EBA/GL/2017/10

18/12/2017

Obecné pokyny

k oznamování významných incidentů podle směrnice (EU) 2015/2366 o platebních službách na vnitřním trhu (PSD2)

1. Dodržování předpisů a oznamovací povinnost

Status těchto obecných pokynů

1. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010[1]. V souladu s čl. 16 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 příslušné orgány a finanční instituce vynaloží veškeré úsilí, aby se těmito obecnými pokyny řídily.

2. Obecné pokyny formulují názor orgánu EBA na náležité postupy dohledu v rámci Evropského systému dohledu nad finančním trhem nebo na to, jak by unijní právní předpisy měly být uplatňovány v konkrétní oblasti. Příslušné orgány ve smyslu čl. 4 odst. 2 nařízení (EU) č. 1093/2010, na které se tyto obecné pokyny vztahují, by s nimi měly být v souladu a začlenit je do svých postupů (např. pozměněním právního rámce nebo dohledových postupů), včetně případů, kdy jsou obecné pokyny zaměřeny v prvé řadě na instituce.

Oznamovací povinnost

3. V souladu s čl. 16 odst. 3 nařízení (EU) č. 1093/2010 musí příslušné orgány do 19.02.2018 orgánu EBA oznámit, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě uvést do tohoto data důvody, proč se jimi neřídí či nehodlají řídit. Neposkytnou-li příslušné orgány oznámení v této lhůtě, bude mít orgán EBA za to, že se těmito obecnými pokyny neřídí nebo nehodlají řídit. Oznámení by měla být zasílána na formuláři, který je k dispozici na internetových stránkách orgánu EBA, na adresu compliance@eba.europa.eu s označením „EBA/GL/2017/10“. Oznámení by měly předkládat osoby s příslušným oprávněním oznamovat, zda se jejich příslušné orgány těmito obecnými pokyny řídí nebo hodlají řídit. Jakoukoli změnu stavu dodržování pokynů je rovněž nutno oznámit orgánu EBA.

4. Oznámení budou zveřejněna na internetových stránkách orgánu EBA v souladu s čl. 16 odst. 3.

[1] Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12).

2. Předmět, působnost a definice

Předmět

5. Tyto obecné pokyny vycházejí ze zmocnění Evropského orgánu pro bankovnictví podle čl. 96 odst. 3 směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (PSD2).

6. Tyto obecné pokyny zejména blíže vymezují kritéria pro klasifikaci významných operačních a bezpečnostních incidentů poskytovateli platebních služeb i formát a postupy, které by měli dodržovat při oznamování těchto incidentů příslušnému orgánu v domovském členském státě podle čl. 96 odst. 1 výše uvedené směrnice.

7. Kromě toho se tyto obecné pokyny zabývají tím, jak by tyto příslušné orgány měly posuzovat závažnost incidentu a podrobné informace uvedené ve zprávě o incidentu, které podle čl. 96 odst. 2 uvedené směrnice poskytují dalším vnitrostátním orgánům.

8. Dále se tyto obecné pokyny rovněž zabývají poskytováním příslušných podrobných informací o oznámených incidentech Evropskému orgánu pro bankovnictví a Evropské centrální bance s cílem podpořit společný a jednotný přístup.

Působnost

9. Tyto obecné pokyny se použijí v souvislosti s klasifikací a oznamováním významných operačních nebo bezpečnostních incidentů podle článku 96 směrnice (EU) 2015/2366.

10. Tyto obecné pokyny se vztahují na všechny incidenty obsažené v definici „významného operačního nebo bezpečnostního incidentu“, která zahrnuje externí i interní události, přičemž se může jednat o události způsobené úmyslně i o náhodné události.

11. Tyto obecné pokyny se rovněž použijí v případě, kdy významný operační nebo bezpečnostní incident vznikne mimo Unii (např. nastane-li incident v mateřské společnosti nebo v dceřiné společnosti usazené mimo Unii) a přímo (dotčená společnost nacházející se mimo Unii provádí službu související s platbami) nebo nepřímo (v důsledku incidentu je nějakým způsobem ohrožena způsobilost poskytovatele platebních služeb provádět jeho činnost provádění plateb) ovlivní platební služby poskytované poskytovatelem platebních služeb nacházejícím se v Unii.

Adresáti

12. První soubor obecných pokynů (oddíl 4) je určen poskytovatelům platebních služeb podle vymezení v čl. 4 odst. 11 směrnice (EU) 2015/2366 a uvedeným v čl. 4 odst. 1 nařízení (EU) č. 1093/2010.

13. Druhý a třetí soubor obecných pokynů (oddíly 5 a 6) je určen příslušným orgánům podle vymezení v čl. 4 odst. 2 bodě i) nařízení (EU) č. 1093/2010.

Definice

14. Není-li stanoveno jinak, mají pojmy používané a definované ve směrnici (EU) 2015/2366 stejný význam jako v těchto obecných pokynech. Kromě toho pro účely těchto obecných pokynů platí tyto definice:

Operační nebo bezpečnostní incident	Jednorázová událost nebo řada souvisejících událostí neplánovaných poskytovatelem platebních služeb, která má nebo pravděpodobně bude mít nepříznivý dopad na integritu, dostupnost, důvěrnost, autenticitu a/nebo kontinuitu služeb souvisejících s platbami.
Integrita	Zajištění správnosti a úplnosti aktiv (včetně údajů).
Dostupnost	Skutečnost, že služby související s platbami jsou přístupné uživatelům platebních služeb a uživatelé platebních služeb je mohou používat.
Důvěrnost	Skutečnost, že informace se nezpřístupňují ani nesdělují neoprávněným osobám, subjektům nebo pro nedovolené účely.
Autenticita	Vlastnost zajišťující, že zdroj je tím, čím tvrdí, že je.
Kontinuita	Skutečnost, že procesy, úlohy a aktiva organizace potřebné za účelem poskytování služeb souvisejících s platbami jsou plně přístupné a probíhají na přijatelných, předem stanovených úrovních.
Služby související s platbami	Jakákoliv podnikatelská činnost ve smyslu čl. 4 odst. 3 směrnice o platebních službách (PSD2) a všechny technické podpůrné úlohy nezbytné pro správné poskytování platebních služeb.

3. Provádění

Datum použití

15. Tyto obecné pokyny se použijí od 13. ledna 2018.

4. Obecné pokyny určené poskytovatelům platebních služeb a týkající se oznamování významných operačních nebo bezpečnostních incidentů příslušnému orgánu v domovském členském státě

Obecný pokyn 1: Klasifikace významného incidentu

1.1. Poskytovatelé platebních služeb by měli jako významné klasifikovat operační nebo bezpečnostní incidenty, které splňují

a. alespoň jedno z kritérií na „vyšší úrovni dopadu“ nebo

b. alespoň tři z kritérií na „nižší úrovni dopadu“

podle vymezení v obecném pokynu 1.4 a na základě posouzení stanoveného v těchto pokynech.

