EBA/GL/2017/10

19/12/2017

Wytyczne

dotyczące zgłaszania poważnych incydentów zgodnie z dyrektywą (UE) 2015/2366 (PSD2)

1. Zapewnienie zgodności i obowiązki sprawozdawcze

Status Wytycznych

1. Dokument ten zawiera wytyczne wydane na podstawie artykułu 16 rozporządzenia 1093/2010[1]. W nawiązaniu do artykułu 16 ust. 3 rozporządzenia1093/2010 właściwe organy I instytucje finansowe muszą podjąć wszystkie niezbędne wysiłki, aby zapewnić zgodność z Wytycznymi.

2. Wytyczne prezentują punkt widzenia EUNB na problematykę adekwatnych praktyk nadzorczych w ramach Europejskiego Systemu Nadzoru Finansowego lub stosowania regulacji Unijnych w konkretnych obszarach. Właściwe władze określone w artykule 4 ust. 2 rozporządzenia 1093/2010, do których stosowane są Wytyczne, powinni zapewnić zgodność z nimi poprzez wdrożenie ich do własnych praktyk jako właściwych (m.in. poprzez uzupełnienie swoich ram prawnych działalności lub procesów nadzorczych), w tym gdzie Wytyczne są kierowane głównie bezpośrednio do instytucji.

Wymogi sprawozdawcze

3. W nawiązaniu do artykułu 16 ust. 3 rozporządzenia 1093/2010 właściwe władze muszą notyfikować EUNB, że są zgodne lub chcą być zgodne z Wytycznymi, a w innym przypadku podać powody niezgodności przed dniem 19/02/2018. W przypadku braku notyfikacji do wskazanej daty właściwe władze zostaną uznane przez EUNB za nieprzestrzegające Wytycznych. Powiadomienia powinny zostać wysłane przy wykorzystaniu formularza dostępnego na stronie EUNB i przesłane na adres compliance@eba.europa.eu, z odwołaniem do „EBA/GL/2017/07”. Powiadomienia powinny być złożone przez osobę posiadającą odpowiednie uprawnienia do zgłoszenia zgodności w imieniu właściwych władz. EUNB musi być informowany o jakichkolwiek zmianach w zakresie zgodności.

4. Notyfikacje zostaną opublikowane na stronie 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 upoważnienia 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, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE (PSD2).

6. W szczególności Wytyczne określają kryteria klasyfikacji poważnych incydentów operacyjnych i poważnych incydentów związanych z bezpieczeństwem przez dostawców usług płatniczych, jak również format i procedury, które powinni stosować w celu zgłoszenia takich incydentów właściwym organom w państwie członkowskim pochodzenia, a które zostały określone w art. 96 ust. 1 wyżej wymienionej dyrektywy.

7. Ponadto Wytyczne określają sposób oceny przez te właściwe organy znaczenia incydentu oraz szczegółów dotyczących sprawozdań z incydentów, które zgodnie z art. 96 ust. 2 wymienionej dyrektywy, udostępnią innym organom krajowym.

8. Dodatkowo, Wytyczne określają sposób udostępnienia EUNB i EBC stosownych szczegółów dotyczących zgłoszonych incydentów dla celów promowania wspólnego i spójnego podejścia.

Zakres stosowania

9. Wytyczne mają zastosowanie w odniesieniu do klasyfikacji i zgłaszania poważnych incydentów operacyjnych lub poważnych incydentów związanych z bezpieczeństwem zgodnie z art. 96 dyrektywy (UE) 2015/2366.

10. Wytyczne mają zastosowanie do wszystkich incydentów, które mieszczą się w definicji „poważnych incydentów operacyjnych lub poważnych incydentów związanych z bezpieczeństwem" obejmując zarówno zdarzenia zewnętrze, jak i wewnętrzne, które mogą być zarówno umyślne, jak i przypadkowe.

11. Wytyczne mają również zastosowanie w przypadku, gdy poważny incydent operacyjny lub poważny incydent związany z bezpieczeństwem pochodzi spoza Unii (np. kiedy incydent pochodzi z firmy macierzystej lub oddziału utworzonego poza Unią) i ma bezpośredni wpływ na usługi płatnicze świadczone przez dostawcę usług płatniczych zlokalizowanego w Unii (usługa związana z płatnością jest realizowana przez firmę spoza Unii objętą skutkami incydentu) lub ma pośredni wpływ (zdolność dostawcy usług płatniczych do dalszego prowadzenia działalności płatniczej jest zagrożona w inny sposób w wyniku nastąpienia incydentu).

Adresaci

12. Pierwsza grupa Wytycznych (rozdział 4) jest skierowana do dostawców usług płatniczych określonych w art. 4 ust. 11 dyrektywy (UE) 2015/2366, o których mowa w art. 4 ust. 1 rozporządzenia (UE) 1093/2010.

13. Druga i trzecia grupa Wytycznych (rozdziały 5 i 6) są skierowane do właściwych organów określonych w art. 4 ust. 2 lit. i) rozporządzenia (UE) nr 1093/2010.

Definicje

14. O ile nie określono inaczej, pojęcia stosowane i zdefiniowane w dyrektywie (UE) nr 2015/2366 mają takie samo znaczenie w Wytycznych. Ponadto do celów 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 mieć niekorzystny wpływ na integralność, dostępność, poufność, uwierzytelnienie i/lub ciągłość 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 dostępności i możliwości korzystania z nich przez użytkowników
Poufność	Właściwość polegająca na braku dostępności informacji lub nieujawnianiu ich nieupoważnionym osobom fizycznym, podmiotom lub procesom.
Uwierzytelnienie	Właściwość polegająca na tym, że źródło jest tym, za które się podaje.
Ciągłość	Właściwość polegająca na pełniej dostępności do procesów, zadań i aktywów organizacji koniecznych do świadczenia usług związanych z płatnościami i ich funkcjonowaniu na dopuszczalnych, z góry określonych poziomach.
Usługi związane z płatnościami	Każda działalność gospodarcza w rozumieniu art. 4 ust. 3 dyrektywy PSD2 oraz wszelkie konieczne wspierające zadania techniczne konieczne do właściwego świadczenia usług płatniczych.

