) 2022/2554, może korzystać ze wzoru określonego w załączniku I do niniejszego rozporządzenia, aby przedstawić zagregowane informacje na temat poważnego incydentu związanego z ICT mającego wpływ na wiele podmiotów finansowych w ramach jednego powiadomienia lub sprawozdania, oraz może przedłożyć to powiadomienie lub sprawozdanie właściwemu organowi w imieniu wszystkich podmiotów finansowych, których dotyczy dany incydent, pod warunkiem że spełnione są wszystkie następujące warunki:

a) poważny incydent związany z ICT, który ma zostać zgłoszony, wywodzi się od dostawcy usług będącego osobą trzecią lub został przez niego spowodowany;

b) ten dostawca usług będący osobą trzecią świadczy daną usługę ICT na rzecz więcej niż jednego podmiotu finansowego lub na rzecz grupy;

c) incydent związany z ICT został sklasyfikowany jako poważny przez każdy podmiot finansowy uwzględniony w zagregowanym powiadomieniu lub sprawozdaniu;

d) poważny incydent związany z ICT wywiera wpływ na podmioty finansowe w jednym państwie członkowskim, a zagregowane sprawozdanie dotyczy podmiotów finansowych nadzorowanych przez ten sam właściwy organ;

e) właściwe organy wyraźnie zezwoliły temu rodzajowi podmiotów finansowych na sprawozdawczość zagregowaną.

2. Ust. 1 nie ma zastosowania do instytucji kredytowych, które uznaje się za istotne nadzorowane podmioty, o których mowa w art. 2 pkt 16 rozporządzenia (UE) nr 468/2014 Europejskiego Banku Centralnego ([8]), operatorów systemów obrotu i kontrahentów centralnych, którzy korzystają ze wzoru określonego w załączniku I wyłącznie do indywidualnego przedkładania swojemu właściwemu organowi powiadomień lub sprawozdań dotyczących poważnych incydentów związanych z ICT.

3. W przypadku gdy właściwe organy zwracają się o udostępnienie informacji na temat indywidualnego wpływu poważnego incydentu związanego z ICT na jeden podmiot finansowy, ten podmiot finansowy, na wniosek właściwego organu, przedkłada indywidualne powiadomienie lub sprawozdanie dotyczące poważnego incydentu związanego z ICT.

([8]) Rozporządzenie (UE) nr 468/2014 Europejskiego Banku Centralnego z dnia 16 kwietnia 2014 r. ustanawiające ramy współpracy pomiędzy Europejskim Bankiem Centralnym a właściwymi organami krajowymi oraz wyznaczonymi organami krajowymi w ramach Jednolitego Mechanizmu Nadzorczego (rozporządzenie ramowe w sprawie Jednolitego Mechanizmu Nadzorczego) (EBC/2014/17) (Dz.U. L 141 z 14.5.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Artykuł 8

Powiadamianie o znaczących cyberzagrożeniach

1. Podmioty finansowe, które powiadamiają właściwe organy o znaczących cyberzagrożeniach zgodnie z art. 19 ust. 2 rozporządzenia (UE) 2022/2554, korzystają ze wzoru określonego w załączniku III do niniejszego rozporządzenia oraz stosują glosariusz danych i instrukcje określone w załączniku IV do niniejszego rozporządzenia.

2. Podmioty finansowe zapewniają kompletność i dokładność informacji przedstawianych w powiadomieniu o znaczących cyberzagrożeniach.

Artykuł 9

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

ZAŁĄCZNIK I

WZORY NA POTRZEBY ZGŁASZANIA POWAŻNYCH INCYDENTÓW

Numer pola	Pole danych	
Ogólne informacje o podmiocie finansowym		
1.1	Rodzaj zgłoszenia	
1.2	Nazwa podmiotu przedkładającego sprawozdanie	
1.3	Kod identyfikacyjny podmiotu przedkładającego sprawozdanie	
1.4	Rodzaj podmiotu finansowego, którego dotyczy incydent	
1.5	Nazwa podmiotu finansowego, którego dotyczy incydent	
1.6	Kod LEI podmiotu finansowego, którego dotyczy incydent	
1.7	Imię i nazwisko głównej osoby wyznaczonej do kontaktów	
1.8	Adres e-mail głównej osoby wyznaczonej do kontaktów	
1.9	Numer telefonu głównej osoby wyznaczonej do kontaktów	
1.10	Imię i nazwisko dodatkowej osoby wyznaczonej do kontaktów	
1.11	Adres e-mail dodatkowej osoby wyznaczonej do kontaktów	
1.12	Numer telefonu dodatkowej osoby wyznaczonej do kontaktów	
1.13	Nazwa jednostki dominującej najwyższego szczebla	
1.14	Kod LEI jednostki dominującej najwyższego szczebla	
1.15	Waluta sprawozdawcza	
Zawartość wstępnego powiadomienia		
2.1	Kod referencyjny incydentu nadany przez podmiot finansowy	
2.2	Data i godzina wykrycia poważnego incydentu związanego z ICT	
2.3	Data i godzina sklasyfikowania incydentu związanego z ICT jako poważny	
2.4	Opis poważnego incydentu związanego z ICT	
2.5	Kryteria klasyfikacji, które doprowadziły do zgłoszenia incydentu	
2.6	Progi istotności dla kryterium klasyfikacji „Zasięg geograficzny”	
2.7	Wykrycie poważnego incydentu związanego z ICT	

Numer pola	Pole danych	
2.8	Wskazanie, czy poważny incydent związany z ICT wywodzi się od dostawcy będącego osobą trzecią lub innego podmiotu finansowego	
2.9	Uruchomienie planu ciągłości działania, jeżeli plan został uruchomiony	
2.10	Inne istotne informacje	
Zawartość sprawozdania śródokresowego		
3.1	Kod referencyjny incydentu podany przez właściwy organ	
3.2	Data i godzina wystąpienia poważnego incydentu związanego z ICT	
3.3	Data i godzina przywrócenia usług, działań lub operacji	
3.4	Liczba klientów, których dotyczy incydent	
3.5	Odsetek klientów, których dotyczy incydent	
3.6	Liczba kontrahentów finansowych, których dotyczy incydent	
3.7	Odsetek kontrahentów finansowych, których dotyczy incydent	
3.8	Skutki dla odpowiednich klientów lub kontrahentów finansowych	
3.9	Liczba transakcji, których dotyczy incydent	
3.10	Odsetek transakcji, których dotyczy incydent	
3.11	Wartość transakcji, których dotyczy incydent	
3.12	Informacja, czy dane liczbowe są rzeczywiste czy szacunkowe, lub czy nie wystąpiły jakiekolwiek skutki	
3.13	Skutki reputacyjne	
3.14	Informacje kontekstowe na temat skutków reputacyjnych	
3.15	Czas trwania poważnego incydentu związanego z ICT	
3.16	Przerwa w świadczeniu usług	
3.17	Informacja, czy dane liczbowe dotyczące czasu trwania incydentu i przerwy w świadczeniu usług są rzeczywiste czy szacunkowe	
3.18	Rodzaje skutków w państwach członkowskich	
3.19	Opis skutków poważnego incydentu związanego z ICT w innych państwach członkowskich	
3.20	Progi istotności dla kryterium klasyfikacji „Utrata danych”	
3.21	Opis utraty danych	

Numer pola	Pole danych	
3.22	Kryterium klasyfikacji „Usługi krytyczne, których dotyczy incydent”	
3.23	Rodzaj poważnego incydentu związanego z ICT	
3.24	Inne rodzaje incydentów	
3.25	Zagrożenia i techniki stosowane przez agresora	
3.26	Inne rodzaje technik	
3.27	Informacje na temat obszarów funkcjonalnych i procesów biznesowych, których dotyczy incydent	
3.28	Elementy infrastruktury wspierające procesy biznesowe, których to elementów dotyczy incydent	
3.29	Informacje na temat elementów infrastruktury wspierających procesy biznesowe, których to elementów dotyczy incydent	
3.30	Wpływ na interesy finansowe klientów	
3.31	Składanie sprawozdań innym organom	
3.32	Określenie „innych” organów	
3.33	Tymczasowe działania/środki podjęte lub planowane w celu przywrócenia sytuacji sprzed incydentu	
3.34	Opis wszelkich tymczasowych działań i środków podjętych lub planowanych w celu przywrócenia sytuacji sprzed incydentu	
3.35	Oznaki naruszenia integralności systemu	
Zawartość sprawozdania końcowego		
4.1	Ogólna klasyfikacja przyczyn źródłowych incydentu	
4.2	Szczegółowa klasyfikacja przyczyn źródłowych incydentu	
4.3	Dodatkowa klasyfikacja przyczyn źródłowych incydentu	
4.4	Inne rodzaje przyczyn źródłowych	
4.5	Informacje na temat przyczyn źródłowych incydentu	
4.6	Streszczenie dotyczące zaradzenia incydentowi	
4.7	Data i godzina usunięcia przyczyny źródłowej incydentu	
4.8	Data i godzina zaradzenia incydentowi	
4.9	Informacja, czy data trwałego zaradzenia incydentowi różni się od pierwotnie planowanej daty wdrożenia	
4.10	Ocena ryzyka dla funkcji krytycznych do celów restrukturyzacji i uporządkowanej likwidacji	
4.11	Informacje istotne dla organów ds. restrukturyzacji i uporządkowanej likwidacji	

Numer pola	Pole danych	
4.12	Próg istotności dla kryterium klasyfikacji „Skutki gospodarcze”	
4.13	Kwota bezpośrednich i pośrednich kosztów i strat brutto	
4.14	Kwota odzyskanych środków finansowych	
4.15	Informacja, czy incydenty inne niż poważne powtarzały się	
4.16	Data i godzina wystąpienia powtarzających się incydentów	

ZAŁĄCZNIK II

GLOSARIUSZ DANYCH I INSTRUKCJE DOTYCZĄCE ZGŁASZANIA POWAŻNYCH INCYDENTÓW

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
Ogólne informacje o podmiocie finansowym						
1.1.	Rodzaj zgłoszenia	Należy wskazać rodzaj powiadomienia lub sprawozdania dotyczącego incydentu przedkładanego właściwemu organowi.	Tak	Tak	Tak	Wybór: — wstępne powiadomienie; — sprawozdanie śródokresowe; — sprawozdanie końcowe; — poważny incydent przeklasyfikowany jako inny niż poważny.
1.2.	Nazwa podmiotu przedkładającego sprawozdanie	Pełna nazwa prawna podmiotu przedkładającego sprawozdanie.	Tak	Tak	Tak	Alfanumeryczne
1.3.	Kod identyfikacyjny podmiotu przedkładającego sprawozdanie	Kod identyfikacyjny podmiotu przedkładającego sprawozdanie. W przypadku gdy powiadomienie/sprawozdanie przedkładają podmioty finansowe, kodem identyfikacyjnym jest identyfikator podmiotu prawnego (LEI), który jest niepowtarzalnym kodem składającym się z 20 znaków alfanumerycznych, zgodnie z ISO 17442-1:2020. Dostawca będący osobą trzecią, który przedkłada sprawozdanie w imieniu podmiotu finansowego, może stosować kod identyfikacyjny określony w wykonawczych standardach technicznych przyjętych na podstawie art. 28 ust. 9 rozporządzenia (UE) 2022/2554.	Tak	Tak	Tak	Alfanumeryczne
1.4.	Rodzaj podmiotu finansowego, którego dotyczy incydent	Rodzaj podmiotu, o którym mowa w art. 2 ust. 1 lit. a)–t) rozporządzenia (UE) 2022/2554, w odniesieniu do którego przedkładane jest sprawozdanie. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, należy wybrać różne rodzaje podmiotów finansowych objętych sprawozdawczością zagregowaną.	Tak	Tak	Tak	Wybór (można wybrać więcej niż jedną opcję): — instytucja kredytowa; — instytucja płatnicza; — zwolniona instytucja płatnicza; — dostawca świadczący usługę dostępu do informacji o rachunku; — instytucja pieniądza elektronicznego; — zwolniona instytucja pieniądza elektronicznego; — firma inwestycyjna; — dostawca usług w zakresie kryptoaktywów; — emitent tokenów powiązanych z aktywami; — centralny depozyt papierów wartościowych; — kontrahent centralny; — system obrotu; — repozytorium transakcji;