1.2. Poskytovatelé platebních služeb by měli posoudit operační nebo bezpečnostní incident na základě následujících kritérií a souvisejících ukazatelů:

i. Dotčené transakce

Poskytovatelé platebních služeb by měli určit celkovou hodnotu dotčených transakcí i počet ohrožených plateb vyjádřený jako procentuální podíl běžné úrovně platebních transakcí prováděných dotčenými platebními službami.

ii. Dotčení uživatelé platebních služeb

Poskytovatelé platebních služeb by měli určit počet dotčených uživatelů platebních služeb, a to v absolutním vyjádření i jako procentuální podíl z celkového počtu uživatelů platebních služeb.

iii. Délka výpadku služby

Poskytovatelé platebních služeb by měli určit dobu, po kterou služba bude uživateli platební služby pravděpodobně nedostupná nebo kdy platební příkaz ve smyslu čl. 4 odst. 13 směrnice o platebních službách nemůže poskytovatel platebních služeb splnit.

iv. Ekonomický dopad

Poskytovatelé platebních služeb by měli uceleně určit peněžní náklady související s incidentem a zohlednit jejich absolutní výši a případně relativní význam těchto nákladů v poměru k velikosti poskytovatele platebních služeb (tj. k výši kapitálu tier 1 poskytovatele platebních služeb).

v. Vysoká úroveň interní eskalace

Poskytovatelé platebních služeb by měli určit, zda tento incident byl nebo pravděpodobně bude nahlášen jejich řídicím pracovníkům.

vi. Ostatní potenciálně dotčení poskytovatelé platebních služeb nebo příslušné infrastruktury

Poskytovatelé platebních služeb by měli určit systémové důsledky, které incident pravděpodobně bude mít, tj. jeho potenciální přelévání mimo původně dotčeného poskytovatele platebních služeb mezi další poskytovatele platebních služeb, infrastruktury finančního trhu a/nebo systémy pro platby prováděné kartou.

vii. Dopad na dobrou pověst

Poskytovatelé platebních služeb by měli určit, jak incident může ohrozit důvěru uživatelů v poskytovatele platebních služeb a obecněji v související službu nebo trh jako celek.

1.3. Poskytovatelé platebních služeb by měli vypočítávat hodnotu ukazatelů pomocí následující metodiky:

i. Dotčené transakce

Poskytovatelé platebních služeb by obecně měli jako „dotčené transakce“ chápat veškeré vnitrostátní a přeshraniční transakce, které incidentem byly nebo pravděpodobně budou přímo nebo nepřímo dotčeny, a zejména pak transakce, které nebylo možné iniciovat nebo zpracovat, transakce, u kterých došlo k pozměnění obsahu platební zprávy, a transakce, k nimž byl příkaz zadán podvodně (bez ohledu na to, zda finanční prostředky byly či nebyly získány zpět).

Dále by poskytovatelé platebních služeb měli za běžnou úroveň platebních transakcí považovat denní roční průměr vnitrostátních a přeshraničních platebních transakcí provedených prostřednictvím stejných platebních služeb, které byly incidentem dotčeny, s použitím předchozího roku jako referenčního období při výpočtu. Jestliže poskytovatelé platebních služeb tento údaj nepovažují za vypovídající (např. kvůli sezónnosti), měli by místo toho použít jiné, více vypovídající měřítko a sdělit příslušnému orgánu příslušné odůvodnění tohoto přístupu v odpovídajícím poli formuláře (viz příloha 1).

ii. Dotčení uživatelé platebních služeb

Poskytovatelé platebních služeb by měli jako „dotčené uživatele platebních služeb“ chápat všechny klienty (vnitrostátní nebo zahraniční, spotřebitele nebo podniky), kteří mají s dotčeným poskytovatelem platebních služeb smlouvu, na jejímž základě mají přístup k dotčené platební službě, a kteří pociťují nebo pravděpodobně pocítí důsledky incidentu.

Při určování počtu uživatelů platebních služeb, kteří by bývali mohli platební službu využívat během trvání incidentu, by poskytovatelé platebních služeb měli použít odhady vycházející z dřívější aktivity.

V případě skupin by měl každý poskytovatel platebních služeb vzít v úvahu pouze svoje vlastní uživatele platebních služeb. V případě poskytovatele platebních služeb nabízejícího operační služby jiným by měl dotyčný poskytovatel platebních služeb vzít v úvahu pouze svoje případné vlastní uživatele platebních služeb, přičemž poskytovatelé platebních služeb, kteří jsou příjemci těchto operačních služeb, by měli posoudit incident ve vztahu ke svým vlastním uživatelům platebních služeb.

Dále by poskytovatelé platebních služeb měli jako celkový počet uživatelů platebních služeb použít souhrnný počet vnitrostátních a přeshraničních uživatelů platebních služeb, kteří jsou k nim smluvně vázáni v okamžiku incidentu (popřípadě nejaktuálnější dostupný údaj) a mají přístup k dotčené platební službě bez ohledu na jejich velikost nebo na to, zda jsou považováni za aktivní nebo pasivní uživatele platebních služeb.

iii. Délka výpadku služby

Poskytovatelé platebních služeb by měli zohlednit dobu, po kterou trvá nebo pravděpodobně bude trvat výpadek jakékoliv úlohy, procesu nebo kanálu vztahujícího se k poskytování platebních služeb, který tudíž znemožňuje i) iniciování a/nebo provedení platební služby a/nebo ii) přístup k platebnímu účtu. Poskytovatelé platebních služeb by měli měřit délku výpadku služby od okamžiku, kdy výpadek začne, a měli by zohlednit časové úseky, kdy mají otevřeno pro obchody potřebné pro provedení platebních služeb, a v případě potřeby i dobu, kdy mají zavřeno a kdy provádí údržbu. Nemohou-li poskytovatelé platebních služeb určit, kdy výpadek služby začal, měli by ve výjimečných případech měřit délku výpadku služby od okamžiku, kdy byl výpadek zjištěn.

iv. Ekonomický dopad

Poskytovatelé platebních služeb by měli zohlednit náklady přímo související s incidentem i náklady, které se k incidentu vztahují nepřímo. Poskytovatelé platebních služeb by měli mimo jiné vzít v úvahu ztracené finanční prostředky nebo aktiva, reprodukční náklady hardwaru nebo softwaru, další soudní náklady nebo náklady na nápravu škod, poplatky v důsledku nedodržení smluvních povinností, sankce, externí závazky a ušlé výnosy. Pokud jde o nepřímé náklady, poskytovatelé platebních služeb by měli zohlednit pouze ty, které jsou již známy nebo které velmi pravděpodobně vzniknou.

v. *Vysoká úroveň interní eskalace*

Poskytovatelé platebních služeb by měli zvážit, zda v důsledku dopadu na služby související s platbami byl nebo pravděpodobně bude o incidentu informován ředitel informačních technologií (nebo osoba zastávající podobnou funkci), a to mimo pravidelný postup podávání zpráv a průběžně po dobu trvání incidentu. Dále by poskytovatelé platebních služeb měli zohlednit, zda v důsledku dopadu incidentu na služby související s platbami byl nebo pravděpodobně bude zahájen krizový režim.

vi. *Ostatní potenciálně dotčení poskytovatelé platebních služeb nebo příslušné infrastruktury*

Poskytovatelé platebních služeb by měli posoudit dopad incidentu na finanční trh, který je chápán jako infrastruktury finančního trhu a/nebo systémy pro platby prováděnou kartou podporující tyto a další poskytovatele platebních služeb. Poskytovatelé platebních služeb by zejména měli posoudit, zda se incident projevil nebo pravděpodobně projeví u jiných poskytovatelů platebních služeb, zda ovlivnil nebo pravděpodobně ovlivní hladké fungování infrastruktur finančního trhu a zda ohrozil nebo pravděpodobně ohrozí řádný provoz finančního systému jako celku. Poskytovatelé platebních služeb by měli zohlednit různé dimenze, například to, zda jsou dotčená složka/software soukromé nebo obecně dostupné, zda je ohrožená síť interní nebo externí a zda poskytovatel platebních služeb přestal nebo pravděpodobně přestane plnit svoje povinnosti v infrastrukturách finančního trhu, jichž je členem.

vii. *Dopad na dobrou pověst*

Poskytovatelé platebních služeb by měli zvážit úroveň viditelnosti, které podle jejich nejlepšího vědomí incident na trhu dosáhl nebo pravděpodobně dosáhne. Poskytovatelé platebních služeb by jako dobrý ukazatel možného dopadu na jejich dobrou pověst měli zejména vzít v úvahu pravděpodobnost toho, že incident bude mít negativní společenský dopad. Poskytovatelé platebních služeb by měli zohlednit, zda i) se incident dotkl viditelného procesu, a tudíž se mu pravděpodobně dostane nebo již dostalo mediálního pokrytí (jsou uvažována nejen tradiční média jako noviny, ale také blogy, sociální sítě atd.), ii) došlo nebo pravděpodobně dojde k nesplnění regulačních povinností, iii) došlo nebo pravděpodobně dojde k porušení sankcí nebo iv) ke stejnému druhu incidentu došlo již dříve.

