EBA/GL/2021/03

10 czerwca 2021 r.

Zmienione wytyczne

dotyczące zgłaszania poważnych incydentów zgodnie z dyrektywą PSD2

1. Zapewnienie zgodności i obowiązki sprawozdawcze

Status wytycznych

1. Niniejszy dokument zawiera wytyczne wydane na podstawie art. 16 rozporządzenia w sprawie ustanowienia EUNB[1]. Zgodnie z art. 16 ust. 3 rozporządzenia w sprawie ustanowienia EUNB właściwe organy i instytucje finansowe muszą dołożyć wszelkich starań, aby zastosować się do wytycznych.

2. Wytyczne przedstawiają stanowisko EUNB w sprawie właściwych praktyk nadzorczych w ramach Europejskiego Systemu Nadzoru Finansowego lub sposobu, w jaki należy stosować prawo unijne w danym obszarze. Właściwe organy zdefiniowane w art. 4 ust. 2 rozporządzenia w sprawie ustanowienia EUNB, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez odpowiednie włączenie ich do swoich praktyk (np. poprzez dostosowanie swoich ram prawnych lub procesów nadzorczych), również w przypadku, gdy wytyczne są skierowane przede wszystkim do instytucji.

Wymogi sprawozdawcze

3. Zgodnie z art. 16 ust. 3 rozporządzenia w sprawie EUNB każdy właściwy organ ma obowiązek powiadomić EUNB w terminie do (07.11.2021) o tym, czy stosuje się lub zamierza stosować się do niniejszych wytycznych, albo podać uzasadnienie niestosowania się do nich. W razie nieotrzymania powiadomienia w wyznaczonym terminie EUNB uzna, że właściwe organy nie stosują się do niniejszych wytycznych. Powiadomienia należy przesyłać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB z dopiskiem „EBA/GL/2021/03”. Powiadomienia przekazują osoby odpowiednio upoważnione do informowania o stosowaniu się do wytycznych w imieniu właściwych organów. Do EUNB należy również zgłaszać wszelkie zmiany związane ze stosowaniem się do wytycznych.

4. Powiadomienia zostaną opublikowane na stronie internetowej EUNB, zgodnie z art. 16 ust. 3.

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

2. Przedmiot, zakres stosowania i definicje

Przedmiot

5. Niniejsze wytyczne wynikają z mandatu udzielonego EUNB w art. 96 ust. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 2002/65/WE, 2009/110/WE i 2013/36/UE oraz rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE (PSD2).

6. W szczególności niniejsze wytyczne określają kryteria klasyfikacji przez dostawców usług płatniczych poważnych incydentów operacyjnych lub incydentów związanych z bezpieczeństwem, a także format i procedury, które powinni stosować w celu zgłoszenia takich incydentów właściwemu organowi w państwie członkowskim pochodzenia, jak przewidziano w art. 96 ust. 1 dyrektywy PSD2.

7. Ponadto niniejsze wytyczne dotyczą sposobu, w jaki te właściwe organy powinny oceniać istotność incydentu oraz szczegóły zgłoszeń incydentów, które zgodnie z art. 96 ust. 2 dyrektywy PSD2 udostępniają innym organom krajowym.

8. Ponadto niniejsze wytyczne dotyczą również udostępniania EUNB i EBC istotnych szczegółów zgłoszonych incydentów w celu promowania wspólnego i spójnego podejścia.

Zakres stosowania

9. Niniejsze wytyczne mają zastosowanie do klasyfikacji i zgłaszania poważnych incydentów operacyjnych lub incydentów związanych z bezpieczeństwem zgodnie z art. 96 dyrektywy PSD2.

10. Niniejsze wytyczne mają zastosowanie do wszystkich incydentów objętych definicją „poważnego incydentu operacyjnego lub incydentu związanego z bezpieczeństwem", która obejmuje zarówno incydenty zewnętrzne, jak i wewnętrzne, które mogą być złośliwe lub przypadkowe.

11. Niniejsze wytyczne mają również zastosowanie w przypadku, gdy poważny incydent operacyjny lub incydent związany z bezpieczeństwem ma miejsce poza Unią (np. gdy incydent pochodzi ze spółki dominującej lub jednostki zależnej mającej siedzibę poza Unią) i ma wpływ na usługi płatnicze świadczone przez dostawcę usług płatniczych z siedzibą w Unii bezpośrednio (usługa związana z płatnością jest świadczona przez poszkodowane przedsiębiorstwo spoza Unii) lub pośrednio (zdolność dostawcy usług płatniczych do dalszego prowadzenia działalności płatniczej jest zagrożona w inny sposób w wyniku incydentu).

12. Niniejsze wytyczne mają również zastosowanie do poważnych incydentów mających wpływ na funkcje zlecane osobom trzecim przez dostawców usług płatniczych.

Adresaci

13. Pierwszy zestaw wytycznych (część 4) skierowany jest do dostawców usług płatniczych zdefiniowanych w art. 4 pkt 11 dyrektywy PSD2 i o których mowa w art. 4 ust. 1 rozporządzenia (UE) nr 1093/2010.

14. Drugi i trzeci zestaw wytycznych (część 5 i 6) są skierowane do właściwych organów określonych w art. 4 pkt 2 ppkt (i) rozporządzenia (UE) nr 1093/2010.

Definicje

15. O ile nie określono inaczej, terminy używane i zdefiniowane w dyrektywie PSD2 mają takie samo znaczenie w wytycznych. Ponadto do celów niniejszych wytycznych stosuje się następujące definicje:

Incydent operacyjny lub incydent związany z bezpieczeństwem	Pojedyncze zdarzenie lub seria powiązanych zdarzeń nieplanowanych przez dostawcę usług płatniczych, które mają lub prawdopodobnie będą miały negatywny wpływ na integralność, dostępność, poufność lub autentyczność usług związanych z płatnościami.
Integralność	Właściwość polegająca na ochronie dokładności i kompletności aktywów (w tym danych).
Dostępność	Właściwość usług powiązanych z usługami płatniczymi polegająca na ich pełnej dostępności i możliwości korzystania przez użytkowników, zgodnie z dopuszczalnymi poziomami określonymi przez dostawcę usług płatniczych.
Poufność	Właściwość polegająca na braku dostępności informacji lub nieujawnianiu ich nieupoważnionym osobom fizycznym, podmiotom lub procesom.
Autentyczność	Właściwość polegająca na tym, że źródło jest tym, za które się podaje.
Usługi związane z płatnościami	Każda działalność gospodarcza w rozumieniu art. 4 pkt 3 dyrektywy PSD2 oraz wszelkie konieczne wspierające zadania techniczne konieczne do właściwego świadczenia usług płatniczych.

3. Wdrożenie

Data rozpoczęcia stosowania

16. Niniejsze wytyczne stosuje się od dnia 1 stycznia 2022 r.

Uchylenie

17. Następujące wytyczne tracą moc ze skutkiem od dnia 1 stycznia 2022 r.:

Wytyczne dotyczące zgłaszania poważnych incydentów zgodnie z dyrektywą (UE) 2015/2366 (PSD2) (EBA/GL/2017/10)

4. Wytyczne skierowane do dostawców usług płatniczych dotyczące zgłaszania poważnych incydentów operacyjnych lub incydentów związanych z bezpieczeństwem właściwemu organowi w państwie członkowskim ich pochodzenia

Wytyczna 1: Klasyfikacja jako poważny incydent

1.1. Dostawcy usług płatniczych powinni klasyfikować jako poważne takie incydenty operacyjne lub incydenty związane z bezpieczeństwem, które spełniają

a. co najmniej jedno kryterium na „poziomie posiadania dużego wpływu" lub

b. co najmniej trzy kryteria na „poziomie posiadania niewielkiego wpływu",

jak określono w wytycznej 1.4., oraz zgodnie z oceną określoną w niniejszych wytycznych.

1.2. Dostawcy usług płatniczych powinni ocenić incydent operacyjny lub incydent związany z bezpieczeństwem na podstawie następujących kryteriów i leżących u ich podstaw wskaźników:

i. Transakcje objęte skutkami incydentu

Dostawcy usług płatniczych powinni określić całkowitą wartość transakcji objętych skutkami incydentu, jak również liczbę zagrożonych płatności jako odsetek zwykłego poziomu zrealizowanych transakcji płatniczych w stosunku do usług płatniczych objętych skutkami incydentu.

ii. Użytkownicy usług płatniczych objęci skutkami incydentu

Dostawcy usług płatniczych powinni określić liczbę użytkowników usług płatniczych objętych skutkami incydentu zarówno w ujęcie bezwzględnym, jak i jako odsetek całkowitej liczby użytkowników usług płatniczych.

iii. Naruszenie bezpieczeństwa sieci lub systemów informatycznych

Dostawcy usług płatniczych powinni określić, czy jakiekolwiek działanie złośliwe zagroziło bezpieczeństwu sieci lub systemów informatycznych związanych ze świadczeniem usług płatniczych.

iv. Przestój w świadczeniu usług

Dostawcy usług płatniczych powinni określić okres, w którym usługa prawdopodobnie będzie niedostępna dla użytkownika usług płatniczych lub w którym zlecenie płatnicze – w rozumieniu art. 4 ust. 13 dyrektywy PSD2 – nie może zostać zrealizowane przez dostawcę usług płatniczych.

v. Skutek ekonomiczny

Dostawcy usług płatniczych powinni określić całościowy koszt pieniężny związany z incydentem, uwzględniając zarówno wartość bezwzględną jak i, gdy ma to zastosowanie, stosunkowe znaczenie takich kosztów do wielkości dostawcy usług płatniczych (tj. kapitału Tier I dostawcy usług płatniczych).

vi. Przekazanie na wyższy szczebel

Dostawcy usług płatniczych powinni ustalić, czy incydent ten został lub prawdopodobnie zostanie zgłoszony ich kadrze kierowniczej.

vii. Inni dostawcy usług płatniczych lub ważna infrastruktura, potencjalnie objęci skutkami incydentu

Dostawcy usług płatniczych powinni określić systemowe skutki, jakie incydent prawdopodobnie wywoła, tj. możliwość rozszerzenia się poza początkowo objętego skutkami incydentu dostawcę usług płatniczych na innych dostawców usług płatniczych, infrastrukturę rynku finansowego i/lub systemy płatności.

viii. Skutek reputacyjny

Dostawcy usług płatniczych powinni określić, jak incydent może podważyć zaufanie użytkowników do samego dostawcy usług płatniczych oraz, ogólnie, do danej usługi lub do całego rynku.

1.3. Dostawcy usług płatniczych powinni obliczyć wartość wskaźników zgodnie z następującą metodyką:

i. Transakcje objęte skutkami incydentu

Zasadniczo dostawcy usług płatniczych powinni rozumieć jako „transakcje objęte skutkami incydentu" wszystkie transakcje krajowe i transgraniczne, na które incydent miał lub prawdopodobnie będzie miał bezpośredni lub pośredni wpływ, a w szczególności transakcje, których nie można było zainicjować lub przetworzyć, transakcje, w odniesieniu do których zmieniono treść wiadomości płatniczej, oraz transakcje, które zostały zamówione nieuczciwie (bez względu na to, czy środki zostały odzyskane czy nie) lub w przypadku których właściwe wykonanie jest niemożliwe lub utrudnione w jakikolwiek inny sposób.

W przypadku incydentów operacyjnych wpływających na zdolność inicjowania lub przetwarzania transakcji dostawcy usług płatniczych powinni zgłaszać tylko incydenty trwające dłużej niż jedną godzinę. Czas trwania incydentu należy mierzyć od momentu wystąpienia incydentu do momentu przywrócenia regularnych działań/operacji do poziomu usług świadczonych przed incydentem.

Ponadto dostawcy usług płatniczych powinni rozumieć jako zwykły poziom transakcji płatniczych średnioroczną dzienną liczbę transakcji płatniczych krajowych i zagranicznych zrealizowanych w zakresie takich samych usług płatniczych, jak te, na które wpływ miał incydent, biorąc do wyliczenia rok poprzedni jako okres odniesienia. W przypadku gdy dostawcy usług płatniczych nie uznają tej wartości za reprezentatywną (np. w związku z sezonowością), powinni zamiast tego skorzystać z innej, bardziej reprezentatywnej miary i podać właściwemu organowi powód stosowania takiego podejścia w odpowiednim polu formularza (zob. załącznik).

ii. Użytkownicy usług płatniczych objęci skutkami incydentu

Dostawcy usług płatniczych powinni rozumieć jako „użytkowników usług płatniczych objętych skutkami incydentu" wszystkich klientów (konsumentów krajowych i zagranicznych oraz firmy krajowe i zagraniczne), którzy zawarli umowę z dostawcą usług płatniczych objętym skutkami incydentu, który udziela im dostępu do usługi płatniczej objętej skutkami incydentu, oraz którzy ponieśli lub prawdopodobnie poniosą konsekwencje wystąpienia incydentu. Aby określić liczbę użytkowników usług płatniczych, którzy mogli korzystać z usług płatniczych w okresie trwania incydentu, dostawcy usług płatniczych powinni odnieść się do szacunków opartych o przeszłą działalność.