3. Wykonanie

Data rozpoczęcia stosowania

15. Wytyczne stosuje się od dnia 13 stycznia 2018 r.

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

Wytyczna nr 1: Klasyfikacja jako poważny incydent

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

a. jedno lub więcej kryteriów na „poziomie posiadania dużego wpływu" lub

b. trzy lub więcej kryteriów na „poziomie posiadania niewielkiego wpływu"

określone w Wytycznej 1.4 oraz zgodnie z oceną określoną w 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. Przestój w świadczeniu usług

Dostawcy usług płatniczych powinni określić okres czasu, w którym usługa będzie prawdopodobnie 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.

iv. Skutek ekonomiczny

Dostawcy usług płatniczych powinni określić całościowy koszt pieniężny związany z nastąpieniem incydentu, uwzględniając zarówno wartość bezwzględną jak i jeśli dotyczy, stosunkowe znaczenie takich kosztów do wielkości dostawcy usług płatniczych (tj. kapitału Tier I dostawcy usług płatniczych).

v. Przekazanie na wyższy szczebel

Dostawcy usług płatniczych powinni określić, czy incydent został lub prawdopodobnie zostanie zgłoszony dyrektorom wykonawczym (kadrze kierowniczej).

vi. Inni dostawcy usług płatniczych lub ważna infrastruktura, potencjalnie objęta 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 kartą.

vii. 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 następującymi metodami:

i. Transakcje objęte skutkami incydentu

Zasadniczo pod pojęciem „transakcji objętej skutkami incydentu" dostawcy usług płatniczych powinni rozumieć wszystkie krajowe i zagraniczne transakcje, na które incydent ma lub prawdopodobnie będzie miał bezpośredni lub pośredni wpływ, w szczególności transakcje, które nie mogą zostać zainicjowane lub zrealizowane takie, w przypadku których treść komunikatu płatniczego została zmieniona i takie, które zostały zlecone oszukańczo (bez względu na to, czy środki pieniężne zostały odzyskane).

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. Jeśli dostawcy usług płatniczych 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 odpowiednim polu formularza (zob. załącznik 1).

ii. Użytkownicy usług płatniczych objęci skutkami incydentu

Dostawcy usług płatniczych pod pojęciem „użytkowników usług płatniczych objętych skutkami incydentu"' 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, 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.

Ponadto dostawcy usług płatniczych powinni wziąć 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 czy są uważani za aktywnych czy pasywnych użytkowników usług płatniczych.

iii. 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.

iv. 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.

v. *Przekazanie na wyższy szczebel*

Dostawcy usług płatniczych powinni określić, czy w wyniku wywarcia przez incydent wpływu na usługi związane z płatnościami dyrektor działu informatyki (lub osoba na podobnym stanowisku) został lub prawdopodobnie zostanie poinformowany o incydencie poza procedurą okresowego powiadamiania oraz jest lub będzie na bieżąco informowany w okresie trwania incydentu. Ponadto dostawcy usług płatniczych powinni określić, czy w wyniku wywarcia wpływu przez incydent na usługi związane z płatnościami, wdrożony został lub prawdopodobnie zostanie plan kryzysowy.

vi. *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 system kart płatniczych, które wspierają takich dostawców i innych dostawców usług płatniczych. W szczególności dostawcy usług płatniczych powinni ocenić, czy incydent został lub prawdopodobnie zostanie powtórzony 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: czy komponent/oprogramowanie objęty(-e) skutkami incydentu jest zastrzeżony(-e) czy ogólnie dostępny(-e), 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.

vii. *Skutek reputacyjny*

Dostawcy usług płatniczych powinni uwzględnić poziom widoczności, jaki zgodnie z ich najlepszą 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) incydent miał wpływ na widoczne procesy i dlatego prawdopodobnie będzie lub już jest relacjonowany w mediach (uwzględniając nie tylko media tradycyjne, takie jak gazety, ale również blogi, sieci społecznościowe, etc.), (ii) obowiązki regulacyjne zostały naruszone lub prawdopodobnie zostaną naruszone, (iii) sankcje zostały lub prawdopodobnie zostaną niedotrzymane lub (iv) ten sam incydent miał miejsce w przeszłości.

1.4. Dostawcy usług płatniczych powinni ocenić incydent, określając dla każdego kryterium, czy stosowne progi z tabeli 1 są lub prawdopodobnie będą osiągnięte przed rozwiązaniem incydentu.

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** > 100 000 EUR	> 25% zwykłego poziomu transakcji dostawcy usług płatniczych (pod względem liczby transakcji) **lub** > 5 milionów EUR
Użytkownicy usług płatniczych objęci skutkami incydentu	> 5 000 **oraz** > 10% użytkowników usług płatniczych dostawcy usług płatniczych	> 50 000 **lub** > 25% użytkowników usług płatniczych dostawcy usług płatniczych
Przestój w świadczeniu usług	> 2 godziny	Nie dotyczy
Wpływ ekonomiczny	Nie dotyczy	> Maks. (0,1% kapitału Tier I, * 200 000 EUR) **lub** > 5 milionów EUR
Przekazanie na wyższy szczebel	Tak	Tak, oraz plan kryzysowy (lub odpowiednik) zostanie prawdopodobnie wprowadzony
Inni dostawcy usług płatniczych lub określona infrastruktura, potencjalnie objęci skutkami incydentu	Tak	Nie dotyczy
Wpływ na reputację	Tak	Nie dotyczy

*Kapitał Tier I określony w 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 przed rozwiązaniem incydentu (np. może to mieć miejsce podczas wstępnego etapu prowadzenia dochodzenia).

1.6. Dostawcy usług płatniczych powinni dokonywać ciągłej oceny podczas okresu 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).

Wytyczna nr 2: Procedura powiadamiania

2.1. Dostawcy usług płatniczych powinni zebrać wszystkie stosowne informacje, sporządzić sprawozdanie o incydencie przy użyciu formularza określonego w załączniku 1 i przekazać go właściwemu organowi w państwie członkowskim pochodzenia. Dostawcy usług płatniczych powinni wypełnić formularz stosując się do instrukcji określonych w załączniku 1.

2.2. Dostawcy usług płatniczych powinni skorzystać z tego samego formularza w celu informowania właściwego organu przez okres trwania incydentu (tj. do wstępnych, okresowych i końcowych sprawozdań opisanych w par. od 2.7 do 2.21). Dostawcy usług płatniczych powinni wypełniać formularz stopniowo, dokładając wszelkich starań, w miarę jako dostępnych jest więcej informacji w trakcie prowadzenia przez nich wewnętrznego dochodzenia.

2.3. Dostawcy usług płatniczych powinni również przedstawić właściwym organom w państwach członkowskich ich pochodzenia, jeśli dotyczy, kopię informacji przekazanych (lub które zostaną przekazane) swoim użytkownikom zgodnie z drugim paragrafem art. 96 ust. 1 dyrektywy PSD2, tak szybko jak będą dostępne.