1.4. Poskytovatelé platebních služeb by měli incident posoudit tak, že u každého jednotlivého kritéria určí, zda před vyřešením incidentu bylo nebo pravděpodobně bude dosaženo příslušných prahových hodnot uvedených v tabulce 1.

Tabulka 1: Prahové hodnoty

Kritéria	Nižší úroveň dopadu	Vyšší úroveň dopadu
Dotčené transakce	> 10 % běžné úrovně transakcí dotyčného poskytovatele platebních služeb (z hlediska počtu transakcí) **a** > 100 000 EUR	> 25 % běžné úrovně transakcí dotyčného poskytovatele platebních služeb (z hlediska počtu transakcí) **nebo** > 5 milionů EUR
Dotčení uživatelé platebních služeb	> 5 000 **a** > 10 % uživatelů platebních služeb dotyčného poskytovatele platebních služeb	> 50 000 **nebo** > 25 % uživatelů platebních služeb dotyčného poskytovatele platebních služeb
Délka výpadku služby	> 2 hodiny	nepoužije se
Ekonomický dopad	nepoužije se	> max. (0,1 % kapitálu tier 1, * 200 000 EUR) **nebo** > 5 milionů EUR

Vysoká úroveň interní eskalace	Ano	Ano a pravděpodobně dojde k vyhlášení krizového (nebo podobného) režimu
Ostatní potenciálně dotčení poskytovatelé platebních služeb nebo příslušné infrastruktury	Ano	nepoužije se
Dopad na dobrou pověst	Ano	nepoužije se

*Kapitál tier 1 podle vymezení v článku 25 nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012.

1.5. Poskytovatelé platebních služeb by měli používat odhady, jestliže nemají skutečné údaje, o které by se mohlo opřít jejich posouzení, zda před vyřešením incidentu je nebo pravděpodobně bude dosažena daná prahová hodnota (například by k tomu mohlo dojít ve fázi počátečního šetření).

1.6. Poskytovatelé platebních služeb by měli toto posouzení během trvání incidentu provádět průběžně s cílem zjistit případnou možnou změnu stavu směrem nahoru (z nevýznamného na významný) nebo směrem dolů (z významného na nevýznamný).

Obecný pokyn 2: Postup pro oznamování

2.1. Poskytovatelé platebních služeb by měli shromáždit všechny příslušné informace, vypracovat zprávu o incidentu s použitím formuláře uvedeného v příloze 1 a zprávu předložit příslušnému orgánu v domovském členském státě. Poskytovatelé platebních služeb by měli formulář vyplnit podle instrukcí uvedených v příloze 1.

2.2. Poskytovatelé platebních služeb by měli prostřednictvím stejného formuláře informovat příslušný orgán během doby trvání incidentu (tj. pro účely úvodní, průběžné a konečné zprávy popsané v odstavcích 2.7 až 2.21). Poskytovatelé platebních služeb by měli formulář vyplňovat postupně s vynaložením maximálního úsilí, na základě toho, jak v průběhu svého interního vyšetřování získávají více informací.

2.3. Poskytovatelé platebních služeb by měli příslušnému orgánu ve svém domovském členském státě rovněž předložit kopii případných informací, které byly (nebo budou) poskytnuty uživatelům v souladu s ustanovením druhého paragrafu čl. 96 odst. 1 směrnice o platebních službách, a to jakmile tyto informace budou k dispozici.

2.4. Formou jedné nebo několika příloh přiložených jako doplňující dokumentace k standardizovanému formuláři by poskytovatelé platebních služeb měli příslušnému orgánu v domovském členském státě poskytnout případné další informace, jsou-li takové informace k dispozici a jsou-li považovány za relevantní pro příslušný orgán.

2.5. Poskytovatelé platebních služeb by měli odpovědět na případné žádosti od příslušného orgánu v domovském členském státě o poskytnutí dalších informací nebo objasnění již podané dokumentace.

2.6. Poskytovatelé platebních služeb by měli vždy zachovávat důvěrnost a integritu informací, které si vyměňují s příslušným orgánem ve svém domovském členském státě, a rovněž příslušnému orgánu ve svém domovském členském státě řádně prokázat svoji totožnost.

Úvodní zpráva

2.7. Poskytovatelé platebních služeb by měli příslušnému orgánu v domovském členském státě v okamžiku, kdy je významný operační nebo bezpečnostní incident poprvé zjištěn, předložit úvodní zprávu.

2.8. Poskytovatelé platebních služeb by měli příslušnému orgánu zaslat úvodní zprávu do 4 hodin od okamžiku, kdy je významný operační nebo bezpečnostní incident poprvé zjištěn, nebo v případě, že je známo, že kanály pro předávání zpráv příslušnému orgánu nejsou v té době dostupné nebo funkční, jakmile budou tyto kanály opět dostupné nebo funkční.

2.9. Poskytovatelé platebních služeb by měli úvodní zprávu předložit také příslušnému orgánu v domovském členském státě v okamžiku, kdy se z dříve nevýznamného incidentu stane incident významný. V tomto konkrétním případě by poskytovatelé platebních služeb měli úvodní zprávu zaslat příslušnému orgánu ihned po zjištění změny stavu nebo v případě, že je známo, že kanály pro předávání zpráv příslušnému orgánu nejsou v té době dostupné nebo funkční, jakmile budou tyto kanály opět dostupné nebo funkční.

2.10. Poskytovatelé platebních služeb by měli ve svých úvodních zprávách uvést základní informace ze záhlaví (tj. oddíl A formuláře), a to včetně základní charakteristiky incidentu a důsledků předpokládaných na základě informací, které jsou k dispozici ihned po zjištění nebo změně klasifikace incidentu. V případě, že skutečné údaje nejsou k dispozici, měli by poskytovatelé platebních služeb použít odhady. V úvodní zprávě by poskytovatelé platebních služeb měli rovněž uvést termín následné aktualizace informací, k níž by mělo dojít co nejdříve a v každém případě nejpozději do 3 pracovních dnů.

Průběžná zpráva

2.11. Poskytovatelé platebních služeb by měli průběžné zprávy předkládat vždy, když se domnívají, že došlo k aktualizaci příslušného stavu, a přinejmenším do data následné aktualizace uvedeného v předchozí zprávě (buď v úvodní zprávě, nebo v předchozí průběžné zprávě).