W przypadku grup każdy dostawca usług płatniczych powinien wziąć pod uwagę wyłącznie swoich własnych użytkowników usług płatniczych. W przypadku dostawców usług płatniczych oferujących usługi operacyjne innym, taki dostawca usług płatniczych powinien wziąć pod uwagę wyłącznie swoich własnych użytkowników usług płatniczych (jeśli dotyczy), a dostawcy usług płatniczych otrzymujący takie usługi operacyjne powinni ocenić skutki incydentu w stosunku do swoich własnych użytkowników usług płatniczych.

W przypadku incydentów operacyjnych wpływających na zdolność inicjowania lub przetwarzania transakcji dostawcy usług płatniczych powinni zgłaszać tylko te incydenty, które dotyczą użytkowników usług płatniczych i trwają dłużej niż jedną godzinę. Czas trwania incydentu należy mierzyć od momentu wystąpienia incydentu do momentu przywrócenia regularnych działań/operacji do poziomu usług świadczonych przed incydentem.

Ponadto dostawcy usług płatniczych powinni przyjąć jako całkowitą liczbę użytkowników usług płatniczych zagregowaną liczbę krajowych i transgranicznych użytkowników usług płatniczych związanych umową w momencie incydentu (lub, ewentualnie, najnowszą dostępną liczbę) oraz z dostępem do danej usługi płatniczej, niezależnie od ich wielkości lub tego, czy są oni uznawani za aktywnych czy biernych użytkowników usług płatniczych.

iii. Naruszenie bezpieczeństwa sieci lub systemów informatycznych

Dostawcy usług płatniczych powinni określić, czy jakiekolwiek działanie złośliwe naruszyło dostępność, autentyczność, integralność lub poufność sieci lub systemów informatycznych (w tym danych) związanych ze świadczeniem usług płatniczych.

iv. Przestój w świadczeniu usług

Dostawcy usług płatniczych powinni uwzględnić okres czasu, w którym zadania, procesy lub kanały związane ze świadczeniem usług płatniczych są lub prawdopodobnie będą niesprawne, a w związku z tym uniemożliwiają (i) zainicjowanie i/lub realizację usługi płatniczej i/lub (ii) dostęp do rachunku płatniczego. Dostawcy usług płatniczych powinni wyliczyć czas przestoju w świadczeniu usług od momentu wystąpienia przestoju oraz powinni uwzględnić zarówno okresy czasu, kiedy prowadzą działalność pozwalającą na realizację usług płatniczych, jak również godziny zamknięcia i okresy prowadzenia konserwacji, jeśli dotyczy. Jeśli dostawcy usług płatniczych nie mogą określić momentu wystąpienia przestoju w świadczeniu usług, powinni oni wyjątkowo liczyć czas przestoju w świadczeniu usług od momentu wykrycia przestoju.

v. *Skutek ekonomiczny*

Dostawcy usług płatniczych powinni uwzględnić zarówno koszty, które mogą być związane z incydentem w sposób bezpośredni, jak i takie, które są związane z incydentem w sposób pośredni. Dostawcy usług płatniczych powinni wziąć pod uwagę między innymi wywłaszczone środki pieniężne lub aktywa, koszty wymiany sprzętu i oprogramowania, inne koszty ekspertyz sądowych i napraw, opłaty z tytułu niedopełnienia umownych zobowiązań, kary, zobowiązania zewnętrzne oraz utracone przychody. Odnośnie do kosztów pośrednich, dostawcy usług płatniczych powinni uwzględnić wyłącznie koszty, które są już znane lub których poniesienie jest bardzo prawdopodobne.

vi. *Przekazanie na wyższy szczebel*

Dostawcy usług płatniczych powinni rozważyć, czy w wyniku wywarcia przez incydent wpływu na usługi związane z płatnościami organ zarządzający zdefiniowany w Wytycznych EUNB w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT został lub prawdopodobnie będzie informowany, zgodnie z wytyczną 60 lit. d) Wytycznych EUNB w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT, o incydencie poza okresową procedurą powiadamiania i w sposób ciągły przez cały okres trwania incydentu. Ponadto dostawcy usług płatniczych powinni rozważyć, czy w wyniku wpływu incydentu na usługi związane z płatnościami uruchomiono lub prawdopodobnie zostanie uruchomiony tryb kryzysowy.

vii. *Inni dostawcy usług płatniczych lub określona infrastruktura, potencjalnie objęci skutkami incydentu*

Dostawcy usług płatniczych powinni ocenić wpływ incydentu na rynek finansowy rozumiany jako infrastruktura rynku finansowego i/lub systemy płatności, które wspierają takich dostawców i innych dostawców usług płatniczych. W szczególności dostawcy usług płatniczych powinni ocenić, czy incydent powtórzył się lub prawdopodobnie powtórzy się u innych dostawców usług płatniczych, czy ma lub prawdopodobnie będzie miał wpływ na płynne funkcjonowanie infrastruktury rynku finansowego oraz czy zagraża lub prawdopodobnie zagrozi właściwemu działaniu całego systemu finansowego. Dostawcy usług płatniczych powinni mieć na uwadze różne aspekty, takie jak: to, czy komponent lub oprogramowanie objęte skutkami incydentu są zastrzeżone czy ogólnie dostępne, czy

zagrożona sieć jest wewnętrzna czy zewnętrzna i czy dostawca usług płatniczych przestał lub prawdopodobnie przestanie wypełniać swoje zobowiązania w infrastrukturze rynku finansowego, którego jest członkiem.

viii. *Skutek reputacyjny*

Dostawcy usług płatniczych powinni uwzględnić poziom widoczności, jaki zgodnie z ich wiedzą incydent osiągnął lub prawdopodobnie osiągnie na rynku. W szczególności dostawcy usług płatniczych powinni uwzględnić prawdopodobieństwo wyrządzenia szkody społeczeństwu przez incydent jako znaczący wskaźnik możliwości wywarcia wpływu na reputację. Dostawcy usług płatniczych powinni wziąć pod uwagę, czy (i) użytkownicy usług płatniczych lub inni dostawcy usług płatniczych zgłaszali skargi dotyczące negatywnych skutków incydentu, (ii) incydent miał wpływ na widoczne procesy związane z usługami płatniczymi i dlatego prawdopodobnie będzie lub już jest relacjonowany w mediach (uwzględniając nie tylko media tradycyjne, takie jak gazety, ale również blogi, sieci społecznościowe, itp.), (iii) doszło lub prawdopodobnie dojdzie do naruszenia zobowiązań umownych, i w konsekwencji – do publikacji informacji o krokach prawnych podjętych wobec dostawcy usług płatniczych, (iv) doszło do naruszenia wymogów regulacyjnych, i w konsekwencji – do zastosowania środków lub sankcji nadzorczych, które zostały lub prawdopodobnie zostaną podane do publicznej wiadomości, oraz (v) taki sam incydent miał miejsce w przeszłości.

1.4. Dostawcy usług płatniczych powinni ocenić incydent, ustalając, dla każdego kryterium, czy stosowne progi określone w Tabeli 1 zostały lub prawdopodobnie zostaną osiągnięte, zanim incydent zostanie opanowany.

Tabela 1: Progi

Kryteria	Poziom niewielkiego wpływu	Poziom dużego wpływu
Transakcje objęte skutkami incydentu	> 10% zwykłego poziomu transakcji dostawcy usług płatniczych (pod względem liczby transakcji) **oraz** czas trwania incydentu > 1 godz.* **lub** > 500 000 EUR **oraz** czas trwania incydentu > 1 godz.*	> 25% zwykłego poziomu transakcji dostawcy usług płatniczych (pod względem liczby transakcji) **lub** > 15 000 000 EUR
Użytkownicy usług płatniczych objęci skutkami incydentu	> 5 000 **oraz** czas trwania incydentu > 1 godz.* **lub** > 10% użytkowników usług płatniczych dostawcy usług płatniczych	> 50 000 **lub** > 25% użytkowników usług płatniczych dostawcy usług płatniczych

	oraz czas trwania incydentu > 1 godz.*	
Przestój w świadczeniu usług	> 2 godzin	Nie dotyczy
Naruszenie bezpieczeństwa sieci lub systemów informatycznych	Tak	Nie dotyczy
Skutek ekonomiczny	Nie dotyczy	> Maks. (0,1% kapitału Tier I**, 200 000 EUR) **lub** >5 000 000 EUR
Przekazanie na wyższy szczebel	Tak	Tak, i istnieje prawdopodobieństwo uruchomienia trybu kryzysowego (lub równoważnego)
Inni dostawcy usług płatniczych lub określona infrastruktura, potencjalnie objęci skutkami incydentu	Tak	Nie dotyczy
Skutek reputacyjny	Tak	Nie dotyczy

* Próg czasu trwania incydentu przez okres dłuższy niż jedna godzina ma zastosowanie wyłącznie do incydentów operacyjnych, które wpływają na zdolność dostawcy usług płatniczych do inicjowania lub przetwarzania transakcji.

**Kapitał Tier I w rozumieniu art. 25 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniającego rozporządzenie (UE) nr 648/2012.

1.5. Dostawcy usług płatniczych powinni odnieść się do szacunków, jeśli nie posiadają faktycznych danych na poparcie swoich ocen odnośnie do tego, czy dany próg został lub prawdopodobnie zostanie osiągnięty, zanim incydent zostanie opanowany (np. może to mieć miejsce na wstępnym etapie prowadzenia dochodzenia).

1.6. Dostawcy usług płatniczych powinni dokonywać ciągłej oceny w okresie trwania incydentu w celu identyfikacji możliwej zmiany sytuacji czy to poprzez podniesienie jego wagi (z innego niż poważny na poważny) czy obniżenia jej (z poważnego na inny niż poważny). O każdym przeklasyfikowaniu incydentu z poważnego na inny niż poważny należy powiadomić właściwy organ zgodnie z wymogiem określonym w wytycznej 2.21 i bez zbędnej zwłoki.

Wytyczna 2: Procedura zgłaszania incydentów

2.1. Dostawcy usług płatniczych powinni zebrać wszystkie stosowne informacje, sporządzić zgłoszenie incydentu, wypełniając w tym celu formularz zawarty w załączniku 1, oraz przekazać je właściwemu organowi w państwie członkowskim pochodzenia. Dostawcy usług płatniczych powinni wypełnić wszystkie pola formularza zgodnie z instrukcjami zawartymi w załączniku.

2.2. Dostawcy usług płatniczych powinni korzystać z tego samego formularza przy składaniu wstępnych, okresowych i końcowych zgłoszeń dotyczących tego samego incydentu. Dostawcy usług płatniczych powinni zatem wypełniać jeden formularz w sposób stopniowy iw stosownych przypadkach aktualizować informacje przekazane wraz w poprzednich zgłoszeniach.

2.3. W stosownym przypadku dostawcy usług płatniczych powinni również przedstawić właściwemu organowi w ich państwie członkowskim pochodzenia kopię informacji, które zostały lub zostaną przekazane ich użytkownikom, zgodnie z drugim akapitem art. 96 ust. 1 dyrektywy PSD2, gdy tylko będą dostępne.

2.4. Dostawcy usług płatniczych powinni, na wniosek właściwego organu w państwie członkowskim pochodzenia, dostarczyć wszelkie dodatkowe dokumenty uzupełniające przedłożone informacje za pomocą standardowego formularza. Dostawcy usług płatniczych powinni podejmować działania w związku z wszelkimi wnioskami właściwego organu w państwie członkowskim pochodzenia o dostarczenie dodatkowych informacji lub wyjaśnień dotyczących już przedłożonej dokumentacji.

2.5. Wszelkie dodatkowe informacje zawarte w dokumentach dostarczonych przez dostawców usług płatniczych właściwemu organowi, z inicjatywy dostawcy usług płatniczych lub na wniosek właściwego organu zgodnie z wytyczną 2.4, powinny zostać uwzględnione przez dostawcę usług płatniczych w formularzu określonym w wytycznej 2.1.