2.4. Dostawcy usług płatniczych powinni przekazać właściwemu organowi w państwie członkowskim pochodzenia wszelkie dodatkowe informacje, jeśli są dostępne i uważane za znaczące dla właściwego organu, dołączając dokumentację uzupełniającą do standardowego formularza jako jeden załącznik lub więcej załączników.

2.5. Dostawcy usług płatniczych powinni uwzględniać żądania właściwych organów w państwie członkowskim pochodzenia i przekazywać dodatkowe informacje lub wyjaśnienia dotyczące już złożonej dokumentacji.

2.6. Dostawcy usług płatniczych powinni przez cały czas zachowywać poufność i integralność informacji wymienianych z właściwym organem w państwie członkowskim ich pochodzenia i również odpowiednio uwierzytelniać się przed właściwym organem w państwie członkowskim pochodzenia.

Sprawozdanie wstępne

2.7. Dostawcy usług płatniczych powinni złożyć sprawozdanie wstępne właściwemu organowi w państwie członkowskim pochodzenia, jeśli wykryty zostaje po raz pierwszy poważny incydent operacyjny lub poważny incydent związany z bezpieczeństwem.

2.8. Dostawcy usług płatniczych powinni przesłać sprawozdanie wstępne właściwemu organowi w terminie 4 godzin od momentu pierwszego wykrycia poważnego incydentu operacyjnego lub poważnego incydentu związanego z bezpieczeństwem lub, jeśli wiadomo, że kanały sprawozdawczości właściwego organu nie są dostępne lub sprawne w danym momencie, tak szybko jest staną się znowu dostępne/sprawne.

2.9. Dostawcy usług płatniczych powinni również złożyć sprawozdanie wstępne właściwemu organowi w państwie członkowskim pochodzenia, jeśli incydent, który został określony jako o niewielkim wpływie, stanie się incydentem o dużym wpływie. W tym szczególnym przypadku, dostawcy usług płatniczych powinni przesłać właściwemu organowi sprawozdanie 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/sprawne.

2.10. Dostawcy usług płatniczych powinni zamieścić w swoim sprawozdaniu wstępnym informacje nagłówkowe (tj. część A formularza), przedstawiając w ten sposób podstawowe cechy incydentu oraz jego oczekiwane skutki w oparciu o informacje dostępne natychmiast po wykryciu lub zmianie klasyfikacji incydentu. Jeśli faktyczne dane nie są dostępne, dostawcy usług płatniczych powinni skorzystać z szacunków. Dostawcy usług płatniczych powinni również zamieścić w swoim sprawozdaniu wstępnym datę następnej aktualizacji, która powinna nastąpić niezwłocznie, a pod żadnym względem nie później niż w terminie 3 dni roboczych.

Sprawozdanie okresowe

2.11. Dostawcy usług płatniczych powinni składać sprawozdania okresowe za każdym razem, kiedy uważają, że konieczna jest aktualizacja określonej sytuacji oraz co najmniej do dnia następnej aktualizacji wskazanej w poprzednim sprawozdaniu (sprawozdaniu wstępnym lub poprzednim sprawozdaniu okresowym).

2.12. Dostawcy usług płatniczych powinni złożyć właściwemu organowi pierwsze sprawozdanie okresowe z bardziej szczegółowym opisem incydentu oraz jego skutków (część B formularza). Ponadto dostawcy usług płatniczych powinni sporządzać dodatkowe sprawozdania okresowe co najmniej aktualizujące informacje już przekazane w częściach A i B formularza, jeśli uzyskają wiedzę o nowych, mających znaczenie informacjach lub nastąpieniu znacznych zmian w stosunku do poprzedniego powiadomienia (np. że incydent nasilił się lub osłabł, nowe zidentyfikowane powody lub czynności podjęte w celu naprawienia problemu). W każdym przypadku dostawcy usług płatniczych powinni sporządzić sprawozdanie okresowe na żądanie właściwego organu w państwie członkowskim pochodzenia.

2.13. Tak jak w przypadku sprawozdania wstępnego, jeśli faktyczne dane nie są dostępne, dostawcy usług płatniczych powinni skorzystać z szacunków.

2.14. Ponadto dostawcy usług płatniczych powinni wskazać w każdym sprawozdaniu datę następnej aktualizacji, która powinna nastąpić niezwłocznie, ale pod żadnym względem nie później niż w terminie 3 dni roboczych. Jeśli dostawca usług płatniczych nie dotrzyma przewidywanego terminu następnej aktualizacji, powinien skontaktować się z właściwym organem w celu wyjaśnienia powodów opóźnienia, zaproponować nowy możliwy termin złożenia sprawozdania (nie dłuższy niż 3 dni robocze) oraz wysłać nowe sprawozdanie okresowe aktualizujące wyłącznie informacje dotyczące przewidywanego terminu następnej aktualizacji.

2.15. Ostatnie sprawozdanie okresowe powinno zostać wysłane przez dostawców usług płatniczych w momencie, kiedy zwykła działalność została przywrócona i firma znowu funkcjonuje normalnie, informując właściwy organ o takich okolicznościach. Dostawcy usług płatniczych powinni uważać firmę za znowu funkcjonującą normalnie, kiedy jej działalność i operacje zostają przywrócone do takiego samego poziomu usług/warunków jak określone przez dostawcę usług płatniczych lub wskazane zewnętrznie w umowie o gwarantowanym

poziomie świadczenia usług (SLA) pod względem terminów realizacji, wydajności, wymogów bezpieczeństwa, etc., a środki awaryjne nie są już stosowane.

2.16. Jeśli firma będzie funkcjonowała znowu normalnie przed upływem 4 godzin od wykrycia incydentu, dostawcy usług płatniczych powinni starać się złożyć jednocześnie sprawozdanie wstępne i ostatnie sprawozdanie okresowe (tj. wypełniając części A i B formularza) w terminie 4 godzin.

Sprawozdanie końcowe

2.17. Dostawcy usług płatniczych powinni wysłać sprawozdanie końcowe, kiedy dokonana została analiza zasadniczej przyczyny incydentu (bez względu na to, czy zastosowano już środki ograniczenia ryzyka i czy zidentyfikowana została ostateczna zasadnicza przyczyna) oraz dostępne są faktyczne dane zastępujące szacunki.

2.18. Dostawcy usług płatniczych powinni dostarczyć sprawozdanie końcowe właściwemu organowi w terminie maksymalnie 2 tygodni od momentu uznania, że firma działa znowu normalnie. Dostawcy usług płatniczych, który potrzebują wydłużenia tego terminu (np. jeśli nie są jeszcze dostępne faktyczne dane dotyczące wpływu incydentu), powinni skontaktować się z właściwym organem przed jego upływem i przedstawić odpowiednie uzasadnienie opóźnienia, jak również nowy przewidywany termin złożenia sprawozdania końcowego.