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
						— zarządzający alternatywnym funduszem inwestycyjnym; — spółka zarządzająca; — dostawca usług w zakresie udostępniania informacji; — zakład ubezpieczeń i zakład reasekuracji; — pośrednik ubezpieczeniowy, pośrednik reasekuracyjny i pośrednik oferujący ubezpieczenia uzupełniające; — instytucja pracowniczych programów emerytalnych; — agencja ratingowa; — administrator kluczowych wskaźników referencyjnych; — dostawca usług finansowania społecznościowego; — repozytorium sekurytyzacji.
1.5.	Nazwa podmiotu finansowego, którego dotyczy incydent	Pełna nazwa prawna podmiotu finansowego, którego dotyczy poważny incydent związany z ICT i który jest zobowiązany do zgłoszenia poważnego incydentu swojemu właściwemu organowi na podstawie art. 19 rozporządzenia (UE) 2022/2554. W przypadku sprawozdawczości zagregowanej: a) wykaz wszystkich nazw podmiotów finansowych, których dotyczy poważny incydent związany z ICT, oddzielonych średnikiem. b) dostawca będący osobą trzecią, który przedkłada powiadomienie lub sprawozdanie dotyczące poważnego incydentu w sposób zagregowany określony w art. 7 niniejszego rozporządzenia, przedstawia wykaz nazw wszystkich podmiotów finansowych, których dotyczy incydent, oddzielonych średnikiem.	Tak, jeżeli podmiot finansowy, którego dotyczy incydent, jest inny niż podmiot przedkładający sprawozdanie oraz w przypadku sprawozdawczości zagregowanej.	Tak, jeżeli podmiot finansowy, którego dotyczy incydent, jest inny niż podmiot przedkładający sprawozdanie oraz w przypadku sprawozdawczości zagregowanej.	Tak, jeżeli podmiot finansowy, którego dotyczy incydent, jest inny niż podmiot przedkładający sprawozdanie oraz w przypadku sprawozdawczości zagregowanej.	Alfanumeryczne
1.6.	Kod LEI podmiotu finansowego, którego dotyczy incydent	Identyfikator podmiotu prawnego (LEI) podmiotu finansowego, którego dotyczy poważny incydent związany z ICT, przypisany zgodnie ze standardem Międzynarodowej Organizacji Normalizacyjnej. W przypadku sprawozdawczości zagregowanej: a) wykaz wszystkich kodów LEI podmiotów finansowych, których dotyczy poważny incydent związany z ICT, oddzielonych średnikiem;	Tak, jeżeli podmiot finansowy, którego dotyczy poważny incydent związany z ICT,	Tak, jeżeli podmiot finansowy, którego dotyczy poważny incydent związany z ICT, jest inny niż	Tak, jeżeli podmiot finansowy, którego dotyczy poważny incydent związany z ICT,	Niepowtarzalny kod składający się z 20 znaków alfanumerycznych, zgodnie z ISO 17442-1:2020

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	b) dostawca będący osobą trzecią, który przedkłada powiadomienie lub sprawozdanie dotyczące poważnego incydentu w sposób zagregowany określony w art. 7 niniejszego rozporządzenia, przedstawia wykaz kodów LEI wszystkich podmiotów finansowych, których dotyczy incydent, oddzielonych średnikiem. Kolejność podawania kodów LEI i nazw podmiotów finansowych musi być identyczna.	jest inny niż podmiot przedkładający sprawozdanie oraz w przypadku sprawozdawczości zagregowanej.	podmiot przedkładający sprawozdanie oraz w przypadku sprawozdawczości zagregowanej.	jest inny niż podmiot przedkładający sprawozdanie oraz w przypadku sprawozdawczości zagregowanej.	
1.7. Imię i nazwisko głównej osoby wyznaczonej do kontaktów	Imię i nazwisko głównej osoby wyznaczonej do kontaktów w podmiocie finansowym. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, imię i nazwisko głównej osoby wyznaczonej do kontaktów w podmiocie przedkładającym sprawozdanie zagregowane.	Tak	Tak	Tak	Alfanumeryczne
1.8. Adres e-mail głównej osoby wyznaczonej do kontaktów	Adres e-mail głównej osoby wyznaczonej do kontaktów, z którego właściwy organ może korzystać do celów dalszej komunikacji. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, adres e-mail głównej osoby wyznaczonej do kontaktów w podmiocie przedkładającym sprawozdanie zagregowane.	Tak	Tak	Tak	Alfanumeryczne
1.9. Numer telefonu głównej osoby wyznaczonej do kontaktów	Numer telefonu głównej osoby wyznaczonej do kontaktów, z którego właściwy organ może korzystać do celów dalszej komunikacji. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, numer telefonu głównej osoby wyznaczonej do kontaktów w podmiocie przedkładającym sprawozdanie zagregowane. Numer telefonu należy podać ze wszystkimi międzynarodowymi prefiksami (np. +33XXXXXXXXX).	Tak	Tak	Tak	Alfanumeryczne
1.10. Imię i nazwisko dodatkowej osoby wyznaczonej do kontaktów	Imię i nazwisko dodatkowej osoby wyznaczonej do kontaktów lub nazwa odpowiedzialnego zespołu podmiotu finansowego lub podmiotu przedkładającego sprawozdanie w imieniu podmiotu finansowego	Tak	Tak	Tak	Alfanumeryczne
1.11. Adres e-mail dodatkowej osoby wyznaczonej do kontaktów	Adres e-mail dodatkowej osoby wyznaczonej do kontaktów lub funkcjonalny adres e-mail zespołu, z których właściwy organ może korzystać do celów dalszej komunikacji.	Tak	Tak	Tak	Alfanumeryczne

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
1.12.	Numer telefonu dodatkowej osoby wyznaczonej do kontaktów	Numer telefonu dodatkowej osoby wyznaczonej do kontaktów lub numer telefonu zespołu, z których właściwy organ może korzystać do celów dalszej komunikacji. Numer telefonu należy podać ze wszystkimi międzynarodowymi prefiksami (np. +33XXXXXXXXX).	Tak	Tak	Tak	Alfanumeryczne
1.13.	Nazwa jednostki dominującej najwyższego szczebla	W stosownych przypadkach, nazwa jednostki dominującej najwyższego szczebla grupy, do której należy dany podmiot finansowy.	Tak, jeżeli podmiot finansowy należy do grupy.	Tak, jeżeli podmiot finansowy należy do grupy.	Tak, jeżeli podmiot finansowy należy do grupy.	Alfanumeryczne
1.14.	Kod LEI jednostki dominującej najwyższego szczebla	W stosownych przypadkach, kod LEI jednostki dominującej najwyższego szczebla grupy, do której należy dany podmiot finansowy. Kod przypisany zgodnie ze standardem Międzynarodowej Organizacji Normalizacyjnej.	Tak, jeżeli podmiot finansowy należy do grupy.	Tak, jeżeli podmiot finansowy należy do grupy.	Tak, jeżeli podmiot finansowy należy do grupy.	Niepowtarzalny kod składający się z 20 znaków alfanumerycznych, zgodnie z ISO 17442-1:2020
1.15.	Waluta sprawozdawcza	Waluta stosowana do zgłaszania incydentów	Tak	Tak	Tak	Wyboru należy dokonać przy użyciu kodów walut zgodnie z ISO 4217
Zawartość wstępnego powiadomienia						
2.1.	Kod referencyjny incydentu nadany przez podmiot finansowy	Niepowtarzalny kod referencyjny nadany przez podmiot finansowy, jednoznacznie identyfikujący poważny incydent związany z ICT. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, kod referencyjny incydentu nadany przez dostawcę będącego osobą trzecią.	Tak	Tak	Tak	Alfanumeryczne
2.2.	Data i godzina wykrycia incydentu związanego z ICT	Data i godzina, kiedy podmiot finansowy dowiedział się o incydencie związanym z ICT. W przypadku powtarzających się incydentów – data i godzina wykrycia ostatniego incydentu związanego z ICT.	Tak	Tak	Tak	Standard UTC zgodny z ISO 8601 (RRRR-MM-DD Thh: mm:ss)

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
2.3. Data i godzina sklasyfikowania incydentu jako poważny	Data i godzina sklasyfikowania incydentu związanego z ICT jako poważny zgodnie z kryteriami klasyfikacji ustanowionymi w rozporządzeniu delegowanym (UE) 2024/1772.	Tak	Tak	Tak	Standard UTC zgodny z ISO 8601 (RRRR-MM-DD Thh: mm:ss)
2.4. Opis incydentu związanego z ICT	Opis najistotniejszych aspektów poważnego incydentu związanego z ICT. Podmioty finansowe przedstawiają ogólny przegląd następujących informacji, takich jak możliwe przyczyny, bezpośrednie skutki, systemy, których dotyczy incydent, i inne. Podmioty finansowe uwzględniają, jeżeli to wiedzą lub mogą tego w uzasadniony sposób oczekiwać, czy incydent ma wpływ na dostawców będących osobami trzecimi lub inne podmioty finansowe, jak również rodzaj dostawcy lub podmiotu finansowego, ich nazwę, odpowiednie kody identyfikacyjne oraz rodzaj kodu identyfikacyjnego (np. LEI lub EUID). W kolejnych sprawozdaniach treści wpisywane do tego pola mogą z czasem ulec zmianie, aby odzwierciedlić aktualną wiedzę na temat incydentu związanego z ICT i opisać wszelkie inne istotne informacje na temat incydentu związanego z ICT, które nie zostały ujęte w polach danych, można przy tym uwzględnić wewnętrzną ocenę dotkliwości przeprowadzoną przez podmiot finansowy (np. bardzo niska, niska, średnia, wysoka, bardzo wysoka) oraz wskazać poziom i nazwę struktur decyzyjnych najwyższego stopnia, które były zaangażowane w reakcję na incydent związany z ICT.	Tak	Tak	Tak	Alfanumeryczne
2.5. Kryteria klasyfikacji, które doprowadziły do zgłoszenia incydentu	Kryteria klasyfikacji określone w rozporządzeniu delegowanym (UE) 2024/1772, które doprowadziły do uznania incydentu związanego z ICT za poważny oraz do późniejszego powiadomienia o nim i późniejszej sprawozdawczości na jego temat. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, kryteria klasyfikacji, które doprowadziły do uznania incydentu związanego z ICT za poważny, w odniesieniu do co najmniej jednego podmiotu finansowego.	Tak	Tak	Tak	Wybór (można wybrać więcej niż jedną opcję): — klienci, kontrahenci finansowi i transakcje, których dotyczy incydent; — skutki reputacyjne; — czas trwania incydentu i przerwa w świadczeniu usług; — zasięg geograficzny; — utrata danych; — usługi krytyczne, których dotyczy incydent; — skutki gospodarcze.
2.6. Progi istotności dla kryterium klasyfikacji „Zasięg geograficzny”	Państwa członkowskie EOG, których dotyczy poważny incydent związany z ICT Oceniając skutki poważnego incydentu związanego z ICT w innych państwach członkowskich, podmioty finansowe uwzględniają art. 4 i 12 rozporządzenia delegowanego (UE) 2024/1772.	Tak, jeżeli osiągnięto próg „Zasięg geograficzny”.	Tak, jeżeli osiągnięto próg „Zasięg geograficzny”.	Tak, jeżeli osiągnięto próg „Zasięg geograficzny”.	Wyboru (można wybrać więcej niż jedną opcję) należy dokonać przy użyciu zgodnego z normą ISO 3166 kodu ALPHA-2 państw, których dotyczy incydent.

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
2.7.	Wykrycie poważnego incydentu związanego z ICT	Wskazanie, w jaki sposób wykryto poważny incydent związany z ICT.	Tak	Tak	Tak	Wybór: — bezpieczeństwo informatyczne; — personel; — audyt wewnętrzny; — audyt zewnętrzny; — klienci; — kontrahenci finansowi; — dostawca usług będący osobą trzecią; — agresor; — systemy monitorowania; — organ/agencja/organ ścigania; — inne.
2.8.	Wskazanie, czy incydent wywodzi się od dostawcy będącego osobą trzecią lub innego podmiotu finansowego	Wskazanie, czy poważny incydent związany z ICT wywodzi się od dostawcy będącego osobą trzecią lub innego podmiotu finansowego. Podmioty finansowe wskazują, czy poważny incydent związany z ICT wywodzi się od dostawcy będącego osobą trzecią lub innego podmiotu finansowego (w tym od podmiotów finansowych należących do tej samej grupy co podmiot zgłaszający), a także podają nazwę i kod identyfikacyjny dostawcy będącego osobą trzecią lub podmiotu finansowego oraz rodzaj kodu identyfikacyjnego (np. LEI lub EUID).	Tak, jeżeli incydent wywodzi się od dostawcy będącego osobą trzecią lub innego podmiotu finansowego.	Tak, jeżeli incydent wywodzi się od dostawcy będącego osobą trzecią lub innego podmiotu finansowego.	Tak, jeżeli incydent wywodzi się od dostawcy będącego osobą trzecią lub innego podmiotu finansowego.	Alfanumeryczne
2.9.	Uruchomienie planu ciągłości działania, jeżeli plan został uruchomiony	Wskazanie, czy podmiot finansowy formalnie uruchomił środki reagowania w zakresie ciągłości działania.	Tak	Tak	Tak	Wartość logiczna (Tak albo Nie)
2.10.	Inne istotne informacje	Wszelkie dodatkowe informacje nieuwzględnione we wzorze. Podmioty finansowe, które przeklasyfikowały poważny incydent związany z ICT jako inny niż poważny, opisują powody, dla których incydent związany z ICT nie spełnia kryteriów uznania za poważny incydent związany z ICT i dla których nie oczekuje się ich spełnienia.	Tak, jeżeli istnieją inne informacje nieuwzględnione we wzorze lub	Tak, jeżeli istnieją inne informacje nieuwzględnione we wzorze lub jeżeli poważny	Tak, jeżeli istnieją inne informacje nieuwzględnione we wzorze lub	Alfanumeryczne

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
			jeżeli poważny incydent związany z ICT został przeklasyfikowany jako inny niż poważny.	incydent związany z ICT został przeklasyfikowany jako inny niż poważny.	jeżeli poważny incydent związany z ICT został przeklasyfikowany jako inny niż poważny.	
Zawartość sprawozdania śródokresowego						
3.1.	Kod referencyjny incydentu podany przez właściwy organ	Niepowtarzalny kod referencyjny nadany przez właściwy organ w momencie otrzymania wstępnego powiadomienia w celu jednoznacznej identyfikacji poważnego incydentu związanego z ICT.	Nie	Tak, w stosownych przypadkach.	Tak, w stosownych przypadkach.	Alfanumeryczne
3.2.	Data i godzina wystąpienia incydentu	Data i godzina wystąpienia poważnego incydentu związanego z ICT, jeżeli różnią się od daty i godziny, kiedy podmiot finansowy dowiedział się o poważnym incydencie związanym z ICT. W przypadku powtarzających się poważnych incydentów związanych z ICT – data i godzina wystąpienia ostatniego poważnego incydentu związanego z ICT.	Nie	Tak	Tak	Standard UTC zgodny z ISO 8601 (RRRR-MM-DD Thh: mm:ss)
3.3.	Data i godzina przywrócenia usług, działań lub operacji	Informacja o dacie i godzinie przywrócenia usług, działań lub operacji, na które wpłynął poważny incydent związany z ICT.	Nie	Tak, jeżeli wypełniono pole danych 3.16. „Przerwa w świadczeniu usług”.	Tak, jeżeli wypełniono pole danych 3.16. „Przerwa w świadczeniu usług”.	Standard UTC zgodny z ISO 8601 (RRRR-MM-DD Thh: mm:ss)
3.4.	Liczba klientów, których dotyczy incydent	Liczba klientów, których dotyczy poważny incydent związany z ICT, korzystających z usługi świadczonej przez podmiot finansowy. Oceniając liczbę klientów, których dotyczy incydent, podmioty finansowe uwzględniają w swojej ocenie art. 1 ust. 1 i art. 9 ust. 1 lit. b) rozporządzenia delegowanego (UE) 2024/1772. Podmiot finansowy, który nie może określić faktycznej liczby klientów, których dotyczy incydent, stosuje szacunki oparte na dostępnych danych pochodzących z porównywalnych okresów odniesienia. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, łączna liczba klientów, których dotyczy incydent, we wszystkich podmiotach finansowych.	Nie	Tak	Tak	Liczba całkowita

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
3.5.	Odsetek klientów, których dotyczy incydent	Odsetek klientów, których dotyczy poważny incydent związany z ICT, w stosunku do łącznej liczby klientów korzystających z usługi świadczonej przez podmiot finansowy, której dotyczy incydent. W przypadku więcej niż jednej usługi, której dotyczy incydent, usługi podaje się w sposób zagregowany. Podmioty finansowe uwzględniają w swojej ocenie art. 1 ust. 1 i art. 9 ust. 1 lit. a) rozporządzenia delegowanego (UE) 2024/1772. Podmiot finansowy, który nie może określić faktycznego odsetka klientów, których dotyczy incydent, stosuje szacunki oparte na dostępnych danych pochodzących z porównywalnych okresów odniesienia. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, podmiot finansowy dzieli sumę wszystkich klientów, których dotyczy incydent, przez łączną liczbę klientów wszystkich podmiotów finansowych, których dotyczy incydent.	Nie	Tak	Tak	Jeśli pozycja ta jest wyrażona jako wartość procentowa – dowolna wartość do 5 znaków numerycznych, w tym do 1 miejsca po przecinku, wyrażona jako odsetek (np. 2,4 zamiast 2,4 %). Jeśli wartość ma więcej niż 1 cyfrę po przecinku, kontrahenci dokonujący zgłoszenia zaokrąglają wartość w górę.
3.6.	Liczba kontrahentów finansowych, których dotyczy incydent	Liczba kontrahentów finansowych, których dotyczy incydent związany z ICT, którzy zawarli umowę z podmiotem finansowym. Oceniając liczbę kontrahentów finansowych, których dotyczy incydent, podmioty finansowe uwzględniają w swojej ocenie art. 1 ust. 2 rozporządzenia delegowanego (UE) 2024/1772. Podmiot finansowy, który nie może określić faktycznej liczby kontrahentów finansowych, których dotyczy incydent, stosuje szacunki oparte na dostępnych danych pochodzących z porównywalnych okresów odniesienia. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, łączna liczba kontrahentów finansowych, których dotyczy incydent, we wszystkich podmiotach finansowych.	Nie	Tak	Tak	Liczba całkowita

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
3.7.	Odsetek kontrahentów finansowych, których dotyczy incydent	Odsetek kontrahentów finansowych, których dotyczy incydent związany z ICT, w stosunku do łącznej liczby kontrahentów finansowych, którzy zawarli umowę z podmiotem finansowym. Oceniając odsetek kontrahentów finansowych, których dotyczy incydent, podmioty finansowe uwzględniają w swojej ocenie art. 1 ust. 1 i art. 9 ust. 1 lit. c) rozporządzenia delegowanego (UE) 2024/1772. Podmiot finansowy, który nie może określić faktycznego odsetka kontrahentów finansowych, których dotyczy incydent, stosuje szacunki oparte na dostępnych danych pochodzących z porównywalnych okresów odniesienia. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, należy wskazać sumę wszystkich kontrahentów finansowych, których dotyczy incydent, podzieloną przez łączną liczbę kontrahentów finansowych wszystkich podmiotów finansowych, których dotyczy incydent.	Nie	Tak	Tak	Jeśli pozycja ta jest wyrażona jako wartość procentowa – dowolna wartość do 5 znaków numerycznych, w tym do 1 miejsca po przecinku, wyrażona jako odsetek (np. 2,4 zamiast 2,4 %). Jeśli wartość ma więcej niż 1 cyfrę po przecinku, kontrahenci dokonujący zgłoszenia zaokrąglają wartość w górę.
3.8.	Skutki dla odpowiednich klientów lub kontrahentów finansowych	Wszelkie rozpoznane skutki dla odpowiednich klientów lub kontrahentów finansowych, o których mowa w art. 1 ust. 3 i art. 9 ust. 1 lit. f) rozporządzenia delegowanego (UE) 2024/1772.	Nie	Tak, jeżeli osiągnięto próg „Znaczenie klientów i kontrahentów finansowych”.	Tak, jeżeli osiągnięto próg „Znaczenie klientów i kontrahentów finansowych”.	Wartość logiczna (Tak albo Nie)
3.9.	Liczba transakcji, których dotyczy incydent	Liczba transakcji, których dotyczy poważny incydent związany z ICT. Oceniając wpływ na transakcje, podmioty finansowe uwzględniają art. 1 ust. 4 rozporządzenia delegowanego (UE) 2024/1772, w tym wszystkie obejmujące kwotę pieniężną transakcje krajowe i transgraniczne, których dotyczy incydent, w przypadku których co najmniej jedna część transakcji została przeprowadzona w Unii.	Nie	Tak, jeżeli incydent wywarł wpływ na jakąkolwiek transakcję.	Tak, jeżeli incydent wywarł wpływ na jakąkolwiek transakcję.	Liczba całkowita

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
		Podmiot finansowy, który nie może określić faktycznej liczby transakcji, których dotyczy incydent, stosuje szacunki oparte na dostępnych danych pochodzących z porównywalnych okresów odniesienia. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, należy podać całkowitą liczbę transakcji, których dotyczy incydent, we wszystkich podmiotach finansowych.				
3.10.	Odsetek transakcji, których dotyczy incydent	Odsetek transakcji, których dotyczy incydent, w stosunku do średniej dziennej liczby transakcji krajowych i transgranicznych przeprowadzanych przez podmiot finansowy w związku z usługą, której dotyczy incydent. Podmioty finansowe uwzględniają art. 1 ust. 4 i art. 9 ust. 1 lit. d) rozporządzenia delegowanego (UE) 2024/1772. Podmiot finansowy, który nie może określić faktycznego odsetka transakcji, na które incydent wywarł wpływ, stosuje szacunki. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, podmiot finansowy sumuje liczbę wszystkich transakcji, których dotyczy incydent, i dzieli tę sumę przez całkowitą liczbę transakcji wszystkich podmiotów finansowych, których dotyczy incydent.	Nie	Tak, jeżeli incydent wywarł wpływ na jakąkolwiek transakcję.	Tak, jeżeli incydent wywarł wpływ na jakąkolwiek transakcję.	Jeśli pozycja ta jest wyrażona jako wartość procentowa – dowolna wartość do 5 znaków numerycznych, w tym do 1 miejsca po przecinku, wyrażona jako odsetek (np. 2,4 zamiast 2,4 %). Jeśli wartość ma więcej niż 1 cyfrę po przecinku, kontrahenci dokonujący zgłoszenia zaokrąglają wartość w górę.
3.11.	Wartość transakcji, których dotyczy incydent	Całkowitą wartość transakcji, których dotyczy poważny incydent związany z ICT, ocenia się zgodnie z art. 1 ust. 4 i art. 9 ust. 1 lit. e) rozporządzenia delegowanego (UE) 2024/1772. Podmiot finansowy, który nie może określić faktycznej wartości transakcji, których dotyczy incydent, stosuje szacunki oparte na dostępnych danych pochodzących z porównywalnych okresów odniesienia. Podmiot finansowy wykazuje kwotę pieniężną jako wartość dodatnią. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, całkowita wartość transakcji, których dotyczy incydent, we wszystkich podmiotach finansowych.	Nie	Tak, jeżeli incydent wywarł wpływ na jakąkolwiek transakcję.	Tak, jeżeli incydent wywarł wpływ na jakąkolwiek transakcję.	Wartość pieniężna Podmioty finansowe przedstawiają punkt danych w jednostkach, stosując minimalną dokładność odpowiadającą tysiącom jednostek (np. 2,5 zamiast 2 500 EUR).