2.6. Dostawcy usług płatniczych powinni przez cały czas zapewniać poufność, integralność i odpowiednie uwierzytelnienie informacji przekazywanych właściwym organom w ich państwie członkowskim pochodzenia.

Zgłoszenie wstępne

2.7. Dostawcy usług płatniczych powinni przekazać właściwemu organowi w państwie członkowskim pochodzenia zgłoszenie wstępne, jeśli wykryto po raz pierwszy poważny incydent operacyjny lub poważny incydent związany z bezpieczeństwem. Właściwe organy powinny bez zbędnej zwłoki potwierdzić otrzymanie zgłoszenia wstępnego i przypisać niepowtarzalny kod referencyjny jednoznacznie identyfikujący incydent. Dostawcy usług płatniczych powinni wskazać ten kod referencyjny przy składaniu aktualizacji zgłoszenia wstępnego lub zgłoszeń okresowych i końcowych dotyczących tego samego incydentu, chyba że zgłoszenia okresowe i końcowe są przedkładane razem ze zgłoszeniem wstępnym.

2.8. Dostawcy usług płatniczych powinni przesłać zgłoszenie wstępne właściwemu organowi w ciągu czterech godzin od momentu zaklasyfikowania incydentu operacyjnego lub incydentu związanego z bezpieczeństwem jako poważnego. Jeżeli wiadomo, że kanały zgłaszania nieprawidłowości właściwego organu nie są dostępne lub sprawne w tym czasie, dostawcy usług płatniczych powinni przesłać zgłoszenie wstępne, gdy tylko kanały staną się ponownie dostępne lub sprawne.

2.9. Dostawcy usług płatniczych powinni dokonać klasyfikacji incydentu zgodnie z wytycznymi 1.1 i 1.4 w odpowiednim czasie po wykryciu incydentu, jednak nie później niż 24 godziny po wykryciu incydentu, i bez zbędnej zwłoki po udostępnieniu dostawcy usług płatniczych informacji wymaganych do klasyfikacji incydentu. Jeżeli klasyfikacja incydentu wymaga dłuższego czasu, dostawcy usług płatniczych powinni wyjaśnić w zgłoszeniu wstępnym przedłożonym właściwemu organowi przyczyny takiego stanu rzeczy.

2.10. Dostawcy usług płatniczych powinni również przedłożyć właściwemu organowi w państwie członkowskim pochodzenia zgłoszenie wstępne w przypadku, gdy poprzedni incydent inny niż poważny został sklasyfikowany jako poważny incydent. W tym szczególnym przypadku dostawcy usług płatniczych powinni przesłać właściwemu organowi zgłoszenie wstępne niezwłocznie po zidentyfikowaniu zmiany sytuacji lub, jeśli wiadomo, że kanały sprawozdawczości właściwych organów nie są dostępne lub sprawne w danym momencie, tak szybko jak staną się znowu dostępne lub sprawne.

2.11. Dostawcy usług płatniczych powinni zamieścić w swoim zgłoszeniu wstępnym informacje nagłówkowe (tj. część A formularza), przedstawiając w ten sposób podstawowe cechy incydentu oraz jego oczekiwane skutki na podstawie informacji dostępnych natychmiast po zakwalifikowaniu go jako poważnego. Jeśli faktyczne dane nie są dostępne, dostawcy usług płatniczych powinni skorzystać z szacunków.

Zgłoszenie okresowe

2.12. Dostawcy usług płatniczych powinni przedłożyć zgłoszenie okresowe po przywróceniu regularnej działalności i powrocie przedsiębiorstwa do normalnego stanu, informując o tej okoliczności właściwy organ. Dostawcy usług płatniczych powinni uznać, że ich przedsiębiorstwo powróciło do normalnego stanu, jeśli przywrócono działalność/operacje przy takim samym poziomie usług/warunków określonych przez dostawcę usług płatniczych lub zewnętrznie w umowie o gwarantowanym poziomie usług (czas przetwarzania, przepustowość, wymogi bezpieczeństwa itp.) oraz gdy środki awaryjne nie są już stosowane. Zgłoszenie okresowe powinno zawierać bardziej szczegółowy opis incydentu i jego skutków (część B formularza).

2.13. Jeżeli regularna działalność nie została jeszcze przywrócona, dostawcy usług płatniczych powinni przekazać właściwemu organowi zgłoszenie okresowe w terminie trzech dni roboczych od przekazania zgłoszenia wstępnego.

2.14. Dostawcy usług płatniczych powinni aktualizować informacje już podane w częściach A i B formularza, gdy tylko uzyskają wiedzę o istotnych zmianach, jakie nastąpiły od momentu złożenia poprzedniego zgłoszenia (np. czy incydent nasilił się lub osłabł, nowe stwierdzone powody lub czynności podjęte w celu naprawienia problemu). Obejmuje to przypadek, w którym incydent nie został opanowany w ciągu trzech dni roboczych, co wymagałoby od dostawców usług płatniczych przedłożenia dodatkowego zgłoszenia okresowego. W każdym

przypadku dostawcy usług płatniczych powinni przekazać dodatkowe zgłoszenie okresowe na wniosek właściwego organu w państwie członkowskim pochodzenia.

2.15. Podobnie jak w przypadku zgłoszeń wstępnych, jeżeli faktyczne dane nie są dostępne, dostawcy usług płatniczych powinni korzystać z szacunków.

2.16. Jeżeli przedsiębiorstwo powróci do normalnego stanu przed upływem czterech godzin od zaklasyfikowania incydentu jako poważnego, dostawcy usług płatniczych powinni dążyć do jednoczesnego przekazania zarówno zgłoszenia wstępnego, jak i okresowego (tj. wypełnienia części A i B formularza) w terminie czterech godzin.

Zgłoszenie końcowe

2.17. Dostawcy usług płatniczych powinni przekazać zgłoszenie końcowe po przeprowadzeniu analizy przyczyn źródłowych (niezależnie od tego, czy wdrożono już środki łagodzące lub określono ostateczną przyczynę źródłową) i dostępne są rzeczywiste dane liczbowe zastępujące wszelkie potencjalne szacunki.

2.18. Dostawcy usług płatniczych powinni przedstawić właściwemu organowi zgłoszenie końcowe w terminie nieprzekraczającym 20 dni roboczych od uznania, że przedsiębiorstwo powróciło do normalnego stanu. Dostawcy usług płatniczych, który potrzebują wydłużenia tego terminu (np. jeśli nie są jeszcze dostępne faktyczne dane dotyczące wpływu incydentu lub przyczyny źródłowe nie zostały jeszcze zidentyfikowane), powinni skontaktować się z właściwym organem przed upływem tego terminu i przedstawić odpowiednie uzasadnienie opóźnienia, jak również nowy przewidywany termin złożenia zgłoszenia końcowego.

2.19. Jeśli dostawcy usług płatniczych mogą przekazać wszystkie informacje wymagane w zgłoszeniu końcowym (tj. część C formularza) w terminie czterech godzin od momentu wykrycia incydentu, powinni oni dążyć do przedstawienia informacji odnoszących się do zgłoszenia wstępnego, zgłoszenia okresowego i zgłoszenia końcowego łącznie.

2.20. Dostawcy usług płatniczych powinni dążyć do przedstawienia w zgłoszeniach końcowych pełnych informacji, tj. (i) faktycznych danych dotyczących wpływu incydentu zamiast szacunków (jak również innych aktualizacji wymaganych w częściach A i B formularza) oraz (ii) części C formularza, która zawiera wskazanie przyczyny źródłowej, jeśli jest już znana, oraz streszczenia środków zastosowanych lub które planuje się zastosować w celu usunięcia problemu i uniemożliwienia jego wystąpienia w przyszłości.

2.21. Dostawcy usług płatniczych powinni również przesłać zgłoszenie końcowe, jeżeli w wyniku ciągłej oceny incydentu stwierdzą, że już zgłoszony incydent nie spełnia już kryteriów incydentu poważnego i przewiduje się, że nie spełni ich przed opanowaniem incydentu. W takim przypadku dostawcy usług płatniczych powinni przesłać zgłoszenie końcowe niezwłocznie po wykryciu takich okoliczności oraz w każdym przypadku – w terminie na złożenie następnego zgłoszenia. W tej szczególnej sytuacji, zamiast wypełniać

część C formularza, dostawcy usług płatniczych powinni zaznaczyć kwadrat „incydent przeklasyfikowany na inny niż poważny" i podać uzasadnienie tego przeklasyfikowania.

Wytyczna 3: Delegowanie i konsolidacja zgłoszeń

3.1. Jeśli jest to dozwolone przez właściwy organ, dostawcy usług płatniczych, którzy chcą delegować obowiązki w zakresie zgłaszania incydentów wynikające z dyrektywy PSD2 osobie trzeciej, powinni poinformować o tym właściwy organ w państwie członkowskim pochodzenia i zapewnić spełnienie następujących warunków:

a. Formalna umowa lub, w stosownych przypadkach, istniejące wewnętrzne ustalenia w ramach grupy pomiędzy dostawcą usług płatniczych a osobą trzecią będące podstawą delegowania obowiązków w zakresie zgłaszania incydentów jednoznacznie określają obowiązki przydzielone wszystkim stronom. W szczególności wyraźnie stanowią, że bez względu na możliwe delegowanie obowiązków w zakresie zgłaszania incydentów, dostawca usług płatniczych objęty skutkami incydentu pozostaje w pełni odpowiedzialny za spełnienie wymogów określonych w art. 96 dyrektywy PSD2 oraz za treść informacji przekazanych właściwemu organowi w państwie członkowskim pochodzenia.

b. Delegowanie obowiązków podlega wymogom dotyczącym zlecania w ramach outsourcingu ważnych funkcji operacyjnych określonych w:

i. art. 19 ust. 6 dyrektywy PSD2 w odniesieniu do instytucji płatniczych i instytucji pieniądza elektronicznego, stosując odpowiednio art. 3 dyrektywy 2009/110/WE lub

ii. wytycznych EUNB w sprawie outsourcingu (EBA/GL/2019/02) w odniesieniu do wszystkich dostawców usług płatniczych.

c. Informacje są przekazywane właściwemu organowi w państwie członkowskim pochodzenia z wyprzedzeniem, a w każdym przypadku zgodnie z terminami i procedurami określonymi przez właściwy organ, jeśli ma to zastosowanie.

d. Poufność danych szczególnie chronionych oraz jakość, spójność, integralność i wiarygodność informacji, które zostaną przekazane właściwemu organowi, są właściwie zapewnione.

3.2. Dostawcy usług płatniczych, którzy chcą zezwolić wyznaczonej osobie trzeciej na wykonanie obowiązków w zakresie zgłaszania incydentów w sposób skonsolidowany (tj. poprzez przekazanie jednego pojedynczego zgłoszenia odnoszącego się do kilku dostawców usług płatniczych objętych skutkami tego samego poważnego incydentu operacyjnego lub incydentu związanego z bezpieczeństwem), powinni poinformować o tym właściwy organ w państwie członkowskim pochodzenia, podać dane kontaktowe w pozycji „DUP objęci skutkami incydentu" w formularzu oraz zapewnić spełnienie następujących warunków:

a. należy włączyć niniejsze postanowienie do umowy stanowiącej podstawę do delegowania obowiązków w zakresie zgłaszania incydentów;

b. należy uzależnić przekazanie zgłoszenia skonsolidowanego od tego, czy incydent został spowodowany przez zakłócenie usług świadczonych przez osobę trzecią;

c. należy ograniczyć zakres zgłoszeń skonsolidowanych do dostawców usług płatniczych ustanowionych w tym samym państwie członkowskim;

d. należy przedstawić wykaz wszystkich dostawców usług płatniczych objętych skutkami incydentu;

e. należy zapewnić, że osoba trzecia oceni stopień istotności incydentu dla każdego dostawcy usług płatniczych objętego skutkami incydentu oraz uwzględnić w zgłoszeniu sprawozdaniu wyłącznie tych dostawców usług płatniczych, w przypadku których incydent został sklasyfikowany jako poważny; ponadto należy zapewnić, że w przypadku wątpliwości dostawca usług płatniczych zostanie ujęty w zgłoszeniu skonsolidowanym, o ile nie istnieją dowody wskazujące na to, że nie powinien być uwzględniony.

f. jeśli w formularzu znajdują się pola, w których wspólna odpowiedź nie jest możliwa (np. części B2, B4 lub C3), należy zapewnić aby osoba trzecia albo (i) wypełniała je osobno dla każdego dostawcy usług płatniczych objętego skutkami incydentu, określając dalej tożsamość każdego dostawcy usług płatniczych, do którego informacje się odnoszą, albo (ii) korzystała z wartości skumulowanych, odnotowanych lub szacowanych w odniesieniu do dostawców usług płatniczych;

g. osoba trzecia przez cały czas przekazuje dostawcy usług płatniczych wszystkie stosowne informacje dotyczące incydentu oraz wszystkich kontaktów, które osoba trzecia odbywa z właściwym organem, oraz ich treści, jednak wyłącznie w takim stopniu, w którym jest to możliwe bez naruszania poufności informacji, które odnoszą się do innych dostawców usług płatniczych

3.3. Dostawcy usług płatniczych nie powinni delegować swoich obowiązków w zakresie zgłaszania incydentów, zanim nie poinformują o tym właściwego organu w państwie członkowskim pochodzenia ani też po otrzymaniu informacji, że umowa w sprawie outsourcingu nie spełnia wymogów określonych w wytycznej 3.1 lit. b).