2.12. Poskytovatelé platebních služeb by měli příslušnému orgánu předložit první průběžnou zprávu s podrobnějším popisem incidentu a jeho důsledků (oddíl B formuláře). Kromě toho by poskytovatelé platebních služeb měli vypracovat další průběžné zprávy aktualizující informace uvedené v oddílech A a B formuláře přinejmenším v případech, kdy od

předchozího oznámení zjistí nové příslušné informace nebo významné změny (např. zda došlo k eskalaci nebo ke zmírnění incidentu, nově zjištěné příčiny nebo opatření přijatá k vyřešení problémů). Poskytovatelé platebních služeb by každopádně měli průběžnou zprávu vypracovat na žádost příslušného orgánu v domovském členském státě.

2.13. Jako v případě úvodních zpráv by poskytovatelé platebních služeb, když nejsou k dispozici skutečné údaje, měli použít odhady.

2.14. Dále by poskytovatelé platebních služeb měli v každé zprávě uvést termín následné aktualizace informací, k níž by mělo dojít co nejdříve a v každém případě nejpozději do 3 pracovních dnů. Jestliže poskytovatel platebních služeb nemůže dodržet předpokládaný termín následné aktualizace, měl by kontaktovat příslušný orgán a vysvětlit důvody zpoždění, navrhnout novou reálnou lhůtu pro předložení informací (ne delší než 3 pracovní dny) a zaslat novou průběžnou zprávu aktualizující výhradně informace o předpokládaném termínu následné aktualizace.

2.15. Poskytovatelé platebních služeb by měli zaslat poslední průběžnou zprávu poté, kdy došlo k obnovení běžné činnosti a k návratu činnosti do normálního stavu, a příslušný orgán v ní o této skutečnosti informovat. Poskytovatelé platebních služeb by za návrat obchodní činnosti do normálního stavu měli považovat situaci, kdy se činnost/provoz navrátily na stejnou úroveň služeb/podmínek, která je stanovena poskytovatelem platebních služeb nebo vymezena externě dohodou o úrovni služeb (SLA) z hlediska doby zpracování, kapacity, bezpečnostních požadavků atd., a kdy již nejsou zavedena nouzová opatření.

2.16. Jestliže dojde k návratu obchodní činnosti do normálního stavu do 4 hodin od zjištění incidentu, poskytovatelé platebních služeb by měli usilovat o předložení úvodní i poslední průběžné zprávy zároveň (tj. vyplnit oddíly A a B formuláře) během uvedené čtyřhodinové lhůty.

Závěrečná zpráva

2.17. Poskytovatelé platebních služeb by měli závěrečnou zprávu zaslat po provedení analýzy příčin (bez ohledu na to, zda již byla přijata opatření ke zmírnění rizik nebo zda již byla zjištěna konečná příčina), kdy jsou již k dispozici skutečné údaje nahrazující případné odhady.

2.18. Poskytovatelé platebních služeb by měli závěrečnou zprávu předat příslušnému orgánu maximálně do 2 týdnů od návratu obchodní činnosti do normálního stavu. Poskytovatelé platebních služeb potřebující prodloužení této lhůty (např. v případě, že ještě nejsou k dispozici skutečné údaje o dopadu) by měli příslušný orgán kontaktovat před uplynutím lhůty a sdělit mu odpovídající zdůvodnění zpoždění i nové předpokládané datum předložení závěrečné zprávy.

2.19. Jsou-li poskytovatelé platebních služeb schopni poskytnout veškeré informace vyžadované v závěrečné zprávě (tj. v oddílu C formuláře) během uvedené čtyřhodinové lhůty po zjištění

incidentu, měli by usilovat o předložení informací vztahujících se k úvodní, poslední průběžné a závěrečné zprávě v úvodní zprávě.

2.20. Poskytovatelé platebních služeb by měli usilovat o uvedení úplných informací v závěrečných zprávách, tj. i) skutečných údajů o dopadu namísto odhadů (i případné další potřebné aktualizace v oddílech A a B formuláře) a ii) oddílu C formuláře, který obsahuje příčinu, pokud je již známa, a shrnutí opatření přijatých nebo plánovaných za účelem odstranění problému a zabránění jeho dalšímu opakování v budoucnu.

2.21. Poskytovatelé platebních služeb by měli závěrečnou zprávu rovněž zaslat v okamžiku, kdy v důsledku průběžného posuzování incidentu zjistí, že již oznámený incident nesplňuje kritéria pro to, aby byl považován za významný, a předpokládá se, že je před vyřešením incidentu již splňovat nebude. V tomto případě by poskytovatelé platebních služeb měli závěrečnou zprávu poslat ihned, jakmile je tato skutečnost zjištěna a v každém případě do předpokládaného data stanoveného pro následnou zprávu. V této konkrétní situaci by poskytovatelé platebních služeb místo vyplnění oddílu C formuláře měli zaškrtnout pole „změna klasifikace incidentu na nevýznamný“ a vysvětlit důvody pro snížení hodnocení významnosti incidentu.

Obecný pokyn 3: Přenesené a konsolidované oznamování

3.1. Jestliže to příslušný orgán povolí, poskytovatelé platebních služeb, kteří chtějí plnění oznamovací povinnosti podle směrnice o platebních službách přenést třetí stranu, by měli informovat příslušný orgán v domovském členském státě a zajistit splnění následujících podmínek:

a. Formální smlouva nebo případně existující interní ujednání v rámci skupiny, které upravují přenesené oznamování mezi poskytovatelem platebních služeb a třetí stranou, jednoznačně definují rozdělení povinností všech stran. Zejména jasně stanovují, že bez ohledu na možné přenesení oznamovací povinnosti dotčený poskytovatel platebních služeb zůstává plně odpovědný za splnění požadavků vymezených v článku 96 směrnice o platebních službách a za obsah informací poskytnutých příslušnému orgánu v domovském členském státě.

b. Přenesení povinnosti splňuje požadavky na outsourcing důležitých provozních funkcí podle ustanovení

i. čl. 19 odst. 6 směrnice platebních službách ve vztahu k platebním institucím a institucím elektronických peněz, uplatněné obdobně podle článku 3 směrnice 2009/110/ES o přístupu k činnosti institucí elektronických peněz (EMD); nebo

ii. Obecných pokynů CEBS k outsourcingu ve vztahu k úvěrovým institucím.

c. Informace se předkládají příslušnému orgánu v domovském členském státě předem a v každém případě v souladu s případnými lhůtami a postupy stanovenými příslušným orgánem.

d. Je řádně zajišťována důvěrnost citlivých údajů a kvalita, soudržnost, integrita a spolehlivost informací, které mají být poskytnuty příslušnému orgánu.

3.2. Poskytovatelé platebních služeb, kteří chtějí určené třetí straně umožnit plnění oznamovací povinnosti konsolidovaným způsobem (tj. předložením jedné jediné zprávy vztahující se k několika poskytovatelům platebních služeb dotčeným stejným významným operačním nebo bezpečnostním incidentem), by měli informovat příslušný orgán v domovském členském státě, uvést kontaktní údaje obsažené ve formuláři v části „Dotčený poskytovatel platebních služeb“ a zajistit splnění následujících podmínek:

a. Uvést toto ustanovení ve smlouvě upravující přenesené oznamování.

b. Podmínit konsolidované oznamování tím, že je incident způsoben narušením služeb poskytovaných určenou třetí stranou.

c. Omezit konsolidované oznamování na poskytovatele platebních služeb usazené ve stejném členském státě.

d. Zajistit, aby třetí strana posoudila významnost incidentu pro každého dotčeného poskytovatele platebních služeb a zahrnula do konsolidované zprávy pouze poskytovatele platebních služeb, u kterých je incident klasifikován jako významný. Dále zajistit, aby byl v případě pochyb poskytovatel platebních služeb zahrnut do konsolidované zprávy, pokud neexistují důkazy pro to, že by do takové zprávy neměl být zahrnut.

e. Zajistit, aby v případě, kdy v některých polích formuláře není možné uvést společnou odpověď (např. oddíl B 2, B 4 nebo C 3), třetí strana buď i) vyplnila tato pole zvlášť pro každého dotčeného poskytovatele platebních služeb a dále uvedla totožnost každého poskytovatele platebních služeb, k němuž se informace vztahují, nebo ii) použila v polích, kde je tato možnost k dispozici, rozmezí představující nejnižší a nejvyšší hodnotu zjištěnou nebo odhadovanou u různých poskytovatelů platebních služeb.

f. Poskytovatelé platebních služeb by měli zajistit, aby jim třetí strana vždy průběžně poskytovala veškeré příslušné informace o incidentu a všech interakcích třetí strany s příslušným orgánem a o jejich obsahu, avšak tak, aby nedošlo k porušení mlčenlivosti u informací, které se vztahují k jiným poskytovatelům platebních služeb.