2.19. Jeśli dostawcy usług płatniczych mogą przekazać wszystkie informacje wymagane dla sprawozdania końcowego (tj. część C formularza) w terminie 4 godzin od momentu wykrycia incydentu, powinni oni dążyć do przedstawienia w sprawozdaniu końcowym informacji odnoszących się do sprawozdania wstępnego, ostatniego sprawozdania okresowego i sprawozdania końcowego.

2.20. Dostawcy usług płatniczych powinni dążyć do przedstawienia w sprawozdaniach 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 zasadniczą przyczynę, jeśli jest już znana, oraz streszczenia środków zastosowanych lub które planuje się zastosować w celu usunięcia problemu i uniemożliwienia jego pojawienia się w przyszłości.

2.21. Dostawcy usług płatniczych powinni również przesłać sprawozdanie końcowe w momencie, w którym w wyniku prowadzenia ciągłej oceny incydentu stwierdzą, że zgłoszony incydent nie spełnia już kryteriów incydentu poważnego i nie oczekuje się, że będzie je spełniał przed jego rozwiązaniem. W takim przypadku dostawcy usług płatniczych powinni przesłać sprawozdanie końcowe niezwłocznie po wykryciu takich okoliczności oraz w każdym przypadku do przewidywanego terminu złożenia następnego sprawozdania. W tej szczególnej sytuacji, zamiast wypełniać część C formularza, dostawcy usług płatniczych powinni zaznaczyć kwadrat „incydent przeklasyfikowany na inny niż poważny” i wyjaśnić powody uzasadniające obniżenie jego znaczenia.

Wytyczna nr 3: Zlecanie i konsolidacja sprawozdań

3.1. Jeśli jest to dozwolone przez właściwy organ, dostawcy usług płatniczych, którzy chcą przekazać obowiązki składania sprawozdań 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, jeśli dotyczy, istniejące wewnętrzne ustalenia w ramach grupy pomiędzy dostawcą usług płatniczych a osobą trzecią będące podstawą zlecenia składania sprawozdań jednoznacznie określają obowiązki przydzielone wszystkich stronom. W szczególności wyraźnie stanowią, że bez względu na możliwe przekazanie zobowiązań składania sprawozdań, 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. Przekazanie 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 (EMD); lub

ii. wytyczne CEBS dotyczące outsourcingu w odniesieniu do instytucji kredytowych.

c. Informacje są przekazywane właściwemu organowi w państwie członkowskim pochodzenia z wyprzedzeniem, a w każdym przypadku zgodnie z terminami i procedurami określonymi przez właściwe organy, jeśli dotyczy.

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 zlecić wyznaczonej osobie trzeciej wypełnienie zobowiązań do składania sprawozdań w sposób skonsolidowany (tj. przekazując jedno pojedyncze sprawozdanie odnoszące się do kilku dostawców usług płatniczych objętych skutkami tego samego poważnego incydentu operacyjnego lub poważnego incydentu związanego z bezpieczeństwem), powinni poinformować o tym właściwy organ w państwie członkowskim pochodzenia, załączyć informacje o umowie pod pozycją „DUP objęci skutkami incydentu” w formularzu oraz zapewnić spełnienie następujących warunków:

a. Włączyć niniejsze postanowienie do umowy stanowiącej podstawę zlecenia składania sprawozdań.

b. Uzależnić złożenie skonsolidowanego sprawozdania od wystąpienia incydentu w wyniku przerwania świadczenia usług przez osobę trzecią.

c. Ograniczyć składanie skonsolidowanych sprawozdań do dostawców usług płatniczych prowadzących działalność w takim samym państwie członkowskim.

d. Zapewnić ocenę stopnia istotności incydentu przez osobę trzecią dla każdego objętego skutkami incydentu dostawcy usług płatniczych i uwzględnić w skonsolidowanym sprawozdaniu wyłącznie tych dostawców usług płatniczych, w przypadku których incydent został sklasyfikowany jako poważny. Ponadto zapewnić, że w przypadku wątpliwości, dostawca usług płatniczych zostanie ujęty w skonsolidowanym sprawozdaniu, tak długo jak nie istnieją dowody wskazujące na to, że nie powinien być uwzględniony.

e. Jeśli są w formularzu pola, w których wspólna odpowiedź nie jest możliwa (np. części B 2, B 4 lub C 3), 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, lub (ii) korzystała z przedziałów w tych polach, w których jest taka możliwość, przedstawiając najniższą i najwyższą wartość odnotowaną lub szacowaną dla różnych dostawców usług płatniczych.

f. Dostawcy usług płatniczych powinni zapewnić, aby osoba trzecia informowała ich przez cały czas o wszystkich stosownych informacjach dotyczących incydentu oraz wszystkich kontaktach, które osoba trzecia posiada z właściwym organem, oraz ich treści, jednak wyłącznie w takim stopniu, w którym jest to możliwe bez naruszania poufności dotyczącej informacji, które odnoszą się do innych dostawców usług płatniczych.

3.3. Dostawcy usług płatniczych nie powinni zlecać swoich obowiązków do składania sprawozdań, zanim nie poinformują o tym właściwego organu w państwie członkowskim pochodzenia lub po otrzymaniu informacji, że umowa outsourcingowa nie spełnia wymogów określonych w Wytycznej 3.1. lit. b).

3.4. Dostawcy usług płatniczych, którzy chcą wycofać zlecenie wykonywania zobowiązań do składania sprawozdań, 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 poinformować właściwy organ w państwie członkowskim pochodzenia o wszelkich istotnych wydarzeniach mających wpływ na wyznaczoną osobę trzecią i jej zdolność do wypełnienia zobowiązań do składania sprawozdań.

3.5. Dostawcy usług płatniczych powinni w znaczącym stopniu wypełnić zobowiązania do składania sprawozdań 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, osobno przez wymienionego dostawcę usług płatniczych, a drugi raz przez osobę trzecią.

Wytyczna nr 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 sposobu oceny znaczenia incydentu oraz szczegółów sprawozdań z incydentów udostępnianych innym organom krajowym

Wytyczna nr 5: Ocena znaczenia incydentu

5.1. Właściwe organy w państwie członkowskim pochodzenia powinny ocenić znaczenie poważnego incydentu operacyjnego lub poważnego incydentu związanego z bezpieczeństwem dla innych organów krajowych na podstawie swoich własnych ekspertyz i korzystając z poniższych kryteriów, które są głównymi wskaźnikami znaczenia wymienionego incydentu:

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

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

Wytyczna nr 6: Informacje udostępniane

6.1. Bez względu na inne wymogi prawne dotyczące udostępniania innym organom krajowym informacji dotyczących incydentu, właściwe organy powinny udzielać informacji o poważnych incydentach operacyjnych lub poważnych incydentach związanych z bezpieczeństwem organom krajowym określonym zgodnie z Wytyczną 5.1 (tj. „innym stosownym organom krajowym") co najmniej w momencie otrzymania sprawozdania wstępnego (lub ewentualnie sprawozdania, które doprowadziło do udostępnienia informacji) oraz powiadomienia, że firma funkcjonuje znowu normalnie (tj. ostatniego sprawozdania okresowego).