3.4. Dostawcy usług płatniczych, którzy chcą cofnąć delegowanie obowiązków w zakresie zgłaszania incydentów, powinni przekazać tą decyzję właściwemu organowi w państwie członkowskim pochodzenia w terminach i zgodnie z procedurami określonymi przez taki organ. Dostawcy usług płatniczych powinni również informować właściwy organ w państwie członkowskim pochodzenia o wszelkich istotnych zmianach mających wpływ na wyznaczoną stronę trzecią i na jej zdolność do wypełniania obowiązków w zakresie zgłaszania incydentów.

3.5. Dostawcy usług płatniczych powinni w znaczącym stopniu wypełnić obowiązki w zakresie zgłaszania incydentów bez korzystania z pomocy zewnętrznej, jeśli wyznaczona osoba trzecia nie poinformuje właściwego organu w państwie członkowskim pochodzenia o poważnym incydencie operacyjnym lub poważnym incydencie związanym z bezpieczeństwem zgodnie z art. 96 dyrektywy PSD2 oraz niniejszymi wytycznymi. Ponadto dostawcy usług płatniczych powinni zapewnić, aby incydent nie został zgłoszony dwa razy, indywidualnie przez danego dostawcę usług płatniczych, a drugi raz – przez osobę trzecią.

3.6. Dostawcy usług płatniczych powinni zapewnić, aby w przypadku gdy incydent jest spowodowany przez zakłócenie usług świadczonych przez dostawcę usług technicznych (lub infrastruktury), które ma wpływ na wielu DUP, delegowanie obowiązków w zakresie zgłaszania incydentów odnosiło się do indywidualnych danych dostawcy usług płatniczych (z wyjątkiem przypadku zgłoszenia skonsolidowanego).

Wytyczna 4: Polityka operacyjna i bezpieczeństwa

4.1. Dostawcy usług płatniczych powinni zapewnić, aby ich ogólna polityka operacyjna i bezpieczeństwa wyraźnie określała wszystkie obowiązki dotyczące zgłaszania incydentów zgodnie z dyrektywą PSD2, jak również procesy wprowadzone w celu spełnienia wymogów określonych w niniejszych wytycznych.

5. Wytyczne skierowane do właściwych organów dotyczące kryteriów oceny znaczenia incydentu oraz informacji o zgłoszeniach incydentów udostępnianych innym organom krajowym

Wytyczna 5: Ocena znaczenia incydentu

5.1. Właściwe organy w państwie członkowskim pochodzenia powinny ocenić znaczenie poważnego incydentu operacyjnego lub incydentu związanego z bezpieczeństwem dla innych organów krajowych, opierając się na własnej opinii ekspertów i stosując następujące kryteria jako główne wskaźniki znaczenia tego incydentu:

a. Przyczyny incydentu leżą w gestii regulacyjnej innego organu krajowego (tj. w zakresie jego kompetencji).
b. Skutki incydentu mają wpływ na cele innego organu krajowego (np. ochronę stabilności finansowej).
c. Incydent ma lub może mieć wpływ na użytkowników usług płatniczych na szeroką skalę.
d. Incydent prawdopodobnie będzie lub już był szeroko relacjonowany w mediach.

5.2. Właściwe organy w państwie członkowskim pochodzenia powinny dokonywać ciągłej oceny w okresie trwania incydentu, aby zidentyfikować każdą możliwą zmianę powodującą, że incydent będzie miał znaczenie, które poprzednio nie było mu przypisywane.

Wytyczna 6: Informacje, które należy udostępnić

6.1. Niezależnie od wszelkich innych wymogów prawnych dotyczących wymiany informacji dotyczących incydentów z innymi organami krajowymi właściwe organy powinny przekazywać informacje o poważnych incydentach operacyjnych lub incydentach związanych z bezpieczeństwem odpowiednim organom krajowym określonym w wyniku zastosowania wytycznej 5.1, co najmniej w momencie otrzymania zgłoszenia wstępnego (lub, ewentualnie, zgłoszenia, które doprowadziło do wymiany informacji) oraz po uzyskaniu powiadomienia o tym, że przedsiębiorstwo powróciło do normalnego stanu (tj. zgłoszenie okresowe).

6.2. Właściwe organy powinny przekazywać odpowiednim organom krajowym informacje niezbędne do uzyskania jasnego obrazu wydarzeń i potencjalnych konsekwencji. W tym celu

powinny one przedstawić co najmniej informacje dostarczone przez dostawcę usług płatniczych w następujących polach formularza (w zgłoszeniu wstępnym lub okresowym):

- Data i godzina zaklasyfikowania incydentu jako poważnego,
- Data i godzina wykrycia incydentu,
- Data i godzina rozpoczęcia incydentu,
- Data i godzina, kiedy incydent został lub przewiduje się, że zostanie opanowany,
- Krótki opis incydentu (w tym jawne części szczegółowego opisu),
- Krótki opis środków podjętych lub planowanych w celu opanowania incydentu,
- Opis, w jaki sposób incydent może wpłynąć na innych dostawców usług płatniczych lub infrastrukturę płatniczą,
- Opis (ewentualnego) przekazu medialnego,
- Przyczyna incydentu.

6.3. Właściwe organy powinny w razie potrzeby dokonać właściwej anonimizacji i pominąć wszelkie informacje, które mogłyby podlegać ograniczeniom związanym z poufnością lub własnością intelektualną, zanim udostępnią właściwym organom krajowym wszelkie informacje związane z incydentami. Właściwe organy powinny jednak przekazać odpowiednim organom krajowym nazwę i adres zgłaszającego dostawcy usług płatniczych, jeżeli organy te mogą zagwarantować, że informacje będą traktowane jako poufne.

6.4. Właściwe organy powinny zawsze zapewniać poufność i integralność przechowywanych i udostępnianych informacji oraz ich odpowiednie uwierzytelnianie wobec właściwych organów krajowych. W szczególności właściwe organy powinny traktować wszystkie informacje otrzymane na podstawie niniejszych wytycznych zgodnie z obowiązkiem zachowania tajemnicy zawodowej określonym w dyrektywie PSD2, bez uszczerbku dla obowiązującego prawa Unii i wymogów krajowych.

6. Wytyczne skierowane do właściwych organów dotyczące kryteriów oceny odpowiednich informacji o zgłoszeniach incydentów, które mają być udostępniane EUNB i EBC, oraz formatu i procedur ich przekazywania

Wytyczna 7: Informacje, które należy udostępnić

7.1. Właściwe organy powinny zawsze przekazywać EUNB i EBC wszystkie zgłoszenia otrzymane bezpośrednio lub pośrednio od dostawców usług płatniczych objętych skutkami poważnego incydentu operacyjnego lub incydentu związanego z bezpieczeństwem, korzystając w tym celu ze standardowego pliku dostępnego na stronie internetowej EUNB.

Wytyczna 8: Komunikacja

8.1. Właściwe organy powinny przez cały czas zapewniać poufność i integralność informacji przechowywanych i udostępnianych EUNB i EBC oraz ich odpowiednie uwierzytelnienie wobec EUNB i EBC. W szczególności właściwe organy powinny traktować wszystkie informacje otrzymane na podstawie niniejszych wytycznych zgodnie z obowiązkami zachowania tajemnicy służbowej określonymi w dyrektywie PSD2, bez uszczerbku dla obowiązującego prawa Unii i wymogów krajowych.

8.2. Aby uniknąć opóźnień w przekazywaniu informacji o incydentach do EUNB lub EBC oraz aby pomóc w zminimalizowaniu ryzyka zakłóceń operacyjnych, właściwe organy powinny korzystać z odpowiednich środków komunikacji.

Załącznik – Formularz zgłoszeń dla dostawców usług płatniczych

Zgłoszenie wstępne

Wstępne sprawozdanie	W ciągu 4 godzin po zaklasyfikowaniu incydentu jako poważnego	Zresetować rozwijane wybory
Data sprawozdania (DD/MM/RRRR)		Godzina (GG:MM)
Kod referencyjny incydentu		

A – Sprawozdanie wstępne						
A 1 – OGÓLNE DANE						
Rodzaj sprawozdania						
Rodzaj sprawozdania						
Dostawca usług płatniczych (DUP) objęty incydentem						
Nazwa DUP						
Krajowy numer identyfikacyjny DUP						
Główny podmiot grupy, jeśli dotyczy						
Kraj/kraje objęte skutkami incydentu	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ LI ☐ GR ☐ HR ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Główna osoba wyznaczona do kontaktów		E-mail		Telefon		
Dodatkowa osoba do kontaktu		E-mail		Telefon		
Podmiot zgłaszający (proszę wypełnić tę cześć, jeśli podmiot zgłaszający nie jest DUP objętym skutkami incydentu, w przypadku zlecenia składania sprawozdań)						
Nazwa jednostki zgłaszającej						
Krajowy numer identyfikacyjny						
Główna osoba wyznaczona do kontaktów		E-mail		Telefon		
Dodatkowa osoba do kontaktu		E-mail		Telefon		
A 2 – WYKRYCIE INCYDENTU i KLASYFIKACJA						
Data i godzina wykrycia incydentu (DD/MM/RRRR GG:MM)						
Data i godzina klasyfikacji incydentu (DD/MM/RRRR GG:MM)						
Incydent został wykryty przez		Jeśli „Inny", proszę wyjaśnić:				
Rodzaj incydentu						
Kryteria uruchamiania zgłoszenia poważnego incydentu	☐ Transakcje objęte	☐ Użytkownicy usług płatniczych objęci	☐ Przerwa w świadczeniu	☐ Naruszenie bezpieczeństwa sieci lub systemów informatycznych	☐ Wpływ ekonomiczny	☐ Wysoki poziom wewnętrznej eskalacji	☐ Inni DUP lub określona infrastruktura, potencjalnie objęci skutkami incydentu	☐ Wpływ na reputację
Krótki i ogólny opis incydentu						
Wpływ w innych państwach członkowskich UE, w stosownych przypadkach						
Składanie sprawozdań innym organom		Jeśli „Tak", proszę wyjaśnić:				
Przyczyny opóźnienia w przedłożeniu wstępnego sprawozdania						

Zgłoszenie okresowe

Sprawozdanie z poważnego incydentu

Sprawozdanie okresowe | Maksymalnie 3 dni robocze od przedłożenia wstępnego sprawozdania | Zresetować rozwijane wybory

Data sprawozdania *(DD/MM/RRRR)* | Godzina *(GG:MM)*

Kod referencyjny incydentu

B – Sprawozdanie okresowe

B 1 – DANE OGÓLNE

Bardziej szczegółowy opis incydentu:	
W czym konkretnie leży problem?	
Jak rozpoczął się incydent?	
Jak się rozwijał?	
Jakie są skutki (w szczególności dla użytkowników usług płatniczych)?	
Czy o incydencie poinformowano użytkowników usług płatniczych?	Jeśli „Tak", proszę wyjaśnić:
Czy był(-y) związany(-e) z poprzednim(-i) incydentem(-ami)?	Jeśli „Tak", proszę wyjaśnić:
Czy inni usługodawcy/osoby trzecie mieli wpływ na sytuację lub byli zaangażowani?	Jeśli „Tak", proszę wyjaśnić:
Czy rozpoczęto zarządzanie kryzysowe (wewnętrzne lub zewnętrzne)?	Jeśli „Tak", proszę wyjaśnić:
Data i godzina początku incydentu (jeśli została już określona) *(DD/MM/RRRR GG:MM)*	
Data i godzina, kiedy incydent został lub przewiduje się, że zostanie usunięty *(DD/MM/RRRR GG:MM)*	
Obszary funkcjonalne objęte skutkami incydentu	☐ Uwierzytelnianie/autoryzacja ☐ Rozrachunek ☐ Komunikacja ☐ Rozrachunek pośredni ☐ Rozliczanie ☐ Inne — Jeśli „Inny", proszę wyjaś
Zmiany wprowadzone do poprzednich sprawozdań	