3.3. Poskytovatelé platebních služeb by neměli oznamovací povinnost přenášet, pokud o tom neinformovali příslušný orgán v domovském členském státě nebo pokud byli informováni, že dohoda o outsourcingu nesplňuje požadavky uvedené v obecném pokynu 3.1 písm. b).

3.4. Poskytovatelé platebních služeb, kteří chtějí zrušit přenesení oznamovací povinnosti, by měli toto rozhodnutí sdělit příslušnému orgánu v domovském členském státě v souladu se lhůtami a postupy stanovenými příslušným orgánem. Poskytovatelé platebních služeb by měli příslušný orgán v domovském členském státě rovněž informovat o případném podstatném vývoji událostí ovlivňujícím určenou třetí stranu a její schopnost plnit oznamovací povinnost.

3.5. Poskytovatelé platebních služeb by měli svoji oznamovací povinnost věcně plnit bez vnější pomoci, jestliže určená třetí strana neinformovala příslušný orgán v domovském členském státě o významném operačním nebo bezpečnostním incidentu v souladu s článkem 96 směrnice o platebních službách a s těmito obecnými pokyny. Dále by poskytovatelé platebních služeb měli zajistit, aby incident nebyl oznámen dvakrát, a to individuálně dotyčným poskytovatelem platebních služeb a ještě jednou touto třetí stranou.

Obecný pokyn 4: Operační a bezpečnostní zásady

4.1. Poskytovatelé platebních služeb by měli zajistit, aby jejich obecné operační a bezpečnostní zásady jasně definovaly veškeré povinnosti související s oznamováním incidentů podle směrnice o platebních službách i procesy zavedené s cílem splnit požadavky stanovené v těchto obecných pokynech.

5. Obecné pokyny určené příslušným orgánům týkající se kritérií pro posuzování závažnosti incidentu a podrobných informací uvedených ve zprávách o incidentu poskytovaných dalším vnitrostátním orgánům

Obecný pokyn 5: Posouzení závažnosti incidentu

5.1. Příslušné orgány v domovském členském státě by měly posoudit závažnost významného operačního nebo bezpečnostního incidentu pro další vnitrostátní orgány na základě vlastního odborného posouzení a s použitím následujících kritérií, které slouží jako primární ukazatele významnosti uvedeného incidentu:

a. Příčiny incidentu spadají do regulační pravomoci jiného vnitrostátního orgánu (tj. do jeho oblasti působnosti).
b. Důsledky incidentu mají dopad na cíle jiného vnitrostátního orgánu (např. zabezpečení finanční stability).
c. Incident ovlivňuje nebo by mohl ve velkém rozsahu ovlivnit uživatele platebních služeb.
d. Incidentu se pravděpodobně dostane nebo dostalo velkého mediálního pokrytí.

5.2. Příslušné orgány v domovském členském státě by měly toto posouzení provádět průběžně během trvání incidentu s cílem zjistit případnou možnou změnu, v důsledku které by se incident mohl stát závažným, přestože dříve za závažný považován nebyl.

Obecný pokyn 6: Poskytované informace

6.1. Nehledě na případné jiné požadavky, které vyplývají z právních předpisů ohledně sdílení informací týkajících se incidentů s dalšími vnitrostátními orgány, by příslušné orgány měly poskytnout informace o významných operačních nebo bezpečnostních incidentech alespoň vnitrostátním orgánům určeným na základě uplatnění ustanovení obecného pokynu 5.1 (tj. „dalším příslušným vnitrostátním orgánům“), a to po obdržení úvodní zprávy (nebo případné zprávy, která je podnětem k sdílení informací) a po té, kdy jsou informovány o tom, že došlo k návratu obchodní činnosti do normálního stavu (tj. v poslední průběžné zprávě).

6.2. Příslušné orgány by měly dalším příslušným vnitrostátním orgánům předložit informace potřebné k utvoření jasného obrazu toho, co se stalo, a potenciálních důsledků. Za tímto účelem by měly poskytnout alespoň informace uvedené poskytovatelem platebních služeb v následujících polích formuláře (v úvodní nebo průběžné zprávě):

- datum a čas zjištění incidentu,
- datum a čas vzniku incidentu,
- datum a čas, kdy během incidentu došlo nebo podle očekávání dojde k návratu do původního stavu,
- stručný popis incidentu (včetně částí podrobného popisu, které nejsou citlivými informacemi),
- stručný popis opatření učiněných nebo plánovaných za účelem obnovy po incidentu,
- popis toho, jak by incident mohl ovlivnit jiné poskytovatele platebních služeb a/nebo infrastruktury,
- popis (případného) mediálního pokrytí,
- příčina incidentu.

6.3. Před poskytnutím informací vztahujících se k incidentu dalším příslušným vnitrostátním orgánům by příslušné orgány měly podle potřeby provést řádnou anonymizaci a vynechat informace, na které by se mohla vztahovat omezení související se zachováním mlčenlivosti nebo s duševním vlastnictvím. Příslušné orgány by však měly dalším příslušným vnitrostátním orgánům sdělit jméno a adresu poskytovatele platebních služeb, který oznámení učinil, pokud dotyčné vnitrostátní orgány mohou zaručit, že s informacemi bude nakládáno jako s důvěrnými.

6.4. Příslušné orgány by měly vždy zachovat důvěrnost a integritu uchovávaných informací a informací, které si vyměňují s dalšími příslušnými vnitrostátními orgány, a rovněž dalším příslušným vnitrostátním orgánům řádně prokázat svoji totožnost. Aniž by bylo dotčeno platné právo Unie a vnitrostátní požadavky, příslušné orgány by se všemi informacemi obdrženými na základě těchto obecných pokynů měly zacházet zejména v souladu s povinností zachovat profesní tajemství, která je vymezena ve směrnici o platebních službách.

6. Obecné pokyny určené příslušným orgánům týkající se kritérií pro posuzování příslušných podrobných informací uvedených ve zprávách o incidentu a poskytovaných orgánu EBA a ECB a k formátu a postupům při jejich komunikaci

Obecný pokyn 7: Poskytované informace

7.1. Příslušné orgány by měly orgánu EBA a ECB vždy poskytovat všechny zprávy obdržené od poskytovatelů platebních služeb (nebo jménem poskytovatelů platebních služeb) dotčených významným operačním nebo bezpečnostním incidentem (tj. úvodní, průběžné a závěrečné zprávy).