6.2. Właściwe organy powinny złożyć innym stosownym organom krajowym informacje konieczne do wyraźnego nakreślenia sytuacji dotyczącej tego, co się stało i potencjalnych skutków. W tym celu powinny przekazać co najmniej informacje udzielone przez dostawcę usług płatniczych w następujących polach formularza (w sprawozdaniu początkowym lub okresowym):

- data i godzina wykrycia incydentu;
- data i godzina początku incydentu;
- data i godzina ponownego nastąpienia incydentu lub przewidywanego ponownego nastąpienia incydentu;
- krótki opis incydentu (w tym nieszczególnie chronione części szczegółowego opisu);
- krótki opis środków podjętych lub planowanych w celu przywrócenia sytuacji po incydencie;
- opis tego, jak incydent mógł wpłynąć na innych DUP i/lub infrastrukturę;
- opis (jeśli dotyczy) relacji medialnych;
- przyczyna nastąpienia incydentu.

6.3. Udostępniając informacje dotyczące incydentu innym stosownym organom krajowym, właściwe organy powinny w razie konieczności dokonać odpowiedniej anonimizacji i pominąć wszelkie informacje, które mogą być poufne lub podlegać ograniczeniom dotyczącym własności intelektualnej. Jednak właściwe organy powinny przekazać innym stosownym organom krajowym nazwę i adres zgłaszającego dostawcy usług płatniczych, jeśli wymienione organy krajowe mogą zagwarantować, że informacje takie będą traktowane jako poufne.

6.4. Właściwe organy powinny przez cały czas zachować poufność i integralność informacji przechowywanych i wymienianych z innymi stosownymi organami krajowymi oraz ponadto odpowiednio się uwierzytelniać przed innymi stosownymi organami krajowymi. W szczególności właściwe organy powinny traktować wszystkie informacje otrzymane na podstawie niniejszych wytycznych zgodnie z obowiązkami zachowania tajemnicy służbowej określonymi w dyrektywie PSD2 z zachowaniem obowiązującego prawa unijnego oraz wymogów krajowych.

6. Wytyczne skierowane do właściwych organów dotyczące kryteriów sposobu oceny istotnych szczegółów sprawozdań z incydentów udostępnianych EUNB i EBC oraz formatu i procedur ich przekazywania

Wytyczna nr 7: Informacje udostępniane

7.1. Właściwe organy powinny zawsze przekazywać EUNB i EBC wszystkie sprawozdania otrzymanie od (lub w imieniu) dostawców usług płatniczych objętych skutkami poważnego incydentu operacyjnego lub poważnego incydentu związanego z bezpieczeństwem (tj. sprawozdania wstępne, okresowe i końcowe).

Wytyczna nr 8: Komunikacja

8.1. Właściwe organy powinny przez cały czas zachować poufność i integralność informacji przechowywanych i wymienianych z EUNB i EBC oraz ponadto odpowiednio się uwierzytelniać przed 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 z zachowaniem obowiązującego prawa unijnego oraz wymogów krajowych.

8.2. Aby uniknąć opóźnień w przekazywaniu informacji EUNB/EBC dotyczących incydentu oraz aby pomóc zminimalizować ryzyko zakłóceń operacyjnych, właściwe organy powinny obsługiwać odpowiednie środki komunikacji.

Załącznik 1 - Formularze sprawozdań dla dostawców usług płatniczych

CLASSIFICATION: RESTRICTED

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date	DD/MM/YYYY	Time	HH:MM
Incident identification number, if applicable (for interim and final reports)			

A - Initial report

A 1 - GENERAL DETAILS

Type of report					
Type of report	☐ Individual ☐ Consolidated				
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected — ☐ Actual figure As a % of regular number of transactions — ☐ Actual figure Value of transactions affected in EUR — ☐ Actual figure Comments:
Payment service users affected [3]	Number of payment service users affected — ☐ Actual figure As a %-of total payment service users — ☐ Actual figure
Service downtime [4]	Total service downtime: DD:HH:MM — ☐ Actual figure
Economic impact [5]	Direct costs in EUR — ☐ Actual figure Indirect costs in EUR — ☐ Actual figure
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)

B 3 - INCIDENT DESCRIPTION

Type of Incident	☐ Operational ☐ Security
Cause of incident	☐ Under investigation ☐ External attack ☐ Internal attack Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other If Other, specify ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other — If Other, specify
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly If indirectly, please provide the service provider's name

B 4 - INCIDENT IMPACT

Building(s) affected (Address), if applicable	
Commercial channels affected	☐ Branches ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittanc ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiatio ☐ Operations required for operating a payment account ☐ Card payments ☐ Account informat ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlemer ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other If Other, specify:
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated? If so, when? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - additional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐ YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐ YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐ YES ☐ NO
If so, please provide details	

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs		
PSP Name	**PSP Unique Identification Number**	**PSP Authorisation number**

INSTRUKCJA WYPEŁNIENIA FORMULARZY

Dostawcy usług płatniczych powinni wypełnić odpowiednie części formularza, które w zależności od etapu składania sprawozdania, będą zamieszczone w części A w przypadku sprawozdania wstępnego, części B w przypadku sprawozdań okresowych i części C w przypadku sprawozdania końcowego. Wszystkie pola są obowiązkowe, chyba że wyraźnie zaznaczono inaczej.

Nagłówek

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

Sprawozdanie okresowe: jest to aktualizacja poprzedniego (wstępnego lub okresowego) sprawozdania dotyczącego tego samego incydentu.

Ostatnie sprawozdanie okresowe: informuje się w nim właściwy organ w państwie członkowskim pochodzenia, że zwykła działalność została przywrócona i firma znowu funkcjonuje normalnie, więc kolejne sprawozdania okresowe nie będą już składane.

Sprawozdanie końcowe: jest to ostatnie sprawozdanie, które DUP prześle odnośnie do incydentu, ponieważ (i) analiza zasadniczej przyczyny została już przeprowadzona i szacunki mogą zostać zastąpione faktycznymi 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 oczekuje się, że będzie je spełniał przed jego rozwiązaniem. DUP powinni wyjaśnić powody uzasadniające obniżenie jego znaczenia.