B 2 – KLASYFIKACJA INCYDENTU / INFORMACJE O INCYDENCIE

Transakcje objęte skutkami incydentu [2]	Poziom oddziaływania Liczba transakcji objętych skutkami incydentu Jako % zwykłej liczby transakcji Wartość transakcji objętych incydentem w EUR Czas trwania incydentu (dotyczy wyłącznie incydentów operacyjnych) Uwagi:
Użytkownicy usług płatniczych objęci skutkami incydentu [3]	Poziom oddziaływania Liczba użytkowników usług płatniczych objętych skutka Jako % wszystkich użytkowników usług płatniczych
Naruszenie bezpieczeństwa sieci lub systemów informatycznych	Opisać w jaki sposób miało to wpływ na sieć lub systemy informatyczne
Przerwa w świadczeniu usług	Całkowity czas przerwy w świadczeniu usług — Dni: — Godziny: — Minuty:
Wpływ ekonomiczny	Poziom oddziaływania Koszty bezpośrednie w EUR Koszty pośrednie w EUR
Wysoki poziom wewnętrznej eskalacji	Proszę opisać poziom szczebla, na który przekazana została informacja o incydencie, wskazując, czy spowodowała lub prawdopodobnie spowoduje wprowadzenie planu kryzysowego (lub jego odpowiednika) i, jeśli tak, proszę go opisać
Inni DUP lub określona infrastruktura, potencjalnie objęci skutkami incydent	Proszę opisać, jak incydent mógł wpłynąć na innych DUP i/lub infrastrukturę
Wpływ na reputację	Proszę opisać, jak incydent mógł wpłynąć na reputację DUP (np. relacje medialne, informacja o działaniach prawnych lub potencjalne naruszenie przepisów prawnych, itp.)

B 3 – OPIS INCYDENTU

Rodzaj incydentu	
Przyczyna wystąpienia incydentu	☐ Prowadzone dochodzenie ☐ Działanie złośliwe ☐ Awaria procesu ☐ Awaria systemu ☐ Błędy ludzkie ☐ Zdarzenia zewnętrzne ☐ Inne — Jeśli „Inny", proszę wyjaśnić:
Czy incydent miał wpływ bezpośredni czy za pośrednictwem dostawcy usług?	Jeśli pośredni, proszę podać nazwę dostawcy usług:

B 4 – WPŁYW INCYDENTU

Ogólny wpływ	☐ Integralność ☐ Poufność ☐ Dostępność ☐ Uwierzytelnienie
Kanały handlowe objęte skutkami incydentu	☐ Oddziały ☐ Bankowość telefoniczna ☐ Punkt sprzedaży ☐ Bankowość elektroniczna ☐ Bankowość mobilna ☐ Inne ☐ handel elektroniczny: ☐ Bankomaty Jeśli „Inny", proszę wyjaśnić:
Usługi płatnicze objęte skutkami incydentu	☐ Lokowanie gotówki na koncie płatniczym ☐ Polecenia przelewu ☐ Usługi przekazu ☐ Podjęcie gotówki z konta płatniczego ☐ Polecenia zapłaty ☐ Usługi inicjowania ☐ Operacje wymagane do obsługi rachunku płatniczego ☐ Płatności kartami ☐ Usługi dostępu do informacji o rachunku ☐ Nabywanie instrumentów płatniczych ☐ Wydawanie instrumentów płatniczych

B 5 – MINIMALIZACJA SKUTKÓW INCYDENTU

Jakie czynności/środki zostały podjęte dotychczas lub są planowane w celu przywrócenia sytuacji po nastąpieniu incydentu?	
Czy włączone zostały plan zapewniający ciągłość działania i/lub plan odtworzeniowy?	
Jeśli tak, kiedy? *(DD/MM/RRRR, GG:MM)*	
Jeśli tak, proszę opisać	

Zgłoszenie końcowe

Sprawozdanie z poważnego incydentu

Proszę wybrać rodzaj sprawozdania: [ ]

w ciągu 20 dni roboczych od przedłożenia sprawozdania okresowego

Proszę opisać: (Dotyczy zdarzeń ponownie sklasyfikowanych jako poważne)

Zresetować/rozwijane wybory

Data sprawozdania *(DD/MM/RRRR)* | Godzina *(GG:MM)*

Kod referencyjny incydentu

C – Sprawozdanie końcowe

Jeśli nie przesłano sprawozdania okresowego, proszę również wypełnić część B

C 1 – OGÓLNE DANE

Aktualizacja informacji zawartych w sprawozdaniu wstępnym i sprawozdaniu okresowym	
Zmiany wprowadzone do poprzednich sprawozdań	
Inne stosowne informacje	
Czy wprowadzono wszystkie oryginalne kontrole? Jeśli „Nie", określić, które kontrole i dodatkowy okres czasu do ich przywrócenia	

C 2 – ANALIZA PRZYCZYN PIERWOTNYCH I DZIAŁANIA NASTĘPCZE

Jaka była pierwotna przyczyna (jeśli jest już znana)?	☐ Działanie złośliwe ☐ Awaria procesu ☐ Awaria systemu ☐ Błąd ludzki ☐ Incydenty zewnętrzne ☐ Inne
Proszę określić:	☐ Kod złośliwy ☐ Gromadzenie informacji ☐ Wtargnięcia ☐ Ataki typu „blokada usługi" ☐ Celowe działania wewnętrzne ☐ Zamierzone zewnętrzne uszkodzenia fizyczne ☐ Bezpieczeństwo treści informacyjnych ☐ Działania oszukańcze ☐ Inne ☐ Niedociągnięcia w zakresie monitorowania i kontroli ☐ Kwestie związane z komunikacją ☐ Niewłaściwe operacje ☐ Nieodpowiednie zdolności w zakresie zarządzania ☐ Nieadekwatność wewnętrznych procedur i dokumentacji ☐ Kwestie związane z ☐ Inne ☐ Awaria sprzętu ☐ Awaria sieci ☐ Kwestie związane ☐ Awaria oprogramowania/aplikacji ☐ Szkody fizyczne ☐ Inne ☐ Niezamierzone ☐ Bezczynność ☐ Niewystarczające zasoby ☐ Inne ☐ Awaria dostawcy/dostawcy usług technicznych ☐ Siła wyższa ☐ Inne Jeśli „Inny", proszę wyjaśnić:
Inne istotne informacje na temat pierwotnej przyczyny	
Główne działania/środki naprawcze podjęte lub planowane w celu uniknięcia ponownego nastąpienia incydentu w przyszłości, jeśli są znane	

C 3 – DODATKOWE INFORMACJE

Czy informacja o incydencie została przekazana innym DUP dla celów informacyjnych?	Jeśli tak, proszę podać szczegóły:
Czy podjęte zostały jakiekolwiek kroki prawne w stosunku do DUP?	Jeśli tak, proszę podać szczegóły:
Ocena prawidłowego funkcjonowania systemów kontroli wewnętrznej	Proszę podać szczegóły:

INSTRUKCJA WYPEŁNIENIA FORMULARZA

Dostawcy usług płatniczych (DUP) powinni wypełnić odpowiednie części formularza, które w zależności od etapu składania zgłoszenia, będą zamieszczone w części A w przypadku zgłoszenia wstępnego, części B w przypadku zgłoszeń okresowych i części C w przypadku zgłoszenia końcowego. DUP powinni korzystać z tego samego wzoru przy składaniu wstępnych, okresowych i końcowych zgłoszeń dotyczących tego samego incydentu. Wszystkie pola są obowiązkowe, chyba że wyraźnie określono inaczej.

Nagłówek

Zgłoszenie wstępne: jest to pierwsze powiadomienie, które DUP przekazuje właściwemu organowi w państwie członkowskim pochodzenia.

Zgłoszenie okresowe: zawiera bardziej szczegółowy opis incydentu i jego skutków. Jest to aktualizacja zgłoszenia wstępnego (oraz, w stosownych przypadkach, poprzedniego zgłoszenia okresowego) na temat tego samego incydentu.

Zgłoszenie końcowe: jest to ostatnie zgłoszenie, które DUP prześle odnośnie do incydentu, ponieważ (i) analiza przyczyn źródłowych została już przeprowadzona i szacunki mogą zostać zastąpione rzeczywistymi danymi lub (ii) incydent nie jest już uważany za poważny.

Incydent przeklasyfikowany na inny niż poważny: incydent nie spełnia już kryteriów incydentu poważnego i nie przewiduje się, że będzie je spełniał przed jego opanowaniem. DUP powinni podać uzasadnienie przeklasyfikowania.

Data i godzina zgłoszenia: dokładna data i godzina przekazania zgłoszenia właściwemu organowi.

Kod referencyjny incydentu (ma zastosowanie do zgłoszeń okresowych i końcowych, a także do aktualizacji zgłoszenia wstępnego): kod referencyjny nadany przez właściwy organ w momencie pierwszego zgłoszenia w celu jednoznacznej identyfikacji incydentu. Każdy właściwy organ powinien umieścić jako prefiks 2-cyfrowy kod ISO [2]swojego państwa członkowskiego.

A - Zgłoszenie wstępne

A 1 - Ogólne

Rodzaj zgłoszenia:

Indywidualne: zgłoszenie odnosi się do jednego DUP.

Skonsolidowane: zgłoszenie odnosi się do kilku DUP, którzy korzystają z możliwości przekazania zgłoszenia skonsolidowanego. Pola w pozycji „DUP objęty skutkami incydentu" powinny być pozostawione puste (z wyjątkiem pola „Państwo/państwa objęte skutkami incydentu") oraz powinien zostać przedstawiony wykaz DUP uwzględnionych w zgłoszeniu poprzez wypełnienie odpowiedniej tabeli (Zgłoszenie skonsolidowane – wykaz DUP).

DUP objęty skutkami incydentu: odnosi się do DUP objętego skutkami incydentu.

Nazwa DUP: pełna nazwa DUP, który podlega procedurze zgłaszania incydentu, zgodnie ze stosownym oficjalnym rejestrem krajowym DUP.

Krajowy numer identyfikacyjny DUP: niepowtarzalny krajowy numer identyfikacyjny stosowany przez właściwy organ państwa członkowskiego pochodzenia w rejestrze krajowym do jednoznacznej identyfikacji DUP.

Główny podmiot grupy: w przypadku grup podmiotów określonych w art. 4 pkt 40 dyrektywy PSD2 proszę podać nazwę jednostki dominującej.

Kraj/kraje objęte skutkami incydentu: państwo lub państwa, w których nastąpiły skutki incydentu (np. skutkami jest objętych kilka oddziałów DUP znajdujących się w różnych krajach),

[2]Zob. kody krajów alfa-2 zgodnie z ISO-3166 na stronie https://www.iso.org/iso-3166-country-codes.html

niezależnie od wagi incydentu w innym kraju/krajach. Może być, ale nie musi taki sam jak państwo członkowskie pochodzenia.

Główna osoba do kontaktu: imię i nazwisko osoby odpowiedzialnej za zgłoszenie incydentu lub, jeśli zgłoszenie przekazuje osoba trzecia w imieniu DUP objętego skutkami incydentu, imię i nazwisko osoby odpowiedzialnej za wydział zarządzania incydentami/wydział zarządzania ryzykiem lub podobny wydział DUP objętego skutkami incydentu.

E-mail: adres poczty elektronicznej, na który w razie konieczności skierowane mogą zostać żądania dalszych wyjaśnień. Może to być prywatny lub służbowy adres e-mail.

Telefon do kontaktu: numer telefonu, za pomocą którego można w razie potrzeby kierować wszelkie prośby o dalsze wyjaśnienia. Może to być prywatny lub służbowy numer telefonu.

Dodatkowa osoba do kontaktu: imię i nazwisko innej osoby, z którą właściwy organ może się kontaktować z zapytaniem o incydent, jeśli główna osoba kontaktowa nie jest dostępna. Jeśli zgłoszenie przekazuje osoba trzecia w imieniu DUP objętego skutkami incydentu, imię i nazwisko innej osoby z wydziału zarządzania incydentami/wydziału zarządzania ryzykiem lub podobnego wydziału DUP objętego skutkami incydentu.

E-mail: adres poczty elektronicznej innej osoby kontaktowej, na który w razie konieczności skierowane mogą zostać żądania dalszych wyjaśnień. Może to być prywatny lub służbowy adres e-mail.

Telefon: numer telefonu innej osoby do kontaktu, pod który w razie konieczności można dzwonić z żądaniami dalszych wyjaśnień. Może to być prywatny lub służbowy numer telefonu.

Podmiot zgłaszający: ta część powinna zostać uzupełniona w przypadku, gdy obowiązki w zakresie zgłaszania incydentów są wypełniane przez osobę trzecią w imieniu DUP objętego skutkami incydentu.

Nazwa podmiotu zgłaszającego: pełna nazwa podmiotu, który zgłasza incydent, zgodnie ze stosownym oficjalnym krajowym rejestrem handlowym.

Krajowy numer identyfikacyjny: niepowtarzalny krajowy numer identyfikacyjny stosowany w państwie, w którym znajduje się strona trzecia, w celu jednoznacznej identyfikacji podmiotu zgłaszającego incydent. Jeżeli osobą trzecią przekazującą zgłoszenie jest DUP, krajowym numerem identyfikacyjnym powinien być niepowtarzalny krajowy numer identyfikacyjny DUP używany przez właściwy organ państwa członkowskiego pochodzenia w rejestrze krajowym.

Główna osoba do kontaktu: imię i nazwisko osoby odpowiedzialnej za zgłoszenie incydentu.

E-mail: adres poczty elektronicznej, na który w razie konieczności skierowane mogą zostać żądania dalszych wyjaśnień. Może to być prywatny lub służbowy adres e-mail.

Telefon do kontaktu: numer telefonu, za pomocą którego można w razie potrzeby kierować wszelkie prośby o dalsze wyjaśnienia. Może to być prywatny lub służbowy numer telefonu.

Dodatkowa osoba do kontaktu: imię i nazwisko innej osoby, z którą właściwy organ może się kontaktować z zapytaniem o incydent, jeśli główna osoba kontaktowa nie jest dostępna.

E-mail: adres poczty elektronicznej innej osoby kontaktowej, na który w razie konieczności skierowane mogą zostać żądania dalszych wyjaśnień. Może to być prywatny lub służbowy adres e-mail.

Telefon: numer telefonu innej osoby do kontaktu, pod który w razie konieczności można dzwonić z żądaniami dalszych wyjaśnień. Może to być prywatny lub służbowy numer telefonu.

A 2 - Wykrycie i klasyfikacja incydentu

Data i godzina wykrycia incydentu: data i godzina, kiedy incydent został po raz pierwszy zidentyfikowany.

Data i godzina klasyfikacji incydentu: data i godzina, kiedy incydent został po raz pierwszy zidentyfikowany jako poważny.

Incydent wykryty przez: proszę wskazać, czy incydent został wykryty przez użytkownika usług płatniczych, inną stronę z DUP (np. pełniącą funkcję wewnętrznego audytora) lub stronę zewnętrzną (np. usługodawcę). Jeśli nie był to nikt z wymienionych, proszę podać wyjaśnienie w odpowiednim polu.

Rodzaj incydentu: proszę wskazać zgodnie ze swoją najlepszą wiedzą i informacjami, jeśli są dostępne, czy jest to incydent operacyjny czy incydent związany z bezpieczeństwem.

> **Operacyjny:** incydent wynikający z nieodpowiednich lub zawodnych procesów, osób i systemów lub zdarzeń siły wyższej, które mają wpływ na integralność, dostępność, poufność lub autentyczność usług związanych z płatnościami.
>
> **Związany z bezpieczeństwem:** nieupoważnione: dostęp, użycie, ujawnienie, zakłócenie, zmiana lub zniszczenie aktywów DUP, które mają wpływ na integralność, dostępność, poufność lub autentyczność usług związanych z płatnościami. Może to mieć miejsce m.in. w przypadku naruszenia przez DUP bezpieczeństwa sieci lub systemów informatycznych.

Kryteria uruchamiania zgłoszenia poważnego incydentu: proszę wskazać, które z kryteriów doprowadziło do zgłoszenia poważnego incydentu. Spośród kryteriów można wybrać wiele opcji: transakcje, których to dotyczy, użytkownicy usług płatniczych, których to dotyczy, czas przestoju usługi, naruszenie bezpieczeństwa sieci lub systemów informatycznych, skutki ekonomiczne, wysoki poziom wewnętrznej eskalacji, inni DUP lub odpowiednie infrastruktury, na które może to mieć wpływ lub skutek reputacyjny.

Krótki i ogólny opis incydentu: proszę krótko wyjaśnić najważniejsze kwestie dotyczące incydentu, podając możliwe przyczyny, bezpośredni wpływ, itp.

Wpływ w innych państwach członkowskich UE, w stosownych przypadkach: proszę krótko opisać wpływ incydentu w innych państwach członkowskich UE (np. na użytkowników usług płatniczych, DUP lub infrastrukturę płatniczą). Jeżeli jest to wykonalne w obowiązujących terminach przekazywania zgłoszeń, proszę przedstawić tłumaczenie na język angielski.

Przekazywanie zgłoszeń innym organom: proszę wskazać, czy incydent został/zostanie zgłoszony innym organom w ramach odrębnych ram zgłaszania incydentów, jeżeli są one znane w momencie dokonywania zgłoszenia. Jeśli tak, proszę określić odpowiednie organy.

Przyczyny opóźnienia w przekazaniu zgłoszenia wstępnego: proszę wyjaśnić powody, dla których sklasyfikowanie incydentu wymagało więcej niż 24 godziny.

B Zgłoszenie okresowe

B 1 – Informacje ogólne

Bardziej szczegółowy opis incydentu: proszę opisać główne cechy incydentu, obejmujące co najmniej informacje na temat konkretnego problemu i związanego z nim kontekstu, opis, w jaki sposób incydent rozpoczął się i ewoluował, a także konsekwencje, zwłaszcza dla użytkowników usług płatniczych itp. Proszę również, w stosownych przypadkach, przedstawić informacje na temat komunikacji z użytkownikami usług płatniczych.

Czy był(-y) związany(-e) z poprzednim(-i) incydentem(-ami)? Proszę wskazać, czy incydent związany jest z poprzednimi incydentami, czy też nie, czy informacje te są dostępne. Jeżeli incydent był związany z poprzednimi incydentami, proszę określić z którymi.

Czy inni usługodawcy/osoby trzecie mieli wpływ na sytuację lub byli zaangażowani? Proszę wskazać, czy incydent miał wpływ na innych usługodawców/osoby trzecie, czy też nie, czy informacje te są dostępne. Jeżeli incydent miał wpływ na innych usługodawców/osoby trzecie lub był z nimi związany, proszę je wymienić i podać więcej informacji.

Czy rozpoczęto zarządzanie kryzysowe (wewnętrzne lub zewnętrzne)? Proszę wskazać czy rozpoczęto zarządzanie kryzysowe (wewnętrzne lub zewnętrzne) czy nie. Jeżeli zarządzanie kryzysowe rozpoczęło się, proszę podać więcej informacji.

Data i godzina początku incydentu: data i godzina, kiedy incydent miał swój początek, jeśli wiadomo.

Data i godzina, kiedy incydent został lub przewiduje się, że zostanie opanowany: proszę wskazać datę i godzinę, od kiedy incydent jest lub przewiduje się, że zostanie opanowany, a przedsiębiorstwo znowu funkcjonuje lub przewiduje się, że będzie funkcjonowało normalnie.

Dotknięte obszary funkcjonalne: wskazać etap lub etapy procesu płatności, na które incydent miał wpływ, takie jak uwierzytelnienie/autoryzacja, komunikacja, rozliczenie, rozrachunek bezpośredni, rozrachunek pośredni i inne.

Uwierzytelnienie/autoryzacja: procedury umożliwiające DUP weryfikację tożsamości użytkownika usług płatniczych lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika oraz użytkownika usług płatniczych (lub osobę trzecią działającą w imieniu tego użytkownika), udzielającego zgody na przekazanie środków pieniężnych lub papierów wartościowych.

Komunikacja: przepływ informacji w celu identyfikacji, uwierzytelnienia, powiadomienia i przekazania informacji pomiędzy DUP obsługującym rachunek a dostawcami usług inicjowania płatności, dostawcami usług dostępu do informacji o rachunku, płatnikami, odbiorcami i innymi DUP.

Rozliczanie: proces przekazywania, uzgadniania i w niektórych przypadkach potwierdzania zlecenia transferu przed rozrachunkiem, w tym ewentualne kompensowanie zleceń i ustalanie sald końcowych do rozrachunku.

Rozrachunek bezpośredni: zakończenie transakcji lub przetwarzania w celu wypełnienia zobowiązań uczestników poprzez transfer środków pieniężnych, kiedy czynność ta jest wykonywana przez samego DUP objętego skutkami incydentu.

Rozliczenie pośrednie: zakończenie transakcji lub przetwarzania w celu wypełnienia zobowiązań uczestników poprzez transfer środków pieniężnych, kiedy czynność ta jest wykonywana przez innego DUP w imieniu DUP objętego skutkami incydentu.

Inne: obszar funkcjonalny objęty skutkami incydentu nie jest żadnym z wyżej wymienionych. Dalsze szczegóły należy podać w pustym polu tekstowym.

Zmiany wprowadzone do poprzednich zgłoszeń: proszę wskazać zmiany wprowadzone w informacjach przekazanych w poprzednich zgłoszeniach dotyczących tego samego incydentu (np. zgłoszenie początkowe lub, w stosownych przypadkach, zgłoszenie okresowe).

B 2 – Klasyfikacja incydentów/informacje o incydencie

Transakcje objęte skutkami incydentu: DUP powinni wskazać, które progi zostały lub prawdopodobnie zostaną przekroczone w wyniku incydentu, jeśli dotyczy, i względne dane: liczbę transakcji objętych skutkami incydentu, procent transakcji objętych skutkami incydentu w stosunku do liczby transakcji płatniczych zrealizowanych w zakresie takich samych usług płatniczych, jakie zostały objęte skutkami incydentu, oraz całkowitą wartość tych transakcji. DUP powinni podać konkretne wartości dla tych zmiennych, które mogą być rzeczywistymi danymi liczbowymi lub szacunkami. Zasadniczo pod pojęciem „transakcji objętej skutkami incydentu" DUP powinni rozumieć wszystkie krajowe i transgraniczne transakcje, na które incydent ma lub prawdopodobnie będzie miał bezpośredni lub pośredni wpływ, w szczególności transakcje, które nie mogą zostać zainicjowane lub zrealizowane, transakcje, w przypadku których treść komunikatu płatniczego została zmieniona, i transakcje, które zostały zlecone w nieuczciwym zamiarze (bez względu na to, czy środki pieniężne zostały odzyskane) Ponadto DUP powinni rozumieć jako zwykły poziom transakcji płatniczych średnioroczną dzienną liczbę transakcji płatniczych krajowych i zagranicznych zrealizowanych w zakresie takich samych usług płatniczych, jak te, na które wpływ miał incydent, biorąc do wyliczenia rok poprzedni jako okres odniesienia. Jeśli DUP nie uważają tej wartości za reprezentatywną (np. w związku z sezonowością), powinni zamiast tego skorzystać z innej, bardziej reprezentatywnej miary i podać właściwemu organowi stosowny powód stosowania takiego podejścia w polu „Uwagi". W przypadkach gdy incydent ma wpływ na transakcje płatnicze w walutach innych niż euro, przy obliczaniu progów i zgłaszaniu wartości transakcji, których to dotyczy, DUP powinni przeliczać na euro kwotę transakcji w walucie innej niż euro, stosując dzienny referencyjny kurs walutowy EBC z dnia poprzedzającego złożenie sprawozdania z incydentu.