Obecný pokyn 8: Komunikace

8.1. Příslušné orgány by měly vždy zachovat důvěrnost a integritu uchovávaných informací a informací, které si vyměňují s orgánem EBA a ECB, a rovněž orgánu EBA a ECB řádně prokázat svoji totožnost. Aniž by bylo dotčeno platné právo Unie a vnitrostátní požadavky, příslušné orgány by se všemi informacemi obdrženými na základě těchto obecných pokynů měly zacházet zejména v souladu s povinností zachovat profesní tajemství, která je vymezena ve směrnici o platebních službách.

8.2. Aby se předešlo prodlení při předávání informací vztahujících se k incidentu orgánu EBA/ECB a přispělo k minimalizaci rizik narušení provozu, příslušné orgány by měly podporovat odpovídající komunikační prostředky.

Příloha 1 – Formuláře pro účely oznamování určené poskytovatelům platebních služeb

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 ☐ Estimation As a % of regular number of transactions — ☐ Actual figure ☐ Estimation Value of transactions affected in EUR — ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected — ☐ Actual figure ☐ Estimation As a %-of total payment service users — ☐ Actual figure ☐ Estimation
Service downtime[4]	Total service downtime DD:HH:MM — ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR — ☐ Actual figure ☐ Estimation Indirect costs in EUR — ☐ Actual figure ☐ Estimation
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 remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ 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 - addittional 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**

INSTRUKCE PRO VYPLNĚNÍ FORMULÁŘŮ

Poskytovatelé platebních služeb by měli vyplnit příslušný oddíl formuláře v závislosti na fázi oznamování, ve které se nacházejí: oddíl A pro úvodní zprávu, oddíl B pro průběžné zprávy a oddíl C pro závěrečnou zprávu. Není-li výslovně stanoveno jinak, všechna pole jsou povinná.

Záhlaví

Úvodní zpráva: jedná se o první oznámení, které poskytovatel platebních služeb předkládá příslušnému orgánu v domovském členském státě.

Průběžná zpráva: jedná se o aktualizaci předchozí (úvodní nebo průběžné) zprávy vztahující se k témuž incidentu.

Poslední průběžná zpráva: informuje příslušný orgán v domovském členském státě o tom, že došlo k obnovení běžné činnosti a k návratu obchodní činnosti do normálního stavu, takže již nebudou předkládány žádné další průběžné zprávy.

Závěrečná zpráva: jedná se o poslední zprávu, kterou poskytovatel platebních služeb v souvislosti s incidentem zašle, neboť i) již byla provedena analýza příčin a odhady byly nahrazeny skutečnými údaji nebo ii) incident již není považován za významný.

Změna klasifikace incidentu na nevýznamný: incident již nesplňuje kritéria pro to, aby byl považován za významný, a nepředpokládá se, že je před vyřešením bude splňovat. Poskytovatelé platebních služeb by měli vysvětlit důvody pro toto snížení hodnocení významnosti.

Datum a čas předložení zprávy: přesné datum a čas předložení zprávy příslušnému orgánu.

Přidělené identifikační číslo incidentu (u průběžných a závěrečných zpráv): referenční číslo přidělené příslušným orgánem na základě úvodní zprávy, které případně jednoznačně identifikuje incident (tj. pokud příslušný orgán takové referenční číslo sdělí).

A – Úvodní zpráva

A 1 – Obecné údaje

Druh zprávy:

Individuální: zpráva se vztahuje k jedinému poskytovateli platebních služeb.

Konsolidovaná: zpráva se vztahuje k několika poskytovatelům platebních služeb a využívá možnosti konsolidovaného oznámení. Pole pod řádkem „Dotčený poskytovatel platebních služeb“ se nevyplňují (s výjimkou pole „Země dotčené incidentem“) a v příslušné tabulce (Konsolidovaná zpráva – Seznam poskytovatelů platebních služeb) by měl být uveden seznam poskytovatelů platebních služeb, kteří jsou do zprávy zahrnuti.

Dotčený poskytovatel platebních služeb: označuje poskytovatele platebních služeb, u něhož k incidentu došlo.

Jméno poskytovatele platebních služeb: celé jméno poskytovatele platebních služeb, jehož se oznámení týká, tak, jak je toto jméno uvedeno v příslušném úředním vnitrostátním registru platebních poskytovatelů služeb.

Případné jedinečné identifikační číslo poskytovatele platebních služeb: příslušné jedinečné identifikační číslo používané v každém členském státě k identifikaci poskytovatele platebních služeb, které se uvede, jestliže není vyplněno pole „Číslo povolení poskytovatele platebních služeb“.

Číslo povolení poskytovatele platebních služeb: číslo povolení v domovském členském státě.

Vedoucí skupiny: v případě skupin podniků podle vymezení v čl. 4 odst. 40 směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES

a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES, uveďte jméno řídicího podniku.

Domovská země: členský stát, ve kterém se nachází sídlo poskytovatele platebních služeb, nebo v případě, že poskytovatel platebních služeb podle vnitrostátního práva nemá žádné sídlo, pak členský stát, ve kterém se nachází jeho ústředí.
Země dotčené incidentem: jedna země nebo více zemí, ve kterých se projevil dopad incidentu (např. je dotčeno několik poboček poskytovatele platebních služeb nacházejících se v různých zemích. Nemusí se jednat o domovský členský stát.
Primární kontaktní osoba: jméno a příjmení osoby odpovědné za oznámení incidentu nebo v případě, že oznámení jménem dotčeného poskytovatele platebních služeb činí třetí osoba, jméno a příjmení osoby odpovědné za oddělení řízení incidentů/rizik nebo podobnou oblast u dotčeného poskytovatele platebních služeb.
E-mail: e-mailová adresa, na kterou lze v případě potřeby zasílat žádosti o bližší vysvětlení. Může se jednat o osobní nebo firemní e-mail.
Telefon: telefonní číslo, na které lze zavolat s případnými žádostmi o bližší vysvětlení. Může se jednat o osobní nebo firemní telefonní číslo.
Sekundární kontaktní osoba: jméno a příjmení alternativní osoby, kterou může příslušný orgán kontaktovat s dotazy týkajícími se incidentu, pokud není primární kontaktní osoba k zastižení. V případě, že oznámení jménem dotčeného poskytovatele platebních služeb činí třetí osoba, jméno a příjmení alternativní osoby z oddělení řízení incidentů/rizik nebo podobné oblasti u dotčeného poskytovatele platebních služeb.
E-mail: e-mailová adresa alternativní kontaktní osoby, na kterou lze v případě potřeby zasílat žádosti o bližší vysvětlení. Může se jednat o osobní nebo firemní e-mailovou adresu.
Telefon: telefonní číslo alternativní kontaktní osoby, na které lze zavolat s případnými žádostmi o bližší vysvětlení. Může se jednat o osobní nebo firemní telefonní číslo.

Oznamující subjekt: tento oddíl se vyplní v případě, že jménem dotčeného poskytovatele platebních služeb plní oznamovací povinnost třetí strana.