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
3.12.	Informacja, czy dane liczbowe są rzeczywiste czy szacunkowe, lub czy nie wystąpiły jakiekolwiek skutki	Informacja, czy wartości podane w polach danych od 3.4 do 3.11 są rzeczywiste czy szacunkowe, lub czy nie wystąpiły jakiekolwiek skutki.	Nie	Tak	Tak	Wybór (można wybrać więcej niż jedną opcję): — rzeczywiste dane liczbowe dotyczące klientów, których dotyczy incydent; — rzeczywiste dane dotyczące kontrahentów finansowych, których dotyczy incydent; — rzeczywiste dane liczbowe dotyczące transakcji, których dotyczy incydent; — szacunki dotyczące klientów, których dotyczy incydent; — szacunki dotyczące kontrahentów finansowych, których dotyczy incydent; — szacunki dotyczące transakcji, których dotyczy incydent; — brak skutków dla klientów; — brak skutków dla kontrahentów finansowych; — brak skutków dla transakcji.
3.13.	Skutki reputacyjne	Informacje na temat skutków reputacyjnych wynikających z poważnego incydentu związanego z ICT, o których mowa w art. 2 i 10 rozporządzenia delegowanego (UE) 2024/1772. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, kategorie skutków reputacyjnych, które mają zastosowanie do co najmniej jednego podmiotu finansowego.	Nie	Tak, jeżeli spełniono kryterium „Skutki reputacyjne”.	Tak, jeżeli spełniono kryterium „Skutki reputacyjne”.	Wybór (można wybrać więcej niż jedną opcję): — poważny incydent związany z ICT został opisany w mediach; — poważny incydent związany z ICT doprowadził do powtarzających się skarg ze strony różnych klientów lub kontrahentów finansowych dotyczących usług ukierunkowanych na klienta lub krytycznych relacji biznesowych; — w wyniku poważnego incydentu związanego z ICT podmiot finansowy nie będzie w stanie lub prawdopodobnie nie będzie w stanie spełnić wymogów regulacyjnych; — w wyniku poważnego incydentu związanego z ICT podmiot finansowy utraci lub prawdopodobnie utraci klientów lub kontrahentów finansowych, co będzie miało istotny wpływ na jego działalność.
3.14.	Informacje kontekstowe na temat skutków reputacyjnych	Informacje opisujące, w jaki sposób poważny incydent związany z ICT wpłynął lub może wpłynąć na reputację podmiotu finansowego, w tym naruszenia prawa, niespełnione wymogi regulacyjne, liczba skarg klientów i inne.	Nie	Tak, jeżeli spełniono kryterium „Skutki reputacyjne”.	Tak, jeżeli spełniono kryterium „Skutki reputacyjne”.	Alfanumeryczne

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	Informacje kontekstowe obejmują rodzaj mediów (np. media tradycyjne i cyfrowe, blogi, platformy transmisji strumieniowej) oraz relacje medialne, w tym zasięg mediów (lokalne, krajowe, międzynarodowe). Relacje medialne w tym kontekście nie oznaczają kilku negatywnych komentarzy osób obserwujących lub użytkowników sieci społecznościowych. Podmiot finansowy wskazuje również, czy w relacjach medialnych zwrócono uwagę na istotne ryzyko dla jego klientów w związku z poważnym incydentem związanym z ICT, w tym ryzyko niewypłacalności podmiotu finansowego lub ryzyko utraty środków finansowych. Podmioty finansowe wskazują również, czy przekazały mediom informacje, które służyły wiarygodnemu informowaniu opinii publicznej o poważnym incydencie związanym z ICT i jego konsekwencjach. Podmioty finansowe mogą również wskazać, czy w mediach pojawiały się fałszywe informacje dotyczące incydentu związanego z ICT, w tym informacje oparte na informacjach celowo wprowadzających w błąd rozpowszechnianych przez agresorów lub informacje dotyczące ataku typu *defacement* na stronę internetową podmiotu finansowego lub informacje ilustrujące taki atak.				
3.15. Czas trwania incydentu	Podmioty finansowe mierzą czas trwania poważnego incydentu związanego z ICT od momentu wystąpienia poważnego incydentu związanego z ICT do momentu zaradzenia temu incydentowi. Podmioty finansowe, które nie są w stanie określić momentu wystąpienia poważnego incydentu związanego z ICT, mierzą czas trwania poważnego incydentu związanego z ICT od wcześniejszego z następujących momentów: momentu wykrycia incydentu przez podmiot finansowy lub momentu zarejestrowania incydentu w dzienniku sieciowym lub systemowym lub w innych źródłach danych. Podmioty finansowe, które nie wiedzą jeszcze, kiedy uda się zaradzić poważnemu incydentowi związanemu z ICT, stosują oszacowania. Wartość wyraża się w dniach, godzinach i minutach. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, jeżeli między podmiotami finansowymi występują różnice, podmioty finansowe mierzą najdłuższy czas trwania poważnego incydentu związanego z ICT.	Nie	Tak	Tak	DD:HH:MM

	Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
3.16.	Przerwa w świadczeniu usług	Przerwa w świadczeniu usług mierzona od momentu, gdy usługa staje się w pełni lub częściowo niedostępna dla klientów, kontrahentów finansowych lub innych użytkowników wewnętrznych lub zewnętrznych, do momentu przywrócenia regularnych działań lub operacji do poziomu usługi świadczonej przed wystąpieniem poważnego incydentu związanego z ICT. W przypadku gdy przerwa w świadczeniu usług powoduje opóźnienie w świadczeniu usługi po przywróceniu regularnych działań lub operacji, podmioty finansowe mierzą czas przestoju od początku poważnego incydentu związanego z ICT do momentu, w którym usługa, w przypadku której wystąpiło opóźnienie, jest świadczona. Podmioty finansowe, które nie są w stanie określić momentu rozpoczęcia przerwy w świadczeniu usług, mierzą przerwę w świadczeniu usług od wcześniejszego z następujących momentów: momentu wykrycia incydentu lub momentu jego zarejestrowania. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, jeżeli między podmiotami finansowymi występują różnice, podmioty finansowe mierzą najdłuższy czas trwania przerwy w świadczeniu usług.	Nie	Tak, jeżeli incydent spowodował przerwę w świadczeniu usług.	Tak, jeżeli incydent spowodował przerwę w świadczeniu usług.	DD:HH:MM
3.17.	Informacja, czy dane liczbowe dotyczące czasu trwania incydentu i przerwy w świadczeniu usług są rzeczywiste czy szacunkowe	Informacja, czy wartości podane w polach danych 3.15 i 3.16 są rzeczywiste czy szacunkowe.	Nie	Tak, jeżeli spełniono kryterium „Czas trwania incydentu i przerwa w świadczeniu usług”.	Tak, jeżeli spełniono kryterium „Czas trwania incydentu i przerwa w świadczeniu usług”.	Wybór: — rzeczywiste dane liczbowe; — szacunki — rzeczywiste dane liczbowe i szacunki; — brak informacji.
3.18.	Rodzaje skutków w państwach członkowskich	Rodzaj skutków w odpowiednich państwach członkowskich EOG. Wskazanie, czy skutki poważnego incydentu związanego z ICT są lub były odczuwalne w innych państwach członkowskich EOG (innych niż państwo członkowskie właściwego organu, któremu incydent jest bezpośrednio zgłaszany), zgodnie z art. 4 rozporządzenia delegowanego (UE) 2024/1772, w szczególności w odniesieniu do znaczenia skutków dla: a) klientów i kontrahentów finansowych, których dotyczy incydent, w innych państwach członkowskich; lub	Nie	Tak, jeżeli osiągnięto próg „Zasięg geograficzny”.	Tak, jeżeli osiągnięto próg „Zasięg geograficzny”.	Wybór (można wybrać więcej niż jedną opcję): — klienci; — kontrahenci finansowi — oddział podmiotu finansowego; — podmioty finansowe należące do grupy prowadzące działalność w danym państwie członkowskim; — infrastruktura rynków finansowych; — dostawcy będący osobami trzecimi, którzy mogą świadczyć usługi na rzecz innych podmiotów finansowych.

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	b) oddziałów lub innych podmiotów finansowych należących do grupy prowadzących działalność w innych państwach członkowskich; lub c) infrastruktur rynków finansowych lub dostawców będących osobami trzecimi, mogących mieć wpływ na podmioty finansowe w innych państwach członkowskich, na rzecz których świadczą usługi.				
3.19. Opis skutków incydentu w innych państwach członkowskich	Opis skutków i dotkliwości poważnego incydentu związanego z ICT w każdym państwie członkowskim, którego dotyczy incydent, w tym ocena skutków i dotkliwości dla: a) klientów; b) kontrahentów finansowych; c) oddziałów podmiotu finansowego; d) innych podmiotów finansowych należących do grupy prowadzących działalność w danym państwie członkowskim; e) infrastruktur rynków finansowych; f) dostawców będących osobami trzecimi, którzy mogą świadczyć usługi na rzecz innych podmiotów finansowych, stosownie do przypadku w innym państwie członkowskim (innych państwach członkowskich).	Nie	Tak, jeżeli osiągnięto próg „Zasięg geograficzny”.	Tak, jeżeli osiągnięto próg „Zasięg geograficzny”.	Alfanumeryczne
3.20. Progi istotności dla kryterium klasyfikacji „Utrata danych”	Rodzaj utraty danych w wyniku poważnego incydentu związanego z ICT w kontekście dostępności, autentyczności, integralności i poufności danych. Podmioty finansowe uwzględniają w swojej ocenie art. 5 i 13 rozporządzenia delegowanego (UE) 2024/1772. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, utrata danych dotycząca co najmniej jednego podmiotu finansowego.	Nie	Tak, jeżeli spełniono kryterium „Utrata danych”.	Tak, jeżeli spełniono kryterium „Utrata danych”.	Wybór (można wybrać więcej niż jedną opcję): — dostępność; — autentyczność; — integralność; — poufność.
3.21. Opis utraty danych	Opis wpływu poważnego incydentu związanego z ICT na dostępność, autentyczność, integralność i poufność danych krytycznych zgodnie z art. 5 i 13 rozporządzenia delegowanego (UE) 2024/1772. Informacje na temat wpływu na osiąganie celów biznesowych podmiotu finansowego lub na spełnienie wymogów regulacyjnych. W ramach przekazywanych informacji podmioty finansowe wskazują, czy dane, których dotyczy incydent, to dane dotyczące klientów, dane dotyczące innych podmiotów (np. kontrahentów finansowych) czy dane dotyczące samego podmiotu finansowego.	Nie	Tak, jeżeli spełniono kryterium „Utrata danych”.	Tak, jeżeli spełniono kryterium „Utrata danych”.	Alfanumeryczne

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	Podmiot finansowy może również wskazać rodzaj danych związanych z incydentem – w szczególności, czy dane są poufne i jakim rodzajem poufności są objęte dane (np. poufność informacji handlowych/tajemnica przedsiębiorstwa, dane osobowe, tajemnica zawodowa: tajemnica bankowa, tajemnica ubezpieczeniowa, tajemnica usług płatniczych itp.). Informacje te mogą również obejmować ewentualne ryzyko związane z utratą danych, na przykład, czy dane, których dotyczy incydent, można wykorzystać do identyfikacji osób fizycznych oraz czy agresor może użyć tych danych do uzyskania kredytu lub pożyczki bez zgody tych osób, do przeprowadzenia profilowanego phishingu, do publicznego ujawnienia informacji. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, ogólny opis wpływu incydentu na podmioty finansowe, których dotyczy incydent. Jeżeli występują różnice w skutkach, w opisie wpływu należy wyraźnie określić konkretny wpływ na poszczególne podmioty finansowe.				
3.22. Kryterium klasyfikacji „Usługi krytyczne, których dotyczy incydent”	Informacje dotyczące kryterium „Usługi krytyczne, których dotyczy incydent”. Podmioty finansowe uwzględniają w swojej ocenie art. 6 rozporządzenia delegowanego (UE) 2024/1772, w tym informacje dotyczące: — usług lub rodzajów działalności, których dotyczy incydent, które wymagają zezwolenia, rejestracji lub są nadzorowane przez właściwe organy; lub — usług ICT lub sieci i systemów informatycznych, które wspierają krytyczne lub istotne funkcje podmiotu finansowego; oraz — charakteru złośliwego i nieuprawnionego dostępu do sieci i systemów informatycznych podmiotu finansowego. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, wpływ na usługi krytyczne, które mają zastosowanie do co najmniej jednego podmiotu finansowego.	Nie	Tak	Tak	Alfanumeryczne