Użytkownicy usług płatniczych objęci skutkami incydentu: DUP powinien wskazać, które progi zostały lub prawdopodobnie zostaną przekroczone w wyniku incydentu, jeśli dotyczy, i względne dane: całkowitą liczbę użytkowników usług płatniczych objętych skutkami incydentu i procent użytkowników usług płatniczych objętych skutkami incydentu w stosunku do całkowitej liczby użytkowników usług płatniczych. DUP powinni podać określone wartości tych zmiennych, które mogą stanowić faktyczne dane albo szacunki. Pod pojęciem „użytkowników usług płatniczych objętych skutkami incydentu" DUP powinni rozumieć wszystkich klientów (konsumentów krajowych i zagranicznych oraz firmy krajowe i zagraniczne), którzy zawarli umowę z dostawcą usług płatniczych objętym skutkami incydentu, który udziela im dostępu do usługi płatniczej objętej skutkami incydentu, oraz którzy ponieśli lub prawdopodobnie poniosą konsekwencje nastąpienia incydentu. Aby określić liczbę użytkowników usług płatniczych, którzy mogli korzystać z usług płatniczych w okresie trwania incydentu, DUP powinni odnieść się do szacunków opartych o przeszłą działalność. W przypadku grup, każdy DUP powinien wziąć pod uwagę wyłącznie swoich własnych użytkowników usług płatniczych. W przypadku DUP oferujących usługi operacyjne innym, taki DUP powinien wziąć pod uwagę wyłącznie swoich własnych użytkowników usług płatniczych (jeśli dotyczy), a DUP otrzymujący takie usługi operacyjne powinni ocenić skutki incydentu w stosunku do swoich własnych użytkowników usług płatniczych. Ponadto DUP powinni uwzględnić jako całkowitą liczbę użytkowników usług płatniczych łączną liczbę krajowych i zagranicznych użytkowników usług płatniczych umownie związanych z nimi w okresie trwania incydentu (lub ewentualnie ostatnio dostępną liczbę) oraz mających dostęp do usług płatniczych objętych skutkami incydentu, bez względu na ich wielkość oraz na to, czy są uważani za aktywnych czy pasywnych użytkowników usług płatniczych.

Naruszenie bezpieczeństwa sieci lub systemów informatycznych: DUP powinni określić, czy jakiekolwiek działanie złośliwe naruszyło dostępność, autentyczność, integralność lub poufność sieci lub systemów informatycznych (w tym danych) związanych ze świadczeniem usług płatniczych.

Przestój w świadczeniu usług: DUP powinien wskazać, czy progi zostały lub prawdopodobnie zostaną przekroczone w wyniku incydentu i względne dane: całkowity czas przestoju w świadczeniu usług. DUP powinni podać konkretne wartości dla tej zmiennej, które mogą być rzeczywistymi danymi liczbowymi lub szacunkami. DUP powinni uwzględnić okres czasu, w którym zadania, procesy lub kanały związane ze świadczeniem usług płatniczych są lub prawdopodobnie będą niesprawne, a w związku z tym uniemożliwiają (i) zainicjowanie i/lub realizację usługi płatniczej i/lub (ii) dostęp do rachunku płatniczego. DUP powinni wyliczyć czas przestoju w świadczeniu usług od momentu wystąpienia przestoju oraz powinni uwzględnić zarówno okresy czasu, kiedy prowadzą działalność pozwalającą na realizację usług płatniczych, jak również godziny zamknięcia i okresy prowadzenia konserwacji, w stosownych przypadkach. Jeśli dostawcy usług płatniczych nie mogą określić momentu wystąpienia przestoju w świadczeniu usług, powinni oni wyjątkowo liczyć czas przestoju w świadczeniu usług od momentu wykrycia przestoju.

Wpływ ekonomiczny: DUP powinien wskazać, czy próg został lub prawdopodobnie zostanie przekroczony w wyniku incydentu i względne dane: koszty bezpośrednie i koszty pośrednie. DUP powinni podać określone wartości tych zmiennych, które mogą stanowić faktyczne dane albo szacunki. DUP powinni uwzględnić zarówno koszty, które mogą być związane z incydentem w sposób bezpośredni, jak i takie, które są związane z incydentem w sposób pośredni. DUP powinni wziąć pod uwagę między innymi przywłaszczone środki pieniężne lub aktywa, koszty wymiany sprzętu i oprogramowania, inne koszty ekspertyz sądowych i napraw, opłaty z tytułu niedopełnienia umownych zobowiązań, kary, zobowiązania zewnętrzne oraz utracone przychody. Odnośnie do kosztów pośrednich DUP powinni uwzględnić wyłącznie koszty, które są już znane lub których poniesienie jest bardzo prawdopodobne. W przypadkach gdy koszty występują w walutach innych niż euro, przy obliczaniu progu i zgłaszaniu wartości wpływu ekonomicznego DUP powinni przeliczać kwotę kosztów w walucie innej niż euro na euro, stosując dzienny referencyjny kurs walutowy EBC z dnia poprzedzającego zgłoszenie incydentu.

Koszty bezpośrednie: kwota pieniędzy (euro) poniesiona bezpośrednio w wyniku wystąpienia incydentu, w tym środki pieniężne konieczne do naprawienia skutków incydentu (np. przywłaszczone środki pieniężne lub aktywa, koszty wymiany sprzętu i oprogramowania, opłaty z tytułu niedopełnienia umownych zobowiązań).

Koszty pośrednie: kwota pieniędzy (euro) poniesiona pośrednio w wyniku wystąpienia incydentu (np. koszty odszkodowań/rekompensat na rzecz klientów, potencjalne koszty prawne)

Wysoki poziom wewnętrznej eskalacji: DUP powinni rozważyć, czy w wyniku wpływu na usługi związane z płatnościami organ zarządzający zdefiniowany w wytycznych EUNB w sprawie ICT i zarządzania ryzykiem związanym z bezpieczeństwem został lub prawdopodobnie będzie informowany, zgodnie z wytyczną 60 lit. d) wytycznych EUNB w sprawie ICT i zarządzania ryzykiem dla bezpieczeństwa, o incydencie poza okresową procedurą powiadamiania i w sposób ciągły przez cały okres trwania incydentu. Ponadto dostawcy usług płatniczych powinni rozważyć, czy w wyniku wpływu incydentu na usługi związane z płatnościami uruchomiono lub prawdopodobnie zostanie zastosowany tryb kryzysowy.

Inni DUP lub stosowna infrastruktura, potencjalnie objęci skutkami incydentu: DUP powinni oceniać wpływ incydentu na rynek finansowy rozumiany jako infrastruktury rynku finansowego lub systemy płatności, które go wspierają, oraz pozostałych DUP. W szczególności DUP powinni ocenić, czy incydent został lub prawdopodobnie zostanie powielony u innych DUP, czy miał lub może mieć wpływ na sprawne funkcjonowanie infrastruktury rynku finansowego lub czy zakłócił lub prawdopodobnie zagroził solidności systemu finansowego jako całości. DUP powinni mieć na uwadze różne wymiary, takie jak to, czy dany komponent/oprogramowanie jest zastrzeżony lub ogólnie dostępny, niezależnie od tego, czy zagrożona sieć ma charakter wewnętrzny czy zewnętrzny, czy też DUP zaprzestał lub prawdopodobnie przestanie wypełniać swoje obowiązki w zakresie infrastruktury rynku finansowego, do której należy.

Skutek reputacyjny: Dostawcy usług płatniczych powinni uwzględnić poziom widoczności, jaki zgodnie z ich wiedzą incydent osiągnął lub prawdopodobnie osiągnie na rynku. W szczególności dostawcy usług płatniczych powinni uwzględnić prawdopodobieństwo wyrządzenia szkody społeczeństwu przez incydent jako znaczący wskaźnik możliwości wywarcia wpływu na reputację. Dostawcy usług płatniczych powinni wziąć pod uwagę, czy (i) użytkownicy usług płatniczych lub inni dostawcy usług płatniczych zgłaszali skargi dotyczące negatywnych skutków incydentu, (ii) incydent miał wpływ na widoczne procesy związane z usługami płatniczymi i dlatego prawdopodobnie będzie lub już jest relacjonowany w mediach (uwzględniając nie tylko media tradycyjne, takie jak gazety, ale również blogi, sieci społecznościowe, itp.), (iii) doszło lub prawdopodobnie dojdzie do naruszenia zobowiązań umownych, i w konsekwencji – do publikacji informacji o krokach prawnych podjętych wobec dostawcy usług płatniczych, (iv) doszło do naruszenia wymogów regulacyjnych, i w konsekwencji – do zastosowania środków lub sankcji nadzorczych, które zostały lub prawdopodobnie zostaną podane do publicznej wiadomości, oraz (v) taki sam incydent miał miejsce w przeszłości

B 3 – Opis incydentu

Rodzaj incydentu: operacyjny lub związany z bezpieczeństwem. Dalsze wyjaśnienia znajdują się w odpowiednim polu w zgłoszeniu wstępnym.

Przyczyna incydentu: proszę podać przyczynę incydentu, a jeżeli nie jest jeszcze znana przyczynę, która jest najbardziej prawdopodobna. Można wybrać kilka opcji.

Prowadzone dochodzenie: proszę zaznaczyć pole, jeżeli przyczyna jest obecnie nieznana.

Działania złośliwe: działania celowe ukierunkowane na DUP. Obejmują one złośliwy kod, gromadzenie informacji, włamania, ataki typu „blokada usługi" (D/DoS), umyślne działania wewnętrzne, umyślne zewnętrzne uszkodzenia fizyczne, bezpieczeństwo informacji, działania oszukańcze i inne. Więcej informacji można znaleźć w części C2 niniejszego formularza.

Awaria procesu: powodem incydentu jest słabe opracowanie i wykonanie procesu płatniczego, kontroli procesów i/lub procesów wspierających (np. procesu zmiany/minimalizacji, testowania, konfiguracji, pojemności, monitorowania).

Awaria systemu: przyczyna incydentu jest związana z nieodpowiednim projektem, wykonaniem, komponentami, specyfikacjami, integracją lub złożonością systemów, sieci, infrastruktur i baz danych, które wspierają działalność płatniczą.

Błędy ludzkie: incydent został spowodowany nieumyślnym błędem osoby, czy to w ramach procedury płatności (np. załadowanie niewłaściwego pliku zbiorczych płatności do systemu płatności), czy też w jakiś sposób (np. energia elektryczna jest przypadkowo odcinana, a czynność płatnicza zostaje wstrzymana).

Incydenty zewnętrzne: przyczyna jest związana z wydarzeniami, które na ogół pozostają poza bezpośrednią kontrolą organizacji (np. klęski żywiołowe, awaria dostawcy usług technicznych).

Inne: powodem incydentu nie jest żaden z wyżej wymienionych powodów. Dalsze szczegóły należy podać w pustym polu tekstowym.

Czy incydent miał wpływ bezpośredni czy za pośrednictwem dostawcy usług? Proszę wskazać, czy incydent był bezpośrednio wymierzony w DUP lub czy wpływa na niego pośrednio za pośrednictwem strony trzeciej, jeżeli informacje te są dostępne. W przypadku wpływu pośredniego, proszę podać nazwę dostawcy usług (dostawców usług).

B 4 – Wpływ incydentu

Ogólny wpływ: proszę wskazać, na jakie kwestie miał wpływ incydent operacyjny lub incydent związany z bezpieczeństwem. Można wybrać kilka opcji.

Integralność: właściwość zapewnienia dokładności i kompletności aktywów (w tym danych).

Dostępność: właściwość usług związanych z płatnościami jest w pełni dostępna i możliwa do wykorzystania przez użytkowników usług płatniczych, zgodnie z dopuszczalnymi z góry określonymi poziomami.

Poufność: właściwość polegająca na braku dostępności do informacji lub nieujawnianiu ich nieupoważnionym osobom fizycznym, podmiotom lub procesom.

Autentyczność: właściwość polegająca na tym, że źródło jest tym, za które się podaje.

Kanały handlowe objęte skutkami incydentu: proszę wskazać kanał lub kanały interakcji z użytkownikami usług płatniczych, które zostały objęte skutkami incydentu. Można zaznaczyć kilka pól.

Oddziały: miejsce prowadzenia działalności (inne niż siedziba zarządu), które jest częścią DUP, nie posiada osobowości prawnej i realizuje w sposób bezpośredni niektóre lub wszystkie transakcje działalności gospodarczej DUP. Wszystkie miejsca prowadzenia działalności utworzone w tym samym państwie członkowskim przez DUP posiadającego siedzibę główną w innym państwie członkowskim powinny być traktowane jako jeden oddział.

Bankowość elektroniczna: korzystanie z komputerów w celu realizacji transakcji finansowych przez Internet.

Bankowość telefoniczna: korzystanie z telefonów w celu realizacji transakcji finansowych.

Bankowość mobilna: korzystanie z określonej aplikacji bankowej na smartfonie lub podobnym urządzeniu w celu realizacji transakcji finansowych.

Bankomaty: urządzenia elektromechaniczne, które umożliwiają użytkownikom usług płatniczych wybieranie gotówki ze swojego konta i/lub korzystanie z dostępu do innych usług.

Punkt sprzedaży: fizyczny lokal sprzedawcy detalicznego, w którym inicjowana jest transakcja.

E-handel: transakcja płatnicza jest inicjowana w wirtualnym punkcie sprzedaży (np. w przypadku płatności inicjowanych przez Internet z wykorzystaniem przelewów bankowych, kart płatniczych, transferu pieniądza elektronicznego między rachunkami pieniądza elektronicznego).