Jméno oznamujícího subjektu: celé jméno subjektu, který incident oznamuje, tak, jak je toto jméno uvedeno v příslušném úředním vnitrostátním obchodním rejstříku.
Případné jedinečné identifikační číslo: příslušné jedinečné identifikační číslo používané v zemi, kde je třetí strana usazena, které slouží k identifikaci subjektu, jenž incident oznamuje, a které se uvede, jestliže není vyplněno pole „Číslo povolení“.
Případné číslo povolení: případné číslo povolení třetí strany v zemi, v níž je usazena.
Primární kontaktní osoba: jméno a příjmení osoby odpovědné za oznámení incidentu.
E-mail: e-mailová adresa, na kterou lze v případě potřeby zasílat žádosti o bližší vysvětlení. Může se jednat o osobní nebo firemní e-mail.
Telefon: telefonní číslo, na které lze zavolat s případnými žádostmi o bližší vysvětlení. Může se jednat o osobní nebo firemní telefonní číslo.
Sekundární kontaktní osoba: jméno a příjmení alternativní osoby v subjektu oznamujícím incident, kterou může příslušný orgán kontaktovat, pokud není primární kontaktní osoba k zastižení.
E-mail: e-mailová adresa alternativní kontaktní osoby, na kterou lze v případě potřeby zasílat žádosti o bližší vysvětlení. Může se jednat o osobní nebo firemní e-mailovou adresu.
Telefon: telefonní číslo alternativní kontaktní osoby, na které lze zavolat s případnými žádostmi o bližší vysvětlení. Může se jednat o osobní nebo firemní telefonní číslo.

A 2 – Zjištění incidentu a prvotní klasifikace

Datum a čas zjištění incidentu: datum a čas, kdy byl incident poprvé identifikován.

Kdo incident zjistil: uveďte, zda incident zjistil uživatel platební služby, jiná strana v rámci poskytovatele platebních služeb (např. funkce interního auditu) nebo externí strana (např. externí poskytovatel služeb). Pokud se nejedná o žádnou z uvedených možností, vysvětlete v příslušném poli.

Stručný a obecný popis incidentu: stručně vysvětlete nejdůležitější problémy související s incidentem, včetně možných příčin, bezprostředních dopadů atd.

Předpokládaný termín následné aktualizace: uveďte předpokládané datum a čas předložení následné aktualizace (průběžné nebo závěrečné zprávy).

B – Průběžná zpráva

B 1 – Obecné údaje

Podrobnější popis incidentu: popište hlavní rysy incidentu a uveďte přitom přinejmenším body zmíněné v dotazníku (s jakým konkrétním problémem se poskytovatel platebních služeb potýká, jak problém začal a jak se vyvíjel, možná souvislost s předchozím incidentem, důsledky, zejména pro uživatele platebních služeb atd.).

Datum a čas vzniku incidentu: datum a čas, kdy incident začal, je-li to známo.

Stav incidentu:

Diagnostika: právě byla stanovena charakteristika incidentu.

Oprava: probíhá rekonfigurace napadených položek.

Obnova: u položek, u kterých došlo k selhání, probíhá navrácení do jejich posledního obnovitelného stavu.

Opětovné zahájení provozu: služba související s platbami je opět poskytována.

Datum a čas, kdy u incidentu došlo nebo podle očekávání dojde k návratu do původního stavu: uveďte datum a čas, kdy incident byl nebo podle očekávání bude pod kontrolou a kdy došlo nebo podle očekávání dojde k návratu obchodní činnosti do normálního stavu.

B 2 – Klasifikace incidentu / informace o incidentu

Celkový dopad: uveďte, které dimenze byly incidentem dotčeny. Je možné zaškrtnout více políček.

Integrita: zajištění správnosti a úplnosti aktiv (včetně údajů).

Dostupnost: skutečnost, že služby související s platbami jsou přístupné uživatelům platebních služeb a uživatelé platebních služeb je mohou používat.

Důvěrnost: skutečnost, že se informace nezpřístupňují ani nesdělují neoprávněným osobám, subjektům nebo pro nedovolené účely.

Autenticita: vlastnost zajišťující, že je zdroj tím, čím tvrdí, že je.

Kontinuita: skutečnost, že procesy, úlohy a aktiva organizace potřebné za účelem poskytování služeb souvisejících s platbami jsou plně přístupné a probíhají na přijatelných, předem stanovených úrovních.

Dotčené transakce: Poskytovatelé platebních služeb by měli uvést, které prahové hodnoty byly nebo pravděpodobně budou incidentem dosaženy, a související údaje: počet dotčených transakcí, procentuální podíl dotčených transakcí z počtu platebních transakcí prováděných prostřednictvím stejných platebních služeb, které byly incidentem dotčeny, a celková hodnota transakcí. Poskytovatelé platebních služeb by měli uvést konkrétní hodnoty těchto proměnných, přičemž se může jednat o skutečné údaje nebo o odhady. Subjekty provádějící oznámení jménem několika poskytovatelů platebních služeb (tj. konsolidované oznámení) mohou místo

toho uvést rozmezí hodnot představující nejnižší a nejvyšší zjištěné nebo odhadované hodnoty v rámci skupiny poskytovatelů platebních služeb zahrnutých do zprávy, přičemž hodnoty se oddělí spojovníkem. Poskytovatelé platebních služeb by obecně měli jako „dotčené transakce" chápat veškeré vnitrostátní a přeshraniční transakce, které incidentem byly nebo pravděpodobně budou přímo nebo nepřímo dotčeny, a zejména pak transakce, které nebylo možné iniciovat nebo zpracovat, transakce, u kterých došlo k pozměnění obsahu platební zprávy, a transakce, k nimž byl příkaz zadán podvodně (bez ohledu na to, zda finanční prostředky byly či nebyly získány zpět). Dále by poskytovatelé platebních služeb měli za běžnou úroveň platebních transakcí považovat denní roční průměr vnitrostátních a přeshraničních platebních transakcí provedených prostřednictvím stejných platebních služeb, které byly incidentem dotčeny, s použitím předchozího roku jako referenčního období při výpočtu. Jestliže poskytovatelé platebních služeb tento údaj nepovažují za vypovídající (např. kvůli sezónnosti), měli by místo toho použít jiné, více vypovídající měřítko a sdělit příslušnému orgánu příslušné odůvodnění tohoto přístupu v poli „Poznámky".

Dotčení uživatelé platebních služeb: Poskytovatelé platebních služeb by měli uvést, které prahové hodnoty byly nebo pravděpodobně budou incidentem dosaženy, a související údaje: celkový počet uživatelů platebních služeb, kteří byli dotčeni, a procentuální podíl dotčených uživatelů platebních služeb z celkového počtu uživatelů platebních služeb. Poskytovatelé platebních služeb by měli uvést konkrétní hodnoty těchto proměnných, přičemž se může jednat o skutečné údaje nebo o odhady. Subjekty provádějící oznámení jménem několika poskytovatelů platebních služeb (tj. konsolidované oznámení) mohou místo toho uvést rozmezí hodnot představující nejnižší a nejvyšší zjištěné nebo odhadované hodnoty v rámci skupiny poskytovatelů platebních služeb zahrnutých do zprávy, přičemž hodnoty se oddělí spojovníkem. Poskytovatelé platebních služeb by měli jako „dotčené uživatele platebních služeb" chápat všechny klienty (vnitrostátní nebo zahraniční, spotřebitele nebo podniky), kteří mají s dotčeným poskytovatelem platebních služeb smlouvu, na jejímž základě mají přístup k dotčené platební službě, a kteří pociťují nebo pravděpodobně pocítí důsledky incidentu. Při určování počtu uživatelů platebních služeb, kteří by bývali mohli platební službu využívat během trvání incidentu, by poskytovatelé platebních služeb měli použít odhady vycházející z dřívější aktivity. V případě skupin by měl každý poskytovatel platebních služeb brát v úvahu pouze svoje vlastní uživatele platebních služeb. V případě poskytovatele platebních služeb nabízejícího operační služby jiným by měl dotyčný poskytovatel platebních služeb brát v úvahu pouze svoje případné vlastní uživatele platebních služeb, přičemž poskytovatelé platebních služeb, kteří jsou příjemci těchto operačních služeb, by měli rovněž posoudit incident ve vztahu ke svým vlastním uživatelům platebních služeb. Dále by poskytovatelé platebních služeb měli jako celkový počet uživatelů platebních služeb použít souhrnný počet vnitrostátních a přeshraničních uživatelů platebních služeb, kteří jsou s nimi smluvně svázáni v okamžiku incidentu (popřípadě nejaktuálnější dostupný údaj) a kteří mají přístup k dotčené platební službě bez ohledu na jejich velikost nebo na to, zda jsou považováni za aktivní nebo pasivní uživatele platebních služeb.