Data i godzina sprawozdania: dokładna data i godzina złożenia sprawozdania właściwemu organowi.

Numer identyfikacyjny incydentu, jeśli dotyczy (w przypadku sprawozdania okresowego i końcowego): numer referencyjny określony przez właściwy organ w momencie złożenia sprawozdania wstępnego w celu jednoznacznej identyfikacji incydentu, jeśli dotyczy (tj. jeśli taki numer referencyjny jest stosowany przez właściwy organ).

A - Sprawozdanie wstępne

A 1 - Ogólne dane

Rodzaj sprawozdania

Indywidualne: sprawozdanie odnosi się do jednego DUP.

Skonsolidowane: sprawozdanie odnosi się do kilku DUP, którzy korzystają z możliwości złożenia sprawozdania skonsolidowanego. Pola poniżej 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 sprawozdaniu poprzez wypełnienie odpowiedniej tabeli (Sprawozdanie skonsolidowane – wykaz DUP).

DUP objęty skutkami incydentu: odnosi się do DUP, który doświadcza incydentu.

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

Niepowtarzalny numer identyfikacyjny DUP, jeśli dotyczy: odpowiedni unikalny numer identyfikacyjny używany w każdym państwie członkowskim w celu identyfikacji DUP, podany przez DUP, jeśli pole „numer zezwolenia DUP" nie jest wypełnione.

Numer zezwolenia DUP: numer zezwolenia w państwie członkowskim pochodzenia.

Główny podmiot grupy: w przypadku grup podmiotów określonych w dyrektywie 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, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE, proszę wskazać nazwę głównego podmiotu.

Kraj pochodzenia: państwo członkowskie, w którym znajduje się siedziba statutowa DUP; lub jeśli DUP nie posiada zgodnie z prawem krajowym siedziby statutowej, państwo członkowskie, w którym znajduje się siedziba jego zarządu.

Kraj/kraje objęte skutkami incydentu: kraj lub kraje, w których nastąpiły skutki incydentu (np. kilka oddziałów DUP znajdujących się w różnych krajach zostało objętych skutkami incydentu). Może być, ale nie musi taki sam jak państwo członkowskie pochodzenia.

Główna osoba kontaktowa: imię i nazwisko osoby odpowiedzialnej za składanie sprawozdań o incydencie lub, jeśli sprawozdanie jest składane przez osobę trzecią w imieniu DUP objętego skutkami incydentu, imię i nazwisko osoby odpowiedzialnej za wydział zarządzenia incydentem/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 e-mail osobisty lub firmowy.

Telefon: numer telefonu, pod który w razie konieczności można dzwonić z żądaniami dalszych wyjaśnień. Może to być numer telefonu osobisty lub firmowy.

Dodatkowa osoba kontaktowa: imię i nazwisko innej osoby, z którą właściwy organ może się kontaktować z zapytaniem o incydent, jeśli główna osoba kontaktowa nie jest dostępna. Jeśli sprawozdanie jest składane przez osobę trzecią w imieniu DUP objętego skutkami incydentu, imię i nazwisko innej osoby z wydziału zarządzenia incydentem/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 e-mail osobisty lub firmowy.

Telefon: numer telefonu innej osoby kontaktowej, pod który w razie konieczności można dzwonić z żądaniami dalszych wyjaśnień. Może to być numer telefonu osobisty lub firmowy.

Podmiot zgłaszający: ta część powinna zostać uzupełniona w przypadku, gdy obowiązki składania sprawozdań 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.

Niepowtarzalny numer identyfikacyjny, jeśli dotyczy: odpowiedni niepowtarzalny numer identyfikacyjny używany w kraju, w którym zlokalizowana jest osoba trzecia, w celu identyfikacji podmiotu zgłaszającego incydent, a który zgłaszający podmiot podaje, jeśli pole „Numer zezwolenia" nie jest wypełnione.

Numer zezwolenia, jeśli dotyczy: numer zezwolenia osoby trzeciej w kraju, w którym jest ona zlokalizowana, jeśli dotyczy.

Główna osoba kontaktowa: imię i nazwisko osoby odpowiedzialnej za składanie sprawozdań o incydencie

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

Telefon: numer telefonu, pod który w razie konieczności można dzwonić z żądaniami dalszych wyjaśnień. Może to być numer telefonu osobisty lub firmowy.

Dodatkowa osoba kontaktowa: imię i nazwisko innej osoby z podmiotu, który zgłasza incydent, z którą właściwy organ może się kontaktować, 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 e-mail osobisty lub firmowy.

Telefon: numer telefonu innej osoby kontaktowej, pod który w razie konieczności można dzwonić z żądaniami dalszych wyjaśnień. Może to być numer telefonu osobisty lub firmowy.

A 2 - Wykrycie incydentu i wstępna klasyfikacja

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

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. zewnętrznego dostawcę usług). Jeśli nie był to nikt z wymienionych, proszę podać wyjaśnienie w odpowiednim polu.

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

Jaki jest przewidywany termin następnej aktualizacji?: proszę wskazać przewidywaną datę i godzinę złożenia następnej aktualizacji (sprawozdania okresowego lub końcowego).

Sprawozdanie okresowe

B 1 - Ogólne dane

Bardziej szczegółowy opis incydentu: proszę opisać główne cechy incydentu, uwzględniając co najmniej punkty podane w kwestionariuszu (z jakimi konkretnymi problemami zmaga się DUP, jak się zaczęły i jak przebiegały, możliwe powiązanie z poprzednim incydentem, skutki, zwłaszcza dla użytkowników usług płatniczych, etc.).

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

Status incydentu:

Diagnoza: zidentyfikowane zostały już cechy incydentu.

Naprawa: zaatakowane elementy zostały już przekonfigurowane.

Odtworzenie: uszkodzone elementy są przywracane do ich ostatniego stanu odzyskiwalnego.

Przywrócenie: usługa związana z płatnościami jest znowu świadczona.

Data i godzina, kiedy incydent został lub przewiduje się, że zostanie usunięty: proszę wskazać datę i godzinę, od kiedy incydent jest lub przewiduje się, że będzie pod kontrolą, a firma znowu funkcjonuje lub przewiduje się, że będzie funkcjonowała normalnie.

B 2 - Klasyfikacja incydentu/Informacje o incydencie

Ogólny wpływ: proszę wskazać, na które aspekty incydent miał wpływ. Można zaznaczyć kilka kwadratów.

Integralność: właściwość polegająca na ochronie dokładności i kompletności aktywów (w tym danych).

Dostępność: właściwość polegająca na dostępności i możliwości korzystania z usług związanych z płatnościami przez użytkowników usług płatniczych.

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

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

Ciągłość: właściwość polegająca na pełniej dostępności do procesów, zadań i aktywów organizacji koniecznych do świadczenia usług związanych z płatnościami i ich funkcjonowaniu na dopuszczalnych, z góry określonych poziomach.

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 określone wartości tych zmiennych, które mogą stanowić faktyczne dane albo szacunki. Podmioty dokonujące zgłoszenia w imieniu kilku DUP (tj. składające sprawozdanie skonsolidowane) mogą podać zamiast tego przedziały wartości, przedstawiając najniższą i najwyższą wartość odnotowaną lub szacowaną w grupie DUP objętych sprawozdaniem, oddzieloną łącznikiem. Zasadniczo pod pojęciem „transakcji objętej skutkami incydentu" DUP powinni rozumieć wszystkie krajowe i zagraniczne 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".

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. Podmioty dokonujące zgłoszenia w imieniu kilku DUP (tj. składające sprawozdanie skonsolidowane) mogą podać zamiast tego przedziały wartości, przedstawiając najniższą i najwyższą wartość odnotowaną lub szacowaną w grupie DUP objętych sprawozdaniem, oddzieloną łącznikiem. 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.

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 określone wartości tych zmiennych, które mogą stanowić faktyczne dane albo szacunki. Podmioty dokonujące zgłoszenia w imieniu kilku DUP (tj. składające sprawozdanie skonsolidowane) mogą podać zamiast tego przedział wartości, przedstawiając najniższą i najwyższą wartość odnotowaną lub szacowaną w grupie DUP objętych sprawozdaniem, oddzieloną łącznikiem. 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, 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.

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. Podmioty dokonujące zgłoszenia w imieniu kilku DUP (tj. składające sprawozdanie skonsolidowane) mogą podać zamiast tego przedział wartości, przedstawiając najniższą i najwyższą wartość odnotowaną lub szacowaną w grupie DUP objętych sprawozdaniem, oddzieloną łącznikiem. 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.

> **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, przychody utracone w wyniku straconych możliwości handlowych, potencjalne koszty prawne).

Przekazanie na wyższy szczebel: DUP powinni określić, czy w wyniku wpływu incydentu na usługi związane z płatnościami dyrektor działu informatyki (lub osoba na podobnym stanowisku) został lub prawdopodobnie zostanie poinformowany o incydencie poza procedurą okresowego powiadamiania oraz jest lub będzie na bieżąco informowany w okresie trwania incydentu. W przypadku zlecenia składania sprawozdań, przekazanie na wyższy szczebel powinno odbyć się u osoby trzeciej. Ponadto DUP powinni określić, czy w wyniku wywarcia wpływu przez incydent na usługi związane z płatnościami, wdrożony został lub prawdopodobnie zostanie plan kryzysowy.

Inni DUP lub stosowna infrastruktura, potencjalnie objęci skutkami incydentu: dostawcy usług płatniczych powinni ocenić wpływ incydentu na rynek finansowy rozumiany jako infrastruktura rynku finansowego i/lub systemy płatności kartą, które obsługują rynek i pozostałych DUP. W szczególności DUP powinni ocenić, czy incydent został lub prawdopodobnie zostanie powtórzony u innych DUP, czy ma lub prawdopodobnie będzie miał wpływ na płynne funkcjonowanie infrastruktury rynku finansowego oraz czy zagraża lub prawdopodobnie zagrozi właściwemu

działaniu całego systemu finansowego. DUP powinni mieć na uwadze różne aspekty, takie jak czy komponent/oprogramowanie objęty(-e) skutkami incydentu jest zastrzeżony(-e) czy ogólnie dostępny(-e), czy zagrożona sieć jest wewnętrzna czy zewnętrzna i czy DUP przestał lub prawdopodobnie przestanie wypełniać swoje zobowiązania w infrastrukturze rynku finansowego, którego jest członkiem.

Wpływ na reputację: DUP powinni uwzględnić poziom widoczności, jaki zgodnie z ich wiedzą, incydent osiągnął lub prawdopodobnie osiągnie na rynku. W szczególności DUP powinni uwzględnić prawdopodobieństwo wyrządzenia szkody społeczeństwu przez incydent jako znaczący wskaźnik możliwości wywarcia wpływu na reputację. DUP powinni wziąć pod uwagę, czy (i) incydent miał wpływ na widoczne procesy i dlatego prawdopodobnie będzie lub już był relacjonowany w mediach (uwzględniając nie tylko media tradycyjne, takie jak gazety, ale również blogi, sieci społecznościowe, etc.), (ii) obowiązki regulacyjne zostały naruszone lub prawdopodobnie zostaną naruszone, (iii) sankcje zostały lub prawdopodobnie zostaną niedotrzymane lub (iv) ten sam incydent miał miejsce w przeszłości.

B 3 - Opis incydentu

Rodzaj incydentu: proszę wskazać zgodnie ze swoją najlepszą wiedzą, czy jest to incydent operacyjny czy dotyczący bezpieczeństwa.

Operacyjny: incydent spowodowany niedoskonałością lub błędem procesów, ludzi i systemów lub zdarzeń siły wyższej, które mają wpływ na integralność, dostępność, poufność, uwierzytelnienie i/lub ciągłość usług związanych z płatnościami.

Dotyczący bezpieczeństwa: nieupoważniany dostęp, nieupoważnione użycie, ujawnienie, zakłócenie, zniszczenie lub nieupoważniona zmiana aktywów DUP, które mają wpływ na integralność, dostępność, poufność, uwierzytelnienie i/lub ciągłość usług związanych z płatnościami. Może się to zdarzyć, kiedy między innymi DUP jest poddawany cyberatakom, posiada nieodpowiednio opracowaną lub wdrożoną politykę bezpieczeństwa lub nieodpowiednio zapewnioną ochronę bezpieczeństwa fizycznego.

Przyczyna nastąpienia incydentu: proszę wskazać przyczynę nastąpienia incydentu lub, jeśli nie jest jeszcze znana, przyczynę, która jest najbardziej prawdopodobna. Można zaznaczyć kilka kwadratów.

Prowadzone dochodzenie: przyczyna nie została jeszcze określona.

Atak zewnętrzny: źródło przyczyny pochodzi z zewnątrz oraz jest celowo wymierzone w DUP (np. ataki przy użyciu złośliwego oprogramowania).

Atak wewnętrzny: źródło przyczyny pochodzi z wewnątrz oraz jest celowo wymierzone w DUP (np. oszustwo wewnętrzne).