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
3.23.	Rodzaj incydentu	Klasyfikacja incydentów według rodzaju.	Nie	Tak	Tak	Wybór (można wybrać więcej niż jedną opcję): — incydent związany z cyberbezpieczeństwem; — awaria procesu; — awaria systemu; — zdarzenie zewnętrzne — incydent związany z płatnością; — inny (proszę określić).
3.24.	Inne rodzaje incydentów	Inne rodzaje incydentów związanych z ICT: podmioty finansowe, które wybrały „inny” rodzaj incydentów w polu danych 3.23, określają rodzaj incydentu związanego z ICT.	Nie	Tak, jeżeli w polu danych 3.23 wybrano „inny” rodzaj incydentów.	Tak, jeżeli w polu danych 3.23 wybrano „inny” rodzaj incydentów.	Alfanumeryczne
3.25.	Zagrożenia i techniki stosowane przez agresora	Należy wskazać zagrożenia i techniki stosowane przez agresora, w tym: a) inżynierię społeczną, w tym phishing; b) (D)DoS; c) kradzież tożsamości; d) szyfrowanie danych na potrzeby ataku, w tym oprogramowanie szantażujące; e) bezprawne zawładnięcie zasobami; f) eksfiltrację danych i manipulację danymi, z wyłączeniem kradzieży tożsamości; g) niszczenie danych; h) atak typu *defacement*; i) atak na łańcuch dostaw; j) inne (proszę określić).	Nie	Tak, jeżeli w polu 3.23 wybrano rodzaj incydentu związanego z ICT „incydent związany z cyberbezpieczeństwem”.	Tak, jeżeli w polu 3.23 wybrano rodzaj incydentu związanego z ICT „incydent związany z cyberbezpieczeństwem”.	Wybór (można wybrać więcej niż jedną opcję): — inżynieria społeczna (w tym phishing); — (D)DoS; — kradzież tożsamości; — szyfrowanie danych na potrzeby ataku, w tym oprogramowanie szantażujące; — bezprawne zawładnięcie zasobami; — eksfiltracja danych i manipulacja danymi, w tym kradzież tożsamości; — niszczenie danych; — atak typu *defacement* — atak na łańcuch dostaw; — inne (proszę określić).
3.26.	Inne rodzaje technik	Inne rodzaje technik Podmioty finansowe, które wybrały „inny” rodzaj technik w polu danych 3.25, określają rodzaj techniki.	Nie	Tak, jeżeli w polu danych 3.25 wybrano „inny” rodzaj technik.	Tak, jeżeli w polu danych 3.25 wybrano „inny” rodzaj technik.	Alfanumeryczne

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
3.27. Informacje na temat obszarów funkcjonalnych i procesów biznesowych, których dotyczy incydent	Wskazanie obszarów funkcjonalnych i procesów biznesowych, których dotyczy incydent, w tym produktów i usług. Obszary funkcjonalne obejmują między innymi: a) marketing i rozwój działalności gospodarczej; b) obsługę klientów; c) zarządzanie produktem; d) przestrzeganie przepisów; e) zarządzanie ryzykiem; f) finanse i rachunkowość; g) usługi w zakresie zasobów kadrowych i usługi ogólne; h) technologie informacyjne. Procesy biznesowe obejmują między innymi: — dostęp do informacji o rachunku; — usługi aktuarialne; — usługi acquiringu transakcji płatniczych; — uwierzytelnianie/autoryzację; — onboarding organu/klienta; — zarządzanie świadczeniami; — zarządzanie wypłatą świadczeń; — zakup i sprzedaż pakietów polis ubezpieczeniowych między zakładami ubezpieczeń; — płatności kartą; — zarządzanie środkami pieniężnymi; — lokaty lub wypłaty środków pieniężnych; — obsługa roszczeń ubezpieczeniowych; — proces dochodzenia roszczeń ubezpieczeniowych; — rozliczenia; — konglomeraty kredytów korporacyjnych; — ubezpieczenia zbiorowe; — polecenia przelewu; — przechowywanie aktywów; — onboarding klientów; — przyjmowanie danych, — przetwarzanie danych; — polecenia zapłaty; — ubezpieczenia eksportowe; — finalizowanie transakcji/umów; — subemisja instrumentów finansowych; — rachunkowość na potrzeby funduszu; — pieniądze na rynku walutowym;	Nie	Tak	Tak	Alfanumeryczne

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	— doradztwo inwestycyjne; — zarządzanie inwestycjami, — wydawanie instrumentów płatniczych; — zarządzanie kredytami; — proces płatności z tytułu ubezpieczeń na życie; — usługi przekazu pieniężnego; — obliczanie aktywów netto; — zlecenie; — inicjowanie płatności; — zawieranie umów ubezpieczenia; — zarządzanie portfelem; — pobieranie składek; — przyjmowanie/przekazywanie/wykonywanie; — reasekuracja; — rozrachunek; — monitorowanie transakcji. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, obszary funkcjonalne i procesy biznesowe, których dotyczy incydent, w co najmniej jednym podmiocie finansowym.				
3.28. Elementy infrastruktury wspierające procesy biznesowe, których to elementów dotyczy incydent	Informacja, czy poważny incydent związany z ICT wpłynął na elementy infrastruktury (serwery, systemy operacyjne, oprogramowanie, serwery aplikacji, oprogramowanie pośredniczące, elementy sieci, inne) wspierające procesy biznesowe.	Nie	Tak	Tak	Wybór: — Tak — Nie — Brak informacji
3.29. Informacje na temat elementów infrastruktury wspierających procesy biznesowe, których to elementów dotyczy incydent	Opis wpływu poważnego incydentu związanego z ICT na elementy infrastruktury wspierające procesy biznesowe, w tym sprzęt i oprogramowanie. Sprzęt obejmuje serwery, komputery, ośrodki przetwarzania danych, przełączniki, routery, centra obsługi. Oprogramowanie obejmuje systemy operacyjne, aplikacje, bazy danych, narzędzia zapewniające bezpieczeństwo, elementy sieci, inne (należy określić). W opisach tych należy opisać lub wymienić elementy lub systemy infrastruktury, których dotyczy incydent, oraz, jeżeli są dostępne: a) informacje na temat wersji; b) infrastruktura wewnętrzna/częściowo zlecana na zewnątrz/całkowicie zlecana na zewnątrz – nazwa dostawcy będącego osobą trzecią;	Nie	Tak, jeżeli incydent wpłynął na elementy infrastruktury wspierające procesy biznesowe.	Tak, jeżeli incydent wpłynął na elementy infrastruktury wspierające procesy biznesowe.	Alfanumeryczne

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
		c) czy infrastruktura jest wspólnie wykorzystywana lub dzielona przez różne funkcje biznesowe; d) obowiązujące odpowiednie ustalenia dotyczące odporności/ciągłości/odzyskiwania/substytucyjności.				
3.30.	Wpływ na interesy finansowe klientów	Informacja, czy poważny incydent związany z ICT wpłynął na interesy finansowe klientów.	Nie	Tak	Tak	Wybór: — Tak; — Nie; — Brak informacji.
3.31.	Składanie sprawozdań innym organom	Określenie, które organy zostały poinformowane o poważnym incydencie związanym z ICT. Biorąc pod uwagę różnice wynikające z przepisów krajowych państw członkowskich, podmioty finansowe powinny rozumieć pojęcie organów ścigania szeroko – jako obejmujące organy publiczne uprawnione do ścigania cyberprzestępstw, w tym policję, organy ścigania i prokuratorów.	Nie	Tak	Tak	Wybór (można wybrać więcej niż jedną opcję): — policja/organy ścigania; — CSIRT; — organ ochrony danych; — krajowa agencja ds. cyberbezpieczeństwa; — żadne; — inne (proszę określić).
3.32.	Określenie „innych" organów	Określenie „innych" rodzajów organów informowanych o poważnym incydencie związanym z ICT. Jeżeli w polu danych 3.31 wybrano „inne", w opisie należy zawrzeć bardziej szczegółowe informacje na temat organu, któremu podmiot finansowy przekazał informacje na temat poważnego incydentu związanego z ICT.	Nie	Tak, jeżeli podmiot finansowy poinformował „inny" rodzaj organów o poważnym incydencie związanym z ICT.	Tak, jeżeli podmiot finansowy poinformował „inny" rodzaj organów o poważnym incydencie związanym z ICT.	Alfanumeryczne
3.33.	Tymczasowe działania/środki podjęte lub planowane w celu przywrócenia sytuacji sprzed incydentu	Wskazanie, czy podmiot finansowy wdrożył (lub planuje wdrożyć) jakiekolwiek tymczasowe działania, które podjęto (lub planuje się podjąć) w celu przywrócenia sytuacji sprzed poważnego incydentu związanego z ICT.	Nie	Tak	Tak	Wartość logiczna (Tak albo Nie)

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
3.34.	Opis wszelkich tymczasowych działań i środków podjętych lub planowanych w celu przywrócenia sytuacji sprzed incydentu	W informacjach tych należy opisać natychmiast podjęte działania, w tym odizolowanie incydentu na poziomie sieci, uruchomione procedury obejścia problemu, zablokowane porty USB, uruchomienie ośrodka odtwarzania danych po awarii systemu, wszelkie inne wprowadzone tymczasowo dodatkowe środki kontroli w zakresie ochrony. Podmioty finansowe podają datę i godzinę wdrożenia działań tymczasowych oraz przewidywaną datę powrotu do głównego miejsca przetwarzania danych. W przypadku wszelkich działań tymczasowych, które nie zostały wdrożone, ale są nadal planowane, należy podać oczekiwany termin ich wdrożenia. Jeżeli nie podjęto żadnych działań/środków tymczasowych, należy podać powód.	Nie	Tak, jeżeli podjęto działania/środki tymczasowe lub planuje się ich podjęcie (pole danych 3.33).	Tak, jeżeli podjęto działania/środki tymczasowe lub planuje się ich podjęcie (pole danych 3.33).	Alfanumeryczne
3.35.	Oznaki naruszenia integralności systemu	W stosownych przypadkach, informacje dotyczące poważnego incydentu związanego z ICT, które mogą pomóc w identyfikowaniu szkodliwych działań w ramach sieci lub systemu informatycznego (oznaki naruszenia integralności systemu). Pole to ma zastosowanie wyłącznie do tych podmiotów finansowych, które są objęte zakresem stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 ([1]), oraz, w stosownych przypadkach, do podmiotów finansowych zidentyfikowanych jako podmioty kluczowe lub ważne zgodnie z przepisami krajowymi transponującymi art. 3 dyrektywy (UE) 2022/2555. Oznaki naruszenia integralności systemu zgłaszane przez podmiot finansowy obejmują następujące kategorie danych: a) adresy IP; b) adresy URL; c) domeny; d) hasze plików; e) dane dotyczące złośliwego oprogramowania (nazwa złośliwego oprogramowania, nazwy plików i ich lokalizacje, konkretne klucze rejestrów związane z działaniem złośliwego oprogramowania); f) dane dotyczące działania sieci (porty, protokoły, adresy, odesłania, aplikacje klienckie, nagłówki, konkretne rejestry lub odmienne schematy ruchu w sieci); g) dane dotyczące wiadomości e-mail (nadawca, odbiorca, temat, nagłówek, treść);	Nie	Tak, jeżeli w polu danych 3.23 jako rodzaj incydentu wybrano „incydent związany z cyberbezpieczeństwem”.	Tak, jeżeli w polu danych 3.23 jako rodzaj incydentu wybrano „incydent związany z cyberbezpieczeństwem”.	Alfanumeryczne