Délka výpadku služby: Poskytovatelé platebních služeb by měli uvést, zda při incidentu je nebo pravděpodobně bude dosaženo prahové hodnoty, a související údaj: celkovou délku výpadku služby. Poskytovatelé platebních služeb by měli uvést konkrétní hodnoty této proměnné, přičemž se může jednat o skutečné údaje nebo o odhady. Subjekty provádějící oznámení jménem několika poskytovatelů platebních služeb (tj. konsolidované oznámení) mohou místo toho uvést rozmezí hodnot představující nejnižší a nejvyšší zjištěné nebo odhadované hodnoty v rámci skupiny poskytovatelů platebních služeb zahrnutých do zprávy, přičemž hodnoty se oddělí spojovníkem. Poskytovatelé platebních služeb by měli zohlednit dobu, po kterou trvá nebo pravděpodobně bude trvat výpadek jakékoliv úlohy, procesu nebo kanálu vztahujícího se k poskytování platebních služeb, který tudíž znemožňuje i) iniciování a/nebo provedení platební

služby a/nebo ii) přístup k platebnímu účtu. Poskytovatelé platebních služeb by měli měřit délku výpadku služby od okamžiku, kdy výpadek začne, a měli by zohlednit časové úseky, kdy mají otevřeno pro obchody potřebné pro provedení platebních služeb, a v případě potřeby i dobu, kdy mají zavřeno a kdy provádějí údržbu. Nemohou-li poskytovatelé platebních služeb určit, kdy výpadek služby začal, měli by ve výjimečných případech měřit délku výpadku služby od okamžiku, kdy byl výpadek zjištěn.

Ekonomický dopad: Poskytovatelé platebních služeb by měli uvést, zda při incidentu je nebo pravděpodobně bude dosaženo prahové hodnoty, a související údaj: přímé náklady a nepřímé náklady. Poskytovatelé platebních služeb by měli uvést konkrétní hodnoty těchto proměnných, přičemž se může jednat o skutečné údaje nebo o odhady. Subjekty provádějící oznámení jménem několika poskytovatelů platebních služeb (tj. konsolidované oznámení) mohou místo toho uvést rozmezí hodnot představující nejnižší a nejvyšší zjištěné nebo odhadované hodnoty v rámci skupiny poskytovatelů platebních služeb zahrnutých do zprávy, přičemž hodnoty se oddělí spojovníkem. Poskytovatelé platebních služeb by měli zohlednit náklady přímo související s incidentem i náklady, které se k incidentu vztahují nepřímo. Poskytovatelé platebních služeb by měli mimo jiné vzít v úvahu ztracené finanční prostředky nebo aktiva, reprodukční náklady hardwaru nebo softwaru, další soudní náklady nebo náklady na nápravu škod, poplatky v důsledku nedodržení smluvních povinností, sankce, externí závazky a ušlé výnosy. Pokud jde o nepřímé náklady, poskytovatelé platebních služeb by měli zohlednit pouze ty, které jsou již známy nebo které velmi pravděpodobně vzniknou.

> **Přímé náklady:** výše přímých nákladů spojených s incidentem v peněžním vyjádření (v eurech), včetně finančních prostředků potřebných k nápravě incidentu (např. ztracené finanční prostředky nebo aktiva, reprodukční náklady hardwaru a softwaru, poplatky v důsledku nedodržení smluvních povinností).
>
> **Nepřímé náklady:** výše nepřímých nákladů spojených s incidentem v peněžním vyjádření (v eurech) (např. náhrada škody / náklady na kompenzaci zákazníků, ušlé výnosy v důsledku promarněných obchodních příležitostí, potenciální právní náklady).

Vysoká úroveň interní eskalace: Poskytovatelé platebních služeb by měli zvážit, zda v důsledku dopadu na služby související s platbami byl nebo pravděpodobně bude o incidentu informován ředitel informačních technologií (nebo osoba zastávající podobnou funkci), a to mimo pravidelný postup podávání zpráv a průběžně po dobu trvání incidentu. V případě přeneseného oznamování by k eskalaci došlo v rámci třetí strany. Dále by poskytovatelé platebních služeb měli zohlednit, zda v důsledku dopadu incidentu na služby související s platbami byl nebo pravděpodobně bude zahájen krizový režim.

Další potenciálně dotčení poskytovatelé platebních služeb nebo příslušné infrastruktury: poskytovatelé platebních služeb by měli posoudit dopad incidentu na finanční trh, který je chápán jako infrastruktury finančního trhu a/nebo systémy pro platby prováděnou kartou podporující tyto a ostatní poskytovatele platebních služeb. Poskytovatelé platebních karet by zejména měli posoudit, zda se incident projevil nebo pravděpodobně projeví u jiných poskytovatelů platebních služeb, zda ovlivnil nebo pravděpodobně ovlivní hladké fungování infrastruktur finančního trhu a zda ohrozil nebo pravděpodobně ohrozí spolehlivost finančního systému jako celku. Poskytovatelé platebních služeb by měli zohlednit různé dimenze, například to, zda jsou dotčená složka/software důvěrné nebo obecně dostupné, zda je ohrožená síť interní nebo externí a zda poskytovatel platebních služeb přestal nebo pravděpodobně přestane plnit svoje povinnosti v infrastrukturách finančního trhu, jichž je členem.

Dopad na dobrou pověst: Poskytovatelé platebních služeb by měli zvážit úroveň viditelnosti, které podle jejich nejlepšího vědomí incident na trhu dosáhl nebo pravděpodobně dosáhne. Poskytovatelé platebních služeb by jako dobrý ukazatel možného dopadu na jejich dobrou

pověst měli vzít v úvahu zejména pravděpodobnost toho, že incident bude mít negativní společenský dopad. Poskytovatelé platebních služeb by měli zohlednit, zda i) se incident dotkl viditelného procesu, a tudíž se mu pravděpodobně dostane nebo již dostalo mediálního pokrytí (jsou uvažována nejen tradiční média jako noviny, ale také blogy, sociální sítě atd.), ii) došlo nebo pravděpodobně dojde k nesplnění regulačních povinností, (iii) došlo nebo pravděpodobně dojde k porušení sankcí nebo iv) ke stejnému druhu incidentu došlo již dříve.

B 3 – Popis incidentu

Druh incidentu: uveďte, zda se podle vašeho nejlepšího vědomí jedná o operační nebo bezpečnostní incident.

Operační: incident vyplývající z nevhodných procesů, osob a systémů či procesů, osob a systémů, u kterých došlo k selhání, nebo událostí vyšší moci, které ovlivňují integritu, dostupnost, důvěrnost, autenticitu a/nebo kontinuitu služeb souvisejících s platbami.

Bezpečnostní: neoprávněný přístup, používání, prozrazení, narušení, modifikace nebo zničení aktiv poskytovatele platebních služeb, které ovlivňují integritu, dostupnost, důvěrnost, autenticitu a/nebo kontinuitu služeb souvisejících s platbami. Tato situace může mimo jiné nastat, když u poskytovatele platebních služeb dojde ke kybