JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 34

5 czerwca 2024 r.

# Wspólne wytyczne

## w sprawie oszacowania zagregowanych rocznych kosztów i strat spowodowanych poważnymi incydentami związanymi z ICT, na podstawie rozporządzenia (UE) 2022/2554

Niniejsze wytyczne zawierają odniesienia do rozporządzeń delegowanych i wykonawczych Komisji Europejskiej, które nie zostały jeszcze opublikowane w Dzienniku Urzędowym UE. Po publikacji tych rozporządzeń w Dzienniku Urzędowym odniesienia te zostaną włączone do niniejszych wytycznych i tym samym wytyczne zostaną sfinalizowane. Odniesienia zostaną umieszczone w sekcjach zaznaczonych kolorem żółtym.

Datę rozpoczęcia stosowania niniejszych wytycznych będzie można ustalić dopiero po ich sfinalizowaniu. Przewidywaną datą rozpoczęcia stosowania niniejszych wytycznych jest 17 stycznia 2025 r. W przypadku opóźnienia finalizacji niniejszych wytycznych stosowanie niniejszych wytycznych rozpocznie się po upływie dwóch miesięcy od daty publikacji tłumaczeń wytycznych we wszystkich językach urzędowych UE.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

# Wspólne wytyczne w sprawie oszacowania zagregowanych rocznych kosztów i strat spowodowanych poważnymi incydentami związanymi z ICT

## Status niniejszych wspólnych wytycznych

Niniejszy dokument zawiera wspólne wytyczne wydane na podstawie art. 16 rozporządzenia (UE) nr 1093/2010[1], art. 16 rozporządzenia (UE) nr 1094/2010[2] oraz art. 16 rozporządzenia (UE) nr 1095/2010[3] – „rozporządzenia w sprawie ustanowienia EUN". Zgodnie z art. 16 ust. 3 odpowiednich rozporządzeń w sprawie ustanowienia EUN właściwe organy i instytucje finansowe muszą dołożyć wszelkich starań, aby zastosować się do wytycznych.

We wspólnych wytycznych określono stanowisko Europejskich Urzędów Nadzoru (EUN) w sprawie odpowiednich praktyk nadzorczych w ramach Europejskiego Systemu Nadzoru Finansowego lub w sprawie sposobu, w jaki należy stosować prawo Unii w danym obszarze. Właściwe organy, do których mają zastosowanie wspólne wytyczne, powinny przestrzegać wytycznych poprzez odpowiednie włączenie ich do swoich praktyk nadzorczych (np. poprzez zmianę obowiązujących ram prawnych lub procesów nadzorczych), również gdy wspólne wytyczne są skierowane przede wszystkim do instytucji.

## Wymogi dotyczące powiadomienia o stosowaniu wytycznych

Zgodnie z art. 16 ust. 3 rozporządzeń w sprawie ustanowienia EUN właściwe organy muszą w terminie do 19.05.2025 (dwa miesiące od wydania) powiadomić odpowiedni EUN, czy stosują się lub zamierzają zastosować się do niniejszych wspólnych wytycznych/zaleceń, albo podać uzasadnienie niestosowania się do nich. W razie braku powiadomienia w wyznaczonym terminie odpowiedni EUN uzna, że właściwe organy nie stosują się do niniejszych wspólnych wytycznych. Powiadomienia należy przesłać na adres: compliance@eba.europa.eu, compliance@eiopa.europa.eu i DORA@esma.europa.eu z dopiskiem „JC/GL/2024/34". Wzór powiadomień jest dostępny na stronach internetowych EUN. Powiadomienia powinny przekazywać osoby odpowiednio upoważnione do informowania o stosowaniu się do wytycznych w imieniu właściwego organu.

[1] 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 i uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

[2] 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).

[3] 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).

Powiadomienia zostaną opublikowane na stronach internetowych EUN zgodnie z art. 16 ust. 3.

# Tytuł I – Przedmiot, zakres, adresaci i definicje

## Przedmiot i zakres stosowania

1. Niniejsze wytyczne mają na celu wykonanie mandatu udzielonego Europejskim Urzędom Nadzoru na mocy art. 11 ust. 11 rozporządzenia (UE) 2022/2554[4] w związku z opracowaniem wspólnych wytycznych w sprawie oszacowania zagregowanych rocznych kosztów i strat wynikających z poważnych incydentów związanych z ICT, o których mowa w art. 11 ust. 10 tego rozporządzenia. Niniejsze wytyczne określają również wspólny wzór do celów przekazywania informacji o zagregowanych rocznych kosztach i stratach.

## Adresaci

2. Niniejsze wytyczne skierowane są do właściwych organów określonych w art. 46 rozporządzenia nr 2022/2554 oraz do instytucji finansowych określonych w art. 4 ust. 1 rozporządzenia (UE) nr 1093/2010, art. 4 ust. 1 rozporządzenia (UE) nr 1094/2010 i art. 4 ust. 1 rozporządzenia (UE) nr 1095/2010.

## Definicje

3. Terminy stosowane i zdefiniowane w rozporządzeniu (UE) nr 2022/2554 mają takie samo znaczenie w niniejszych wytycznych.

# Tytuł II – Wdrożenie

## Data rozpoczęcia stosowania

4. Niniejsze wytyczne stosuje się od dnia 19.05.2025.

[4] Rozporządzenie Parlamentu Europejskiego i Rady (EU) 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 (Dz.U. L 333 z 27.12.2022, s. 1).

# Tytuł III – Przepisy dotyczące oszacowania zagregowanych rocznych kosztów i strat wynikających z poważnych incydentów związanych z ICT

5. Podmioty finansowe powinny oszacować zagregowane roczne koszty i straty wynikające z poważnych incydentów związanych z ICT poprzez zagregowanie kosztów i strat poważnych incydentów związanych z ICT, które wystąpiły w trakcie roku referencyjnego, w odniesieniu do którego właściwy organ zwrócił się o oszacowanie. Podmiot finansowy może wybrać, czy rok referencyjny powinien odpowiadać zakończonemu rokowi kalendarzowemu, czy też zakończonemu rokowi obrachunkowemu podmiotu finansowego, za który podmiot finansowy złożył sprawozdanie finansowe. Po podjęciu przez podmiot finansowy decyzji, czy oszacowanie będzie oparte na roku kalendarzowym, czy roku obrachunkowym, decyzję tę należy zastosować do przyszłych oszacowań łącznych rocznych kosztów i strat. Podmiot finansowy może zmienić tę decyzję, powiadamiając o tym właściwy organ, oraz pod warunkiem, że właściwy organ nie zgłosi sprzeciwu w terminie dwóch miesięcy od otrzymania powiadomienia. Podmioty finansowe nie powinny uwzględniać kosztów i strat związanych z tymi incydentami, które wystąpiły przed tym rokiem referencyjnym lub po jego zakończeniu.

6. Podmioty finansowe powinny uwzględnić w oszacowaniu wszystkie incydenty związane z ICT, które – niezależnie od przyczyny – zostały sklasyfikowane jako poważne zgodnie z rozporządzeniem delegowanym Komisji [OJ L, 2024/1772, 25.6.2024][5] w sprawie klasyfikacji incydentów oraz

   (a) w odniesieniu do których podmiot finansowy złożył sprawozdanie końcowe zgodnie z art. 19 ust. 4 lit. c) rozporządzenia (UE) 2022/2554 w danym roku referencyjnym, lub

   (b) wszelkie incydenty, w odniesieniu do których podmiot finansowy złożył w poprzednich latach referencyjnych sprawozdanie końcowe zgodnie z art. 19 ust. 4 lit. c) rozporządzenia (UE) 2022/2554 , które miały wymierne skutki finansowe dla podmiotu finansowego w danym roku referencyjnym.

7. Podmioty finansowe powinny oszacować zagregowane roczne koszty i straty, stosując następujące kroki w podanej kolejności:

   (a) osobno oszacować koszty i straty dla każdego poważnego incydentu związanego z ICT, o którym mowa w pkt 6. Oszacowanie powinno pokazać koszty i straty brutto, z uwzględnieniem rodzajów kosztów i strat, które określono w art. 7 ust. 1 i 2 rozporządzenia delegowanego Komisji [OJ L, 2024/1772, 25.6.2024];

[5]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. [*OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj*]

(b) dla każdego poważnego incydentu związanego z ICT podmioty finansowe powinny również oszacować kwoty odzyskane, jak określono w załączniku II do rozporządzenia wykonawczego Komisji [OJ L, 2025/302, 20.2.2025][6];

(c) podmioty finansowe powinny zagregować koszty i straty brutto oraz kwoty odzyskane w odniesieniu do poważnych incydentów związanych z ICT.

8. Jako podstawę oszacowania podmioty finansowe powinny odnosić się do kosztów, strat i kwot odzyskanych, które są ujęte w ich sprawozdaniach finansowych, takich jak rachunek zysków i strat, lub, w stosownych przypadkach, w ich sprawozdawczości do celów nadzoru, za dany rok referencyjny. W swoich oszacowaniach podmioty finansowe powinny również uwzględnić rezerwy księgowe, które zostały ujęte w ich sprawozdaniach finansowych, takich jak rachunek zysków i strat za dany rok referencyjny. W przypadku gdy dokładne dane nie są dostępne, podmioty finansowe powinny, w miarę możliwości, opierać swoje oszacowania na innych dostępnych danych i informacjach.

9. Podmioty finansowe powinny uwzględnić korektę oszacowania kosztów i strat przekazanych za poprzedni rok w oszacowaniu kosztów i strat dotyczących tego odpowiedniego roku referencyjnego, w którym dokonano korekty.

10. W sprawozdaniu zawierającym oszacowanie zagregowanych rocznych kosztów i strat podmioty finansowe powinny również zawrzeć podział kosztów i strat brutto oraz kwot odzyskanych na każdy poważny incydent związany z ICT, który uwzględniono w zagregowanych danych.

11. Przy przekazywaniu właściwemu organowi oszacowania zagregowanych rocznych kosztów i strat w odniesieniu do roku referencyjnego, podmioty finansowe powinny korzystać ze wzoru formularza zawartego w załączniku. W odniesieniu do każdej pozycji, o której mowa w pkt 6 i 9 i którą uwzględniono w oszacowaniu dla roku referencyjnego, podmioty finansowe powinny stosować te same kody referencyjne dotyczące incydentów podane przez podmiot finansowy, co kody użyte w sprawozdaniu końcowym, zgodnie z art. 19 ust. 4 lit. c) rozporządzenia (UE) 2022/2554.

[6] 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. [*OJ L, 2025/302, 20.2.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj*]

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

## Załącznik: Wzór sprawozdania dotyczącego kosztów i strat brutto oraz kwot odzyskanych w danym roku referencyjnym

| | |
|---|---|
| Nazwa podmiotu finansowego | |
| Identyfikator podmiotu prawnego | |
| Data rozpoczęcia i zakończenia roku referencyjnego podmiotu finansowego | |
| Waluta | |

| Numer incydentu | Data przekazania sprawozdania końcowego z incydentu | Numer referencyjny incydentu | Koszty i straty brutto dotyczące incydentu w roku referencyjnym (w tys. jednostek) | Kwoty odzyskane dotyczące incydentu w roku referencyjnym (w tys. jednostek) |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| … | | | | |
| Ogółem dla roku referencyjnego | ---------- | ---------- | | |