Inny: kanałem handlowym objętym skutkami incydentu nie jest żaden z wyżej wymienionych. Dalsze szczegóły należy podać w pustym polu tekstowym.

Usługi płatnicze objęte skutkami incydentu: proszę wskazać te usługi płatnicze, które nie funkcjonują w odpowiedni sposób w wyniku nastąpienia incydentu. Można zaznaczyć kilka pól.

Lokowanie gotówki na rachunku płatniczym: przekazanie gotówki do DUP w celu jej zapisania na dobro rachunku płatniczego.

Podjęcie gotówki z rachunku płatniczego: otrzymany przez DUP wniosek użytkownika usług płatniczych o dostarczenie gotówki i obciążenie rachunku płatniczego w odpowiedniej wysokości.

Operacje konieczne do obsługi rachunku płatniczego: czynności, które muszą zostać dokonane na rachunku płatniczym w celu jego aktywacji, dezaktywacji i/lub prowadzenia (np. otwieranie, blokowanie).

Nabywanie instrumentów płatniczych: usługa płatnicza polegająca na zawarciu przez DUP z odbiorcą umowy o akceptowaniu i przetwarzaniu transakcji płatniczych, co skutkuje transferem środków pieniężnych do odbiorcy.

Polecenia przelewu: usługa płatnicza polegającą na uznaniu rachunku płatniczego odbiorcy transakcją płatniczą lub serią transakcji płatniczych z rachunku płatniczego płatnika przez DUP prowadzącego rachunek płatniczy płatnika, na podstawie dyspozycji udzielonych przez płatnika.

Polecenia zapłaty: usługa płatnicza polegającą na obciążeniu rachunku płatniczego płatnika, w przypadku gdy transakcja płatnicza została zainicjowana przez odbiorcę na podstawie zgody udzielonej przez płatnika na rzecz odbiorcy, DUP odbiorcy lub DUP samego płatnika.

Płatności kartą: usługa płatnicza oparta na infrastrukturze systemu płatności kartą oraz zasadach handlowych mająca na celu wykonanie transakcji płatniczej przy użyciu karty, urządzenia telekomunikacyjnego cyfrowego lub informatycznego bądź oprogramowania, jeśli skutkuje to dokonaniem transakcji kartą debetową lub kredytową. Transakcje płatnicze oparte na karcie nie obejmują transakcji opartych o inne rodzaje usług płatniczych.

Wydawanie instrumentów płatniczych: usługa płatnicza polegająca na zawieraniu przez DUP zleceniodawcy umowy o udostępnienie mu instrumentu płatniczego do inicjowania i przetwarzania transakcji płatniczych płatnika.

Usługa przekazu pieniężnego: usługa płatnicza, która umożliwia, bez konieczności tworzenia rachunków płatniczych w imieniu płatnika lub odbiorcy, odbiór środków pieniężnych od płatnika wyłącznie w celu transferu odpowiedniej kwoty do odbiorcy lub innego DUP działającego w imieniu odbiorcy lub odbiór takich środków pieniężnych w imieniu odbiorcy i ich udostępnienie odbiorcy.

Usługi inicjowania płatności: usługa płatnicza polegającą na zainicjowaniu zlecenia płatniczego na wniosek użytkownika usług płatniczych w odniesieniu do rachunku płatniczego posiadanego u innego DUP.

Usługi dostępu do informacji o rachunku: internetowa usługa płatnicza polegająca na dostarczaniu skonsolidowanych informacji o co najmniej jednym rachunku płatniczym prowadzonym przez użytkownika usług płatniczych u innego DUP lub u więcej niż jednego DUP.

B 5 – Łagodzenie skutków incydentów

Jakie czynności/środki zostały podjęte dotychczas lub są planowane w celu opanowania incydentu? proszę podać szczegółowe informacje na temat działań, które zostały lub mają zostać podjęte w celu tymczasowego opanowania incydentu.

Czy włączony został plan ciągłości działania i/lub plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej? Proszę wskazać czy tak, i jeśli tak, proszę podać najbardziej istotne szczegóły dotyczące incydentu (tj. kiedy zostały włączone i na czym plany te polegają).

C – Zgłoszenie końcowe

C 1 – Informacje ogólne

Aktualizacja informacji zawartych w zgłoszeniu wstępnym i zgłoszeniu okresowym (streszczenie): proszę podać dalsze informacje na temat incydentu, w tym konkretne zmiany wprowadzone do informacji przekazanych w zgłoszeniu okresowym. Proszę również podać wszelkie inne istotne informacje.

Czy wprowadzono wszystkie oryginalne kontrole? Proszę wskazać, czy DUP musiał anulować lub osłabić niektóre kontrole w dowolnym momencie incydentu. Jeśli tak, proszę wskazać, czy wszystkie kontrole zostały wprowadzone, a jeśli nie, wyjaśnić w polu tekstowym, które kontrole nie zostały wprowadzone, oraz dodatkowy okres wymagany do ich przywrócenia.

C 2 – Analiza przyczyn źródłowych i działania następcze

Jaka była przyczyna źródłowa, o ile jest już znana? Proszę wskazać przyczynę źródłową incydentu lub, jeżeli nie jest jeszcze znana przyczynę, która jest najbardziej prawdopodobna. Można wybrać kilka opcji. (Należy pamiętać, że przyczynę źródłową należy odróżnić od wpływu incydentu.)

Działania złośliwe: działania zewnętrzne lub wewnętrzne celowo ukierunkowane na DUP. Są one podzielone na następujące kategorie:

Kod złośliwy: np. wirus, robaki, trojan, oprogramowanie szpiegujące.

Gromadzenie informacji: np. skanowanie, inżynieria społeczna.

Wtargnięcia: np. kompromis dotyczący uprzywilejowanego rachunku, nieuprzywilejowany kompromis dotyczący rachunków, kompromis w sprawie stosowania, bot.

Ataki typu „blokada usługi: (D/DoS): próba uniemożliwienia dostępu do usługi sieciowej poprzez przeciążenie jej ruchem pochodzącym z wielu źródeł.

Celowe działania wewnętrzne: np. sabotaż, kradzież.

Zamierzone zewnętrzne uszkodzenia fizyczne: np. sabotaż, atak fizyczny na obiekty/ośrodki danych.

Bezpieczeństwo treści informacyjnych: nieupoważniony dostęp do informacji, nieupoważniona zmiana informacji.

Działania nieuczciwe: nieuprawnione wykorzystanie zasobów, prawa autorskiego, podszywanie się, phishing.

Inne (proszę określić): powodem incydentu nie jest żaden z wyżej wymienionych powodów. Dalsze szczegóły należy podać w pustym polu tekstowym.

Awaria procesu: powodem incydentu jest słabe opracowanie i wykonanie procesu płatniczego, kontroli procesów i/lub procesów wspierających (np. procesu zmiany/minimalizacji, testowania, konfiguracji, pojemności, monitorowania). Są one podzielone na następujące kategorie:

Niedociągnięcia w zakresie monitorowania i kontroli: np. w odniesieniu do eksploatacji, terminów ważności certyfikatu, terminów ważności licencji, dat ważności poprawek, określonych maksymalnych wartości liczników, poziomów wypełnienia bazy danych, zarządzania prawami użytkowników, zasady podwójnej kontroli.

Kwestie związane z komunikacją: np. między uczestnikami rynku lub w ramach organizacji.

Nieprawidłowe operacje: np. brak wymiany certyfikatów, podręczna pamięć jest pełna.

Nieodpowiednie zarządzanie zmianami: np. niezidentyfikowane błędy konfiguracji, wprowadzenie wraz z aktualizacjami, problemy z obsługą techniczną, nieoczekiwane błędy.

Nieadekwatność wewnętrznych procedur i dokumentacji: np. brak przejrzystości w odniesieniu do funkcjonalności, procesów i przypadków nieprawidłowego działania, brak dokumentacji.

Kwestie związane z odzyskiwaniem danych: np. zarządzanie awaryjne, nieodpowiednia redundancja.

Inne (proszę określić): powodem incydentu nie jest żaden z wyżej wymienionych powodów. Dalsze szczegóły należy podać w pustym polu tekstowym.

Awaria systemu: przyczyna incydentu jest związana z nieodpowiednim projektem, wykonaniem, komponentami, specyfikacjami, integracją lub złożonością systemów, sieci, infrastruktur i baz danych, które wspierają działalność płatniczą. Są one podzielone na następujące kategorie:

Awaria sprzętu: awaria fizycznego sprzętu technologicznego, który prowadzi procesy lub przechowuje dane potrzebne DUP do wykonywania czynności związanych z płatnościami (np. awaria dysków twardych, centrów danych, innej infrastruktury).

Awaria sieci: awaria sieci telekomunikacyjnych, publicznych lub prywatnych, które umożliwiają wymianę danych i informacji (np. przez Internet) w trakcie procesu płatności.

Problemy z bazą danych: struktura danych, która przechowuje dane osobowe i dane o płatnościach konieczne do realizacji transakcji płatniczych.

Awaria oprogramowania/aplikacji: awarie programów, systemów operacyjnych itp., które wspierają świadczenie usług płatniczych przez DUP (np. nieprawidłowe działanie, nieznane funkcje).

Szkody fizyczne: np. niezamierzone szkody spowodowane niewłaściwymi warunkami, prace budowlane.

Inne (proszę określić): przyczyną incydentu nie jest żadna z powyższych przyczyn. Dalsze szczegóły należy podać w pustym polu tekstowym.

Błąd ludzki: incydent został spowodowany niezamierzonym błędem człowieka w zakresie procedury płatności (np. pobraniem niewłaściwego pliku wsadowego płatności do systemu płatniczego) lub w jakikolwiek sposób jest z nią związany (np. zasilanie zostaje przypadkowo odcięte i czynność płatnicza zostaje wstrzymana). Są one podzielone na następujące kategorie:

Niezamierzone: np. błędy, pominięcia, brak doświadczenia i wiedzy.

Bezczynność: np. z powodu braku umiejętności, wiedzy, doświadczenia i świadomości.

Niewystarczające zasoby: Np. brak zasobów ludzkich, dostępność personelu.

Inne (proszę określić): przyczyną incydentu nie jest żadna z powyższych przyczyn. Dalsze szczegóły należy podać w pustym polu tekstowym.

Incydenty zewnętrzne: przyczyna jest związana z wydarzeniami, na które organizacja zazwyczaj nie ma wpływu. Są one podzielone na następujące kategorie:

Awaria dostawcy/dostawcy usług technicznych: np. przerwy w dostawie energii elektrycznej, przerwy w dostępie do Internetu, kwestie prawne, kwestie biznesowe, zależności od usług.

Siła wyższa: np. awaria zasilania, pożary, przyczyny naturalne, takie jak trzęsienia ziemi, powodzie, silne opady, silny wiatr.

Inne (proszę określić): przyczyną incydentu nie jest żadna z powyższych przyczyn. Dalsze szczegóły należy podać w pustym polu tekstowym.

Inne: powodem incydentu nie jest żaden z wyżej wymienionych powodów. Dalsze szczegóły należy podać w pustym polu tekstowym.

Inne istotne informacje na temat przyczyny źródłowej: proszę podać wszelkie dodatkowe szczegółowe informacje na temat przyczyny źródłowej, w tym wstępne wnioski wyciągnięte z analizy przyczyn źródłowych.

Główne działania/środki naprawcze podjęte lub planowane w celu uniknięcia ponownego wystąpienia incydentu w przyszłości, jeśli są znane: proszę opisać główne działania/środki naprawcze podjęte lub planowane w celu uniknięcia ponownego wystąpienia incydentu w przyszłości.

C 3 – Informacje dodatkowe

Czy informacje o incydencie udostępniono innym DUP? Proszę podać ogólne informacje o tym, z którymi DUP skontaktowano się w sposób formalny lub nieformalny w celu powiadomienia ich o incydencie, przekazując szczegóły o DUP, którzy zostali poinformowani, informacjach, które zostały udostępnione, oraz podstawowych powodach udostępnienia tych informacji.
Czy podjęte zostały jakiekolwiek kroki prawne w stosunku do DUP? Proszę wskazać, czy na chwilę złożenia ostatecznego sprawozdania, podjęto jakieś kroki prawne w stosunku do DUP (np. został pozwany, utracił licencję) w wyniku wystąpienia incydentu.
Ocena skuteczności podjętych działań: proszę podać, w miarę możliwości, samoocenę skuteczności działań podjętych w czasie trwania incydentu, w tym wszelkie wnioski wyciągnięte z incydentu.