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	h) wnioski DNS i konfiguracje rejestrów; i) czynności związane z kontem użytkownika (loginy, uprzywilejowana działalność związana z kontem użytkownika, eskalacja uprzywilejowania); j) ruch w bazach danych (odczyt/zapis), wnioski o dostęp do tego samego pliku. W praktyce tego rodzaju informacje mogą obejmować dane dotyczące m.in. wskaźników opisujących schematy ruchu w sieci odpowiadające znanym atakom/znanej komunikacji w sieci urządzeń zainfekowanych złośliwym oprogramowaniem, adresy IP urządzeń zainfekowanych złośliwym oprogramowaniem (boty), dane dotyczące serwerów „dowodzenia i kontroli" wykorzystywanych przez złośliwe oprogramowanie (zazwyczaj domeny lub adresy IP) oraz adresy URL dotyczące stron typu phishing lub obserwowanych stron internetowych, na których znajdują się złośliwe oprogramowanie lub narzędzia typu *exploit kit*.				
Zawartość sprawozdania końcowego					
4.1. Ogólna klasyfikacja przyczyn źródłowych incydentu	Ogólna klasyfikacja przyczyn źródłowych poważnego incydentu związanego z ICT w ramach rodzajów incydentów, w tym następujące kategorie ogólne: a) złośliwe działania; b) awaria procesu; c) awaria/nieprawidłowe działanie systemu; d) błąd ludzki; e) zdarzenie zewnętrzne.	Nie	Nie	Tak	Wybór (można wybrać więcej niż jedną opcję): — złośliwe działania; — awaria procesu; — awaria/nieprawidłowe działanie systemu; — błąd ludzki; — zdarzenie zewnętrzne.
4.2. Szczegółowa klasyfikacja przyczyn źródłowych incydentu	Szczegółowa klasyfikacja przyczyn źródłowych poważnego incydentu związanego z ICT w ramach rodzajów incydentów, w tym następujące szczegółowe kategorie powiązane z kategoriami ogólnymi zgłaszanymi w polu danych 4.1: 1. **Złośliwe działania** (w przypadku zaznaczenia tej opcji należy wybrać co najmniej jedną z następujących opcji): a) celowe działania wewnętrzne; b) umyślne uszkodzenie fizyczne/manipulacja/kradzież; c) oszukańcze działania. 2. **Awaria procesu** (w przypadku zaznaczenia tej opcji należy wybrać co najmniej jedną z następujących opcji): a) niewystarczające monitorowanie lub brak monitorowania i kontroli;	Nie	Nie	Tak	Wybór (można wybrać więcej niż jedną opcję): — złośliwe działania: celowe działania wewnętrzne; — złośliwe działania: umyślne uszkodzenie fizyczne/manipulacja/kradzież; — złośliwe działania: oszukańcze działania; — awaria procesu: niewystarczające monitorowanie lub brak monitorowania i kontroli; — awaria procesu: niewystarczający/niejasny podział ról i obowiązków; — awaria procesu: awaria procesu zarządzania ryzykiem związanym z ICT; — awaria procesu: niewystarczające operacje ICT i operacje związane z bezpieczeństwem ICT lub ich niepowodzenie;

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	b) niewystarczający/niejasny podział ról i obowiązków; c) awaria procesu zarządzania ryzykiem związanym z ICT; d) niewystarczające operacje ICT i operacje związane z bezpieczeństwem ICT lub ich niepowodzenie; e) niewystarczające zarządzanie projektami ICT lub jego niepowodzenie; f) nieodpowiednie wewnętrzne polityki, procedury lub dokumentacja; g) nieodpowiednie pozyskiwanie, rozwój lub utrzymanie systemów ICT; h) inne (proszę określić). 3. **Awaria/nieprawidłowe działanie systemu** (w przypadku zaznaczenia tej opcji należy wybrać co najmniej jedną z następujących opcji): a) możliwości i wydajność sprzętu: poważne incydenty związane z ICT spowodowane zasobami sprzętowymi, które pod względem możliwości lub wydajności okazują się niewystarczające do spełnienia mających zastosowanie wymogów prawnych; b) konserwacja sprzętu: poważne incydenty związane z ICT wynikające z nieodpowiedniej lub niewystarczającej konserwacji elementów sprzętu; kategoria inna niż „utrata przydatności/ starzenie się sprzętu"; c) utrata przydatności/starzenie się sprzętu: ten rodzaj przyczyny źródłowej obejmuje poważne incydenty związane z ICT wynikające z przestarzałych lub starzejących się elementów sprzętu; d) kompatybilność/konfiguracja oprogramowania: poważne incydenty związane z ICT spowodowane przez elementy oprogramowania, które są niekompatybilne z innymi konfiguracjami oprogramowania lub systemu, w tym poważne incydenty związane z ICT wynikające z konfliktów oprogramowania, nieprawidłowych ustawień lub nieprawidłowo skonfigurowanych parametrów, które mają wpływ na ogólną funkcjonalność systemu; e) efektywność oprogramowania: poważne incydenty związane z ICT wynikające z elementów oprogramowania, które wykazują słabą wydajność lub nieefektywność z przyczyn innych niż określone w pozycji „kompatybilność/konfiguracja oprogramowania", w tym poważne incydenty związane z ICT spowodowane powolnym czasem reakcji, nadmiernym wykorzystywaniem zasobów lub nieefektywnym przeprowadzaniem zapytań, co wpływa na działanie oprogramowania lub systemu;				— awaria procesu: niewystarczające zarządzanie projektami ICT lub jego niepowodzenie; — awaria procesu: nieodpowiednie wewnętrzne polityki, procedury lub dokumentacja; — awaria procesu: nieodpowiednie pozyskiwanie, rozwój lub utrzymanie systemów ICT; — awaria procesu: inne (należy określić); — awaria systemu: możliwości i wydajność sprzętu; — awaria systemu: konserwacja sprzętu; — awaria systemu: utrata przydatności/starzenie się sprzętu; — awaria systemu: kompatybilność/konfiguracja oprogramowania; — awaria systemu: efektywność oprogramowania; — awaria systemu: konfiguracja sieci; — awaria systemu: uszkodzenie fizyczne; — awaria systemu: inne (należy określić); — błąd ludzki: pominięcie; - — błąd ludzki: błąd; — błąd ludzki: umiejętności i wiedza; — błąd ludzki: niewystarczające zasoby ludzkie; — błąd ludzki: zakłócenia w komunikacji; — błąd ludzki: inne (należy określić); — zdarzenie zewnętrzne: klęski żywiołowe/siła wyższa; — zdarzenie zewnętrzne: awarie ze strony osób trzecich; — zdarzenie zewnętrzne: inne (proszę określić).

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	f) konfiguracja sieci: poważne incydenty związane z ICT wynikające z nieprawidłowych lub nieprawidłowo skonfigurowanych ustawień sieciowych lub infrastruktury, w tym poważne incydenty związane z ICT spowodowane błędami w konfiguracji sieci, problemami z routingiem, niewłaściwą konfiguracją zapory sieciowej lub innymi problemami związanymi z siecią mającymi wpływ na łączność lub komunikację; g) uszkodzenie fizyczne: poważne incydenty związane z ICT spowodowane fizycznym uszkodzeniem infrastruktury ICT, które prowadzi do awarii systemu; h) inne (proszę określić). 4. **Błąd ludzki** (w przypadku zaznaczenia tej opcji należy wybrać co najmniej jedną z następujących opcji): a) pominięcie (nieumyślne); b) błąd; c) umiejętności i wiedza: poważne incydenty związane z ICT wynikające z braku fachowej wiedzy lub biegłości w obsłudze systemów lub procesów ICT, co może być spowodowane nieodpowiednim szkoleniem, niewystarczającą wiedzą lub brakami w umiejętnościach wymaganych do wykonywania określonych zadań lub rozwiązywania problemów technicznych; d) niewystarczające zasoby ludzkie: poważne incydenty związane z ICT spowodowane brakiem niezbędnych zasobów, w tym sprzętu, oprogramowania, infrastruktury lub personelu, w tym sytuacje, w których niewystarczające zasoby prowadzą do niewydolności operacyjnej, awarii systemu lub niemożności zaspokojenia potrzeb biznesowych; e) zakłócenia w komunikacji; f) inne (proszę określić). 5. **Zdarzenie zewnętrzne** (w przypadku zaznaczenia tej opcji należy wybrać co najmniej jedną z następujących opcji): a) klęski żywiołowe/siła wyższa; b) awarie ze strony osób trzecich;				

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	c) inne (proszę określić). Podmioty finansowe biorą pod uwagę, że w przypadku powtarzających się poważnych incydentów związanych z ICT uwzględnia się konkretną, widoczną przyczynę źródłową incydentu, a nie szerokie kategorie wymienione w tym polu.				
4.3. Dodatkowa klasyfikacja przyczyn źródłowych incydentu	Dodatkowa klasyfikacja przyczyn źródłowych poważnego incydentu związanego z ICT w ramach rodzaju incydentu, w tym następujące dodatkowe kategorie klasyfikacji powiązane ze szczegółowymi kategoriami, które należy zgłosić w polu danych 4.2. Pole to jest obowiązkowe w przypadku sprawozdania końcowego, jeżeli w polu danych 4.2 zgłoszono konkretne kategorie, które wymagają uszczegółowienia. 2(a) **Niewystarczające monitorowanie lub brak monitorowania i kontroli:** a) monitorowanie zgodności z polityką; b) monitorowanie usługodawców będących osobami trzecimi; c) monitorowanie i weryfikowanie eliminowania podatności; d) zarządzanie tożsamością i dostępem; e) szyfrowanie i kryptografia; f) rejestrowanie. 2(c) **Awaria procesu zarządzania ryzykiem związanym z ICT:** a) nieokreślenie dokładnych poziomów tolerancji ryzyka; b) niewystarczające oceny podatności na zagrożenia i zagrożeń; c) nieodpowiednie środki zmniejszające ryzyko; d) nieodpowiednie zarządzanie rezydualnym ryzykiem związanym z ICT. 2(d) **Niewystarczające operacje ICT i operacje związane z bezpieczeństwem ICT lub ich niepowodzenie:** a) zarządzanie podatnościami i poprawkami; b) zarządzanie zmianą; c) zarządzanie możliwościami i wydajnością; d) zarządzanie aktywami ICT i klasyfikacja informacji;	Nie	Nie	Tak	Wybór (można wybrać więcej niż jedną opcję): — monitorowanie zgodności z polityką; — monitorowanie usługodawców będących osobami trzecimi; — monitorowanie i weryfikowanie eliminowania podatności; — zarządzanie tożsamością i dostępem; — szyfrowanie i kryptografia; — rejestrowanie; — nieokreślenie dokładnych poziomów tolerancji ryzyka; — niewystarczające oceny podatności na zagrożenia i zagrożeń; — nieodpowiednie środki zmniejszające ryzyko; — nieodpowiednie zarządzanie rezydualnym ryzykiem związanym z ICT; — zarządzanie podatnościami i poprawkami; — zarządzanie zmianą; — zarządzanie możliwościami i wydajnością; — zarządzanie aktywami ICT i klasyfikacja informacji; — kopia zapasowa i przywracanie danych; — obsługa błędów; — nieodpowiednie pozyskiwanie, rozwój lub utrzymanie systemów ICT; — niewystarczające testowanie oprogramowania lub brak/niepowodzenie testowania oprogramowania.

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	e) kopia zapasowa i przywracanie danych; f) obsługa błędów. 2(g) **Nieodpowiednie pozyskiwanie, rozwój lub utrzymanie systemów ICT:** a) nieodpowiednie pozyskiwanie, rozwój lub utrzymanie systemów ICT; b) niewystarczające testowanie oprogramowania lub brak/niepowodzenie testowania oprogramowania.				
4.4. Inne rodzaje przyczyn źródłowych	Podmioty finansowe, które wybrały „inny" rodzaj przyczyny źródłowej w polu danych 4.2, określają inne rodzaje przyczyn źródłowych	Nie	Nie	Tak, jeżeli w polu danych 4.2 wybrano „inny" rodzaj przyczyn źródłowych.	Alfanumeryczne
4.5. Informacje na temat przyczyn źródłowych incydentu	Opis sekwencji zdarzeń, które doprowadziły do poważnego incydentu związanego z ICT, oraz opis podobnej widocznej przyczyny źródłowej poważnego incydentu związanego z ICT, jeżeli incydent ten sklasyfikowano jako powtarzający się incydent, w tym zwięzły opis wszystkich przyczyn i głównych czynników, które przyczyniły się do wystąpienia poważnego incydentu związanego z ICT. W przypadku gdy miały miejsce złośliwe działania, opis przebiegu złośliwego działania, w tym zastosowane taktyki, techniki i procedury, a także wektor wejścia poważnego incydentu związanego z ICT, w tym, w stosownych przypadkach, opis badań i analiz, które doprowadziły do identyfikacji przyczyn źródłowych.	Nie	Nie	Tak	Alfanumeryczne
4.6. Zaradzenie incydentowi	Dodatkowe informacje dotyczące działań/środków podjętych/planowanych w celu trwałego zaradzenia poważnemu incydentowi związanemu z ICT oraz zapobieżenia ponownemu wystąpieniu tego incydentu. Wnioski wyciągnięte z poważnego incydentu związanego z ICT.	Nie	Nie	Tak	Alfanumeryczne

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	Opis zawiera następujące punkty: 1. **Opis działań podjętych w celu zaradzenia incydentowi** a) działania podjęte w celu trwałego zaradzenia poważnemu incydentowi związanemu z ICT (z wyłączeniem wszelkich działań tymczasowych); b) w odniesieniu do każdego podjętego działania należy wskazać potencjalny udział dostawcy będącego osobą trzecią i podmiotu finansowego; c) należy wskazać, czy procedury zostały dostosowane w następstwie poważnego incydentu związanego z ICT; d) należy wskazać wszelkie dodatkowe kontrole, które wprowadzono lub które zaplanowano, wraz z odpowiednim harmonogramem wdrażania. W stosownych przypadkach, potencjalne kwestie zidentyfikowane w odniesieniu do solidności systemów informatycznych, na które incydent wywarł wpływ, lub potencjalne kwestie dotyczące obowiązujących procedur lub kontroli. Podmioty finansowe wyraźnie określają, w jaki sposób planowane działania naprawcze wyeliminują zidentyfikowane przyczyny źródłowe oraz kiedy oczekuje się trwałego zaradzenia poważnemu incydentowi związanemu z ICT. 2. **Wyciągnięte wnioski** Podmioty finansowe opisują ustalenia z przeglądu dokonanego po wystąpieniu incydentu.				
4.7. Data i godzina usunięcia przyczyny źródłowej incydentu	Data i godzina usunięcia przyczyny źródłowej incydentu.	Nie	Nie	Tak	Standard UTC zgodny z ISO 8601 (RRRR-MM-DD Thh: mm:ss)
4.8. Data i godzina zaradzenia incydentowi	Data i godzina zaradzenia incydentowi.	Nie	Nie	Tak	Standard UTC zgodny z ISO 8601 (RRRR-MM-DD Thh: mm:ss)

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
4.9.	Informacja, czy data trwałego zaradzenia incydentowi różni się od pierwotnie planowanej daty wdrożenia	W stosownych przypadkach opis przyczyny, dla której data trwałego zaradzenia poważnym incydentom związanym z ICT różni się od pierwotnie planowanej daty wdrożenia.	Nie	Nie	Tak	Alfanumeryczne
4.10.	Ocena ryzyka dla funkcji krytycznych do celów restrukturyzacji i uporządkowanej likwidacji	Ocena, czy poważny incydent związany z ICT stwarza ryzyko dla funkcji krytycznych w rozumieniu art. 2 ust. 1 pkt 35 dyrektywy Parlamentu Europejskiego i Rady 2014/59/UE ([2]). Podmioty, o których mowa w art. 1 ust. 1 dyrektywy 2014/59/UE, wskazują, czy incydent stwarza ryzyko dla funkcji krytycznych w rozumieniu art. 2 ust. 1 pkt 35 dyrektywy 2014/59/UE, zgłoszonych w szablonie Z07.01 określonym w rozporządzeniu wykonawczym Komisji (UE) 2018/1624 ([3]) i przyporządkowanych do konkretnego podmiotu w szablonie Z07.02.	Nie	Nie	Tak, jeżeli incydent stwarza ryzyko dla funkcji krytycznych podmiotów finansowych w rozumieniu art. 2 ust. 1 pkt 35 dyrektywy 2014/59/UE.	Alfanumeryczne
4.11.	Informacje istotne dla organów ds. restrukturyzacji i uporządkowanej likwidacji	Opis tego, czy poważny incydent związany z ICT wpłynął na możliwość przeprowadzenia skutecznej restrukturyzacji i uporządkowanej likwidacji podmiotu lub grupy, a jeśli tak, to w jaki sposób. Podmioty, o których mowa w art. 1 ust. 1 dyrektywy 2014/59/UE, przekazują informacje na temat tego, czy poważny incydent związany z ICT wpłynął na możliwość przeprowadzenia skutecznej restrukturyzacji i uporządkowanej likwidacji podmiotu lub grupy, a jeśli tak, to w jaki sposób. Podmioty te wskazują również, czy poważny incydent związany z ICT wpływa na wypłacalność lub płynność podmiotu finansowego, oraz potencjalne ilościowe określenie tego wpływu. Podmioty te przekazują również informacje na temat wpływu na ciągłość operacyjną, wpływu na możliwość przeprowadzenia skutecznej restrukturyzacji i uporządkowanej likwidacji podmiotu, wszelkich dodatkowych skutków dla kosztów i strat wynikających z poważnego incydentu związanego z ICT, w tym na pozycję kapitałową podmiotu finansowego, oraz na temat tego, czy ustalenia umowne dotyczące korzystania z usług ICT są nadal solidne i w pełni egzekwowalne w przypadku restrukturyzacji i uporządkowanej likwidacji danego podmiotu.	Nie	Nie	Tak, jeżeli incydent wpłynął na możliwość przeprowadzenia skutecznej restrukturyzacji i uporządkowanej likwidacji danego podmiotu lub danej grupy.	Alfanumeryczne

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
4.12. Próg istotności dla kryterium klasyfikacji „Skutki gospodarcze”	Szczegółowe informacje na temat progów ostatecznie osiągniętych w wyniku poważnego incydentu związanego z ICT w odniesieniu do kryterium „Skutki gospodarcze”, o którym mowa w art. 7 i 14 rozporządzenia delegowanego (UE) 2024/1772.	Nie	Nie	Tak	Alfanumeryczne
4.13. Kwota bezpośrednich i pośrednich kosztów i strat brutto	Łączna kwota bezpośrednich i pośrednich kosztów i strat brutto poniesionych przez podmiot finansowy w wyniku poważnego incydentu związanego z ICT, w tym: a) kwota wywłaszczonych środków finansowych lub aktywów finansowych, za które podmiot finansowy jest odpowiedzialny; b) kwota kosztów zastąpienia lub przeniesienia oprogramowania, sprzętu lub infrastruktury; c) kwota kosztów personelu, w tym kosztów związanych z zastąpieniem lub przeniesieniem personelu, rekrutacją dodatkowych pracowników, wynagrodzeniem za godziny nadliczbowe oraz odzyskaniem utraconych lub ograniczonych umiejętności personelu; d) kwota opłat z tytułu nieprzestrzegania zobowiązań umownych; e) kwota kosztów poniesionych w związku z roszczeniami dochodzonymi przez klientów i wypłaconymi im odszkodowaniami; f) kwota strat wynikających z utraconych dochodów; g) kwota kosztów związanych z komunikacją wewnętrzną i zewnętrzną; h) kwota kosztów doradztwa, w tym kosztów związanych z doradztwem prawnym, usługami kryminalistycznymi i usługami z zakresu środków zaradczych. i) kwota innych kosztów i strat, w tym: (i) odpisy bezpośrednie, w tym z tytułu utraty wartości i rozliczeń, ujmowane w ciężar rachunku zysków i strat, i odpisy aktualizujące wartość wynikłe z poważnego incydentu związanego z ICT; (ii) rezerwy ujęte w rachunku zysków i strat na prawdopodobne straty wynikłe z poważnego incydentu związanego z ICT;	Nie	Nie	Tak	Wartość pieniężna

Pole danych	Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
	(iii) straty oczekujące, w postaci strat wynikłych z poważnego incydentu związanego z ICT, które tymczasowo księguje się na kontach tymczasowych lub przejściowych i które nie są ujęte w rachunku zysków i strat, a które mają zostać w nim ujęte dla okresu odpowiadającego kwocie i wiekowi pozycji oczekującej; (iv) istotne niepobrane przychody wynikające ze zobowiązań umownych wobec osób trzecich, w tym decyzje o wypłaceniu klientowi rekompensaty z tytułu poważnego incydentu związanego z ICT raczej w drodze korekty przychodów poprzez odstąpienie od pobrania opłat umownych lub obniżenie ich wysokości w określonym przyszłym okresie niż w drodze przyznania zwrotu lub dokonania płatności bezpośredniej; (v) straty czasowe, jeśli obejmują okres dłuższy niż jeden rok obrachunkowy i są źródłem ryzyka prawnego. Podmioty finansowe uwzględniają w swojej ocenie art. 7 ust. 1 i 2 rozporządzenia delegowanego (UE) 2024/1772. Podmioty finansowe nie uwzględniają w tej kwocie żadnego rodzaju odzyskanych środków finansowych. Podmioty finansowe wykazują kwotę pieniężną jako wartość dodatnią W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, podmioty finansowe uwzględniają całkowitą kwotę kosztów i strat we wszystkich podmiotach finansowych. Podmioty finansowe przedstawiają punkt danych w jednostkach, stosując minimalną dokładność odpowiadającą tysiącom jednostek.				
4.14. Kwota odzyskanych środków finansowych	Łączna kwota odzyskanych środków finansowych. Odzyskane środki finansowe są związane z pierwotną stratą będącą wynikiem incydentu, niezależnie od momentu ich odzyskania w postaci otrzymania środków finansowych lub wpływu korzyści gospodarczych.	Nie	Nie	Tak	Wartość pieniężna Podmioty finansowe przedstawiają punkt danych w jednostkach, stosując minimalną dokładność odpowiadającą tysiącom jednostek.

Pole danych		Opis	Obowiązkowe w przypadku wstępnego powiadomienia	Obowiązkowe w przypadku sprawozdania śródokresowego	Obowiązkowe w przypadku sprawozdania końcowego	Rodzaj pola
		Podmioty finansowe wykazują kwotę pieniężną jako wartość dodatnią. W przypadku sprawozdawczości zagregowanej, o której mowa w art. 7 niniejszego rozporządzenia, podmioty finansowe uwzględniają całkowitą kwotę odzyskanych środków finansowych we wszystkich podmiotach finansowych.				
4.15.	Informacja, czy incydenty inne niż poważne powtarzały się	Informacja, czy więcej niż jeden incydent inny niż poważny związany z ICT powtarza się i czy łącznie uznaje się je za poważny incydent w rozumieniu art. 8 ust. 2 rozporządzenia delegowanego (UE) 2024/1772. Podmioty finansowe wskazują, czy inne niż poważne incydenty związane z ICT powtarzają się i czy łącznie uznaje się je za jeden poważny incydent związany z ICT. Podmioty finansowe wskazują również liczbę przypadków wystąpienia takich innych niż poważne incydentów związanych z ICT.	Nie	Nie	Tak, jeżeli poważny incydent obejmuje więcej niż jeden inny niż poważny, powtarzający się incydent.	Alfanumeryczne
4.16.	Data i godzina wystąpienia powtarzających się incydentów	W przypadku gdy podmioty finansowe zgłaszają powtarzające się incydenty związane z ICT, należy podać datę i godzinę wystąpienia pierwszego incydentu związanego z ICT.	Nie	Nie	Tak w przypadku powtarzających się incydentów.	Standard UTC zgodny z ISO 8601 (RRRR-MM-DD Thh: mm:ss)

([1]) 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).