Rodzaj ataku:

Rozproszona/Odmowa usługi (D/DoS): próba uniemożliwienia dostępu do usługi sieciowej poprzez przeciążenie jej ruchem pochodzącym z wielu źródeł.

Infekcja systemów wewnętrznych: szkodliwe działanie polegające na zaatakowaniu systemów komputerowych z zamiarem dokonania kradzieży miejsca na dysku twardym lub czasu CPU, uzyskania dostępu do prywatnych informacji, uszkodzenia danych, przesłania spamu, etc.

Ukierunkowane wtargnięcie: nieupoważnione działanie polegające na szpiegowaniu, przeszukiwaniu czy kradzieży informacji w cyberprzestrzeni.

Inne: inny rodzaj ataku, którego DUP może paść ofiarą w sposób bezpośredni lub za pośrednictwem dostawcy usług. W szczególności kwadrat ten należy zaznaczyć, jeśli dokonano ataku wymierzonego w proces autoryzacji i uwierzytelnienia. Szczegóły należy dodać w pustym polu tekstowym.

Zdarzenia zewnętrzne: powód jest związany ze zdarzeniami będącymi w zasadzie poza kontrolą organizacji (np. klęski żywiołowe, sprawy prawne, sprawy handlowe i zależność od usług).

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 przypadkowe odcięte i czynność płatnicza zostaje wstrzymana).

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: powód incydentu jest związany z niewłaściwym opracowaniem, wykonaniem, niewłaściwymi elementami, specyfikacjami, niewłaściwą integracją lub złożonością systemów, które obsługują działalność płatniczą.

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?: incydent może być wymierzony w DUP bezpośrednio lub może mieć na niego wpływ na pośrednictwem osoby trzeciej. W przypadku wpływu pośredniego, proszę podać nazwę dostawcy usług (dostawców usług).

B 4 - Wpływ incydentu

Budynek (budynki) objęty (objęte) skutkami incydentu (Adres), jeśli dotyczy: jeśli skutkami incydentu został objęty budynek fizyczny, proszę podać jego adres.

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

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 gospodarczej ustanowione przez DUP w tym samym państwie członkowskim posiadające siedzibę zarządu 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.

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 odpowiednio sposób w wyniku nastąpienia incydentu. Można zaznaczyć kilka kwadratów.

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

Podjęcie gotówki z konta płatniczego: żądanie otrzymane przez DUP od użytkownika usług płatniczych w celu przekazania gotówki i obciążenia daną kwotą jego rachunku płatniczego.

Operacje konieczne do obsługi rachunku płatniczego: czynności, które muszą zostać dokonane na rachunki 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, dostawcy usług płatniczych odbiorcy lub dostawcy usług płatniczych 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 zawarciu przez DUP umowy z płatnikiem na przekazanie instrumentu płatniczego w celu 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 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: usługi płatnicze online polegające na udzielaniu skonsolidowanych informacji dotyczących jednego rachunku płatniczego bądź wielu rachunków płatniczych posiadanych przez użytkownika usług płatniczych u innego DUP bądź u więcej niż jednego DUP.

Inne: usługa płatnicza objęta skutkami incydentu nie jest żadną z wyżej wymienionych. Dalsze szczegóły należy podać w pustym polu tekstowym.

Obszary funkcjonalne objęte skutkami incydentu: proszę wskazać etap lub etapy procesu płatniczego, które zostały objęte skutkami incydentu. Można zaznaczyć kilka kwadratów.

Uwierzytelnienie/zezwolenie: 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.

Rozrachunek pośredni: 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.

Systemy i elementy objęte skutkami incydentu: proszę wskazać, która część lub które części infrastruktury technologicznej DUP zostały objęte skutkami incydentu. Można zaznaczyć kilka kwadratów.

Aplikacja/oprogramowanie: programy, systemy operacyjne, etc., które wspierają świadczenie usług płatniczych przez DUP.

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

Sprzęt: fizyczny sprzęt technologiczny, który realizuje procesy i/lub przechowuje dane konieczne do prowadzenia przez DUP działalności związanej z płatnościami.

Sieć/infrastruktura: publiczne lub prywatne sieci telekomunikacyjne umożliwiające wymianę danych i informacji podczas procesu płatności (np. internet).

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

Personel objęty skutkami incydentu: proszę wskazać, czy incydent miał wpływ na personel DUP i, jeśli tak, proszę podać szczegóły w pustym polu tekstowym.

B 5 - Minimalizacja skutków incydentu

Jakie czynności/środki zostały podjęte dotychczas lub są planowane w celu przywrócenia sytuacji po nastąpieniu incydentu?: proszę podać szczegóły dotyczące czynności, który zostały podjęte lub są planowane w celu tymczasowego poradzenia sobie z incydentem.

Czy włączony zostały plan zapewniający ciągłość 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 zdarzenia (tj. kiedy zostały włączone i na czym plany te polegają).

Czy DUP cofnął lub osłabił pewne kontrole w związku z incydentem?: proszę wskazać, czy DUP musiał pominąć stosowanie pewnych kontroli (np. przestał korzystać z zasady czworga oczu), aby poradzić sobie z incydentem i, jeśli tak, proszę podać szczegóły podstawowych powodów uzasadniających osłabienie lub cofnięcie kontroli.

C - Sprawozdanie końcowe

C 1 - Ogólne dane

Aktualizacja informacji zawartych w sprawozdaniu okresowym (podsumowanie): proszę podać dalsze informacje dotyczące czynności podjętych w celu przywrócenia sytuacji po nastąpieniu incydentu oraz uniemożliwienia jego ponownego nastąpienia, analizy zasadniczych przyczyn, wyciągnięcia wniosków, etc.

Data i godzina zakończenia incydentu: proszę wskazać datę i godzinę, kiedy incydent został uznany za zakończony.

Czy poprzednie kontrole są znowu stosowane? jeśli DUP cofnął lub osłabił pewne kontrole w związku z incydentem, proszę wskazać czy kontrole takie zostały przywrócone i proszę podać dodatkowe informacje w pustym polu tekstowym.

C 2 - Analiza i uzupełnienie zasadniczej przyczyny

Jaka była zasadnicza przyczyna, jeśli jest już znana?: proszę wyjaśnić, jaka jest zasadnicza przyczyna incydentu lub, jeśli nie jest jeszcze znana, jakie są wstępne wnioski wyciągnięte z analizy zasadniczej przyczyny. DUP mogą załączyć plik ze szczegółowymi informacjami, jeśli uważają to za konieczne.

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

C 3 – Dodatkowe informacje

Czy informacja o incydencie została przekazana innym DUP dla celów informacyjnych?: 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 nastąpienia incydentu.