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

([3]) Rozporządzenie wykonawcze Komisji (UE) 2018/1624 z dnia 23 października 2018 r. ustanawiające wykonawcze standardy techniczne w odniesieniu do procedur i standardowych formularzy i szablonów stosowanych do przekazywania informacji do celów sporządzenia planów restrukturyzacji i uporządkowanej likwidacji w odniesieniu do instytucji kredytowych i firm inwestycyjnych zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2014/59/UE oraz uchylające rozporządzenie wykonawcze Komisji (UE) 2016/1066 (Dz.U. L 277 z 7.11.2018, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

ZAŁĄCZNIK III

WZORY NA POTRZEBY POWIADAMIANIA O ZNACZĄCYCH CYBERZAGROŻENIACH

Numer pola	Pole danych	
1	Nazwa podmiotu przedkładającego powiadomienie	
2	Kod identyfikacyjny podmiotu przedkładającego powiadomienie	
3	Rodzaj podmiotu finansowego przedkładającego powiadomienie	
4	Nazwa podmiotu finansowego	
5	Kod LEI podmiotu finansowego	
6	Imię i nazwisko głównej osoby wyznaczonej do kontaktów	
7	Adres e-mail głównej osoby wyznaczonej do kontaktów	
8	Numer telefonu głównej osoby wyznaczonej do kontaktów	
9	Imię i nazwisko dodatkowej osoby wyznaczonej do kontaktów	
10	Adres e-mail dodatkowej osoby wyznaczonej do kontaktów	
11	Numer telefonu dodatkowej osoby wyznaczonej do kontaktów	
12	Data i godzina wykrycia cyberzagrożenia	
13	Opis znaczącego cyberzagrożenia	
14	Informacje o potencjalnych skutkach	
15	Kryteria klasyfikacji potencjalnych incydentów	
16	Status cyberzagrożenia	
17	Działania podjęte w celu zapobieżenia urzeczywistnieniu się znaczących cyberzagrożeń	
18	Powiadamianie innych zainteresowanych stron	
19	Oznaki naruszenia integralności systemu	
20	Inne istotne informacje	

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

ZAŁĄCZNIK IV

GLOSARIUSZ DANYCH I INSTRUKCJE DOTYCZĄCE POWIADAMIANIA O ZNACZĄCYCH CYBERZAGROŻENIACH

Pole danych		Opis	Pole obowiązkowe	Rodzaj pola
1.	Nazwa podmiotu przedkładającego powiadomienie	Pełna nazwa prawna podmiotu przedkładającego powiadomienie.	Tak	Alfanumeryczne
2.	Kod identyfikacyjny podmiotu przedkładającego powiadomienie	Kod identyfikacyjny podmiotu przedkładającego powiadomienie. W przypadku gdy powiadomienie/sprawozdanie przedkładają podmioty finansowe, kodem identyfikacyjnym jest identyfikator podmiotu prawnego (LEI), który jest niepowtarzalnym kodem składającym się z 20 znaków alfanumerycznych, zgodnie z ISO 17442-1:2020. Dostawca będący osobą trzecią, który przedkłada sprawozdanie w imieniu podmiotu finansowego, może stosować kod identyfikacyjny określony w wykonawczych standardach technicznych przyjętych na podstawie art. 28 ust. 9 rozporządzenia (UE) 2022/2554.	Tak	Alfanumeryczne
3.	Rodzaj podmiotu finansowego przedkładającego powiadomienie	Rodzaj podmiotu, o którym mowa w art. 2 ust. 1 lit. a)–t) rozporządzenia (UE) 2022/2554, który przedkłada powiadomienie.	Tak, jeżeli powiadomienie nie jest przedkładane bezpośrednio przez podmiot finansowy, którego dotyczy znaczące cyberzagrożenie.	Wybór (można wybrać więcej niż jedną opcję): — instytucja kredytowa; — instytucja płatnicza; — zwolniona instytucja płatnicza; — dostawca świadczący usługę dostępu do informacji o rachunku; — instytucja pieniądza elektronicznego; — zwolniona instytucja pieniądza elektronicznego; — firma inwestycyjna; — dostawca usług w zakresie kryptoaktywów; — emitent tokenów powiązanych z aktywami; — centralny depozyt papierów wartościowych; — kontrahent centralny; — system obrotu; — repozytorium transakcji; — zarządzający alternatywnym funduszem inwestycyjnym; — spółka zarządzająca; — dostawca usług w zakresie udostępniania informacji;

Pole danych		Opis	Pole obowiązkowe	Rodzaj pola
				— zakład ubezpieczeń i zakład reasekuracji; — pośrednik ubezpieczeniowy, pośrednik reasekuracyjny i pośrednik oferujący ubezpieczenia uzupełniające; — instytucja pracowniczych programów emerytalnych; — agencja ratingowa; — administrator kluczowych wskaźników referencyjnych; — dostawca usług finansowania społecznościowego; — repozytorium sekurytyzacji.
4.	Nazwa podmiotu finansowego	Pełna nazwa prawna podmiotu finansowego powiadamiającego o znaczącym cyberzagrożeniu.	Tak, jeżeli podmiot finansowy jest inny niż podmiot przedkładający powiadomienie.	Alfanumeryczne
5.	Kod LEI podmiotu finansowego	Identyfikator podmiotu prawnego (LEI) podmiotu finansowego powiadamiającego o znaczącym cyberzagrożeniu, przypisany zgodnie ze standardem Międzynarodowej Organizacji Normalizacyjnej.	Tak, jeżeli podmiot finansowy powiadamiający o znaczącym cyberzagrożeniu jest inny niż podmiot przedkładający powiadomienie.	Niepowtarzalny kod składający się z 20 znaków alfanumerycznych, zgodnie z ISO 17442-1:2020
6.	Imię i nazwisko głównej osoby wyznaczonej do kontaktów	Imię i nazwisko głównej osoby wyznaczonej do kontaktów w podmiocie finansowym.	Tak	Alfanumeryczne
7.	Adres e-mail głównej osoby wyznaczonej do kontaktów	Adres e-mail głównej osoby wyznaczonej do kontaktów, z którego właściwy organ może korzystać do celów dalszej komunikacji.	Tak	Alfanumeryczne
8.	Numer telefonu głównej osoby wyznaczonej do kontaktów	Numer telefonu głównej osoby wyznaczonej do kontaktów, z którego właściwy organ może korzystać do celów dalszej komunikacji. Numer telefonu należy podać ze wszystkimi międzynarodowymi prefiksami (np. +33XXXXXXXXX).	Tak	Alfanumeryczne
9.	Imię i nazwisko dodatkowej osoby wyznaczonej do kontaktów	Imię i nazwisko dodatkowej osoby wyznaczonej do kontaktów ze strony podmiotu finansowego lub podmiotu przedkładającego powiadomienie w imieniu podmiotu finansowego, jeżeli są dostępne.	Tak, jeżeli imię i nazwisko dodatkowej osoby wyznaczonej do kontaktów ze strony podmiotu finansowego lub podmiotu przedkładającego powiadomienie w imieniu podmiotu finansowego są dostępne.	Alfanumeryczne

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Pole danych		Opis	Pole obowiązkowe	Rodzaj pola
10.	Adres e-mail dodatkowej osoby wyznaczonej do kontaktów	Adres e-mail dodatkowej osoby wyznaczonej do kontaktów lub funkcjonalny adres e-mail zespołu, z których właściwy organ może korzystać do celów dalszej komunikacji, jeżeli jest dostępny.	Tak, jeżeli adres e-mail dodatkowej osoby wyznaczonej do kontaktów lub funkcjonalny adres e-mail zespołu, z których właściwy organ może korzystać do celów dalszej komunikacji, jest dostępny.	Alfanumeryczne
11.	Numer telefonu dodatkowej osoby wyznaczonej do kontaktów	Numer telefonu dodatkowej osoby wyznaczonej do kontaktów, z którego właściwy organ może korzystać do celów dalszej komunikacji, jeżeli jest dostępny. Numer telefonu należy podać ze wszystkimi międzynarodowymi prefiksami (np. +33XXXXXXXXX).	Tak, jeżeli numer telefonu dodatkowej osoby wyznaczonej do kontaktów, z którego właściwy organ może korzystać do celów dalszej komunikacji, jest dostępny.	Alfanumeryczne
12.	Data i godzina wykrycia cyberzagrożenia	Data i godzina, kiedy podmiot finansowy dowiedział się o znaczącym cyberzagrożeniu.	Tak	Standard UTC zgodny z ISO 8601 (RRRR-MM-DD Thh: mm:ss)
13.	Opis znaczącego cyberzagrożenia	Opis najistotniejszych aspektów znaczącego cyberzagrożenia. Podmioty finansowe przedstawiają: a) ogólny przegląd najistotniejszych aspektów znaczącego cyberzagrożenia; b) ryzyko wynikające ze znaczącego cyberzagrożenia, w tym potencjalne podatności systemów podmiotu finansowego, które mogą zostać wykorzystane; c) informacje o prawdopodobieństwie urzeczywistnienia się znaczącego cyberzagrożenia; oraz d) informacje dotyczące źródła informacji o cyberzagrożeniu.	Tak	Alfanumeryczne
14.	Informacje o potencjalnych skutkach	Informacje o potencjalnych skutkach cyberzagrożenia dla podmiotu finansowego, jego klientów lub kontrahentów finansowych, jeżeli cyberzagrożenie urzeczywistniło się	Tak	Alfanumeryczne
15.	Kryteria klasyfikacji potencjalnych incydentów	Kryteria klasyfikacji, które mogłyby spowodować zgłoszenie poważnego incydentu w przypadku urzeczywistnienia się cyberzagrożenia.	Tak	Wybór (można wybrać więcej niż jedną opcję): — klienci, kontrahenci finansowi i transakcje, których dotyczy incydent; — skutki reputacyjne; — czas trwania incydentu i przerwa w świadczeniu usług; — zasięg geograficzny; — utrata danych; — usługi krytyczne, których dotyczy incydent; — skutki gospodarcze.

Pole danych		Opis	Pole obowiązkowe	Rodzaj pola
16.	Status cyberzagrożenia	Informacje o statusie cyberzagrożenia dla podmiotu finansowego oraz o tym, czy nastąpiły jakiekolwiek zmiany w działaniu związanym z zagrożeniem. Jeżeli cyberzagrożenie zaprzestało komunikacji z systemami informacyjnymi podmiotu finansowego, status ten można oznaczyć jako nieaktywny. Jeżeli podmiot finansowy posiada informacje, że zagrożenie pozostaje aktywne wobec innych stron lub systemu finansowego jako całości, status ten należy oznaczyć jako aktywny.	Tak	Wybór: — aktywny; — nieaktywny.
17.	Działania podjęte w celu zapobieżenia urzeczywistnieniu się znaczących cyberzagrożeń	W stosownych przypadkach należy podać ogólne informacje dotyczące działań podjętych przez podmiot finansowy w celu zapobieżenia urzeczywistnieniu się znaczących cyberzagrożeń.	Tak	Alfanumeryczne
18.	Powiadamianie innych zainteresowanych stron	Informacje na temat zgłaszania cyberzagrożenia innym podmiotom finansowym lub organom.	Tak, jeżeli inne podmioty finansowe lub organy zostały poinformowane o cyberzagrożeniu.	Alfanumeryczne
19.	Oznaki naruszenia integralności systemu	W stosownych przypadkach, informacje dotyczące znaczącego zagrożenia, które mogą pomóc w identyfikowaniu złośliwej działalności w ramach sieci lub systemu informatycznego (oznaki naruszenia integralności systemu). Oznaki naruszenia integralności systemu zgłaszane przez podmiot finansowy mogą obejmować, między innymi, następujące kategorie danych: a) adresy IP; b) adresy URL; c) domeny; d) hasze plików; e) dane dotyczące złośliwego oprogramowania (nazwa złośliwego oprogramowania, nazwy plików i ich lokalizacje, konkretne klucze rejestrów związane z działaniem złośliwego oprogramowania); f) dane dotyczące działania sieci (porty, protokoły, adresy, odesłania, aplikacje klienckie, nagłówki, konkretne rejestry lub odmienne schematy ruchu w sieci); g) dane dotyczące wiadomości e-mail (nadawca, odbiorca, temat, nagłówek, treść); h) wnioski DNS i konfiguracje rejestrów; i) czynności związane z kontem użytkownika (loginy, uprzywilejowana działalność związana z kontem użytkownika, eskalacja uprzywilejowania); j) ruch w bazach danych (odczyt/zapis), wnioski o dostęp do tego samego pliku. Tego rodzaju informacje mogą obejmować dane dotyczące wskaźników opisujących schematy ruchu w sieci odpowiadające znanym atakom/znanej komunikacji w sieci urządzeń zainfekowanych złośliwym oprogramowaniem, adresy IP urządzeń zainfekowanych złośliwym oprogramowaniem (boty), dane dotyczące serwerów „dowodzenia i kontroli" wykorzystywanych przez złośliwe oprogramowanie (zazwyczaj domeny lub adresy IP) oraz adresy URL dotyczące stron typu phishing lub obserwowanych stron internetowych, na których znajdują się złośliwe oprogramowanie lub narzędzia typu *exploit kit*.	Tak, jeżeli dostępne są informacje na temat oznak naruszenia integralności systemu związanych z cyberzagrożeniem.	Alfanumeryczne
20.	Inne istotne informacje	Wszelkie inne istotne informacje dotyczące znaczącego cyberzagrożenia	Tak, w stosownych przypadkach i jeżeli dostępne są inne informacje, które nie zostały uwzględnione we wzorze.	Alfanumeryczne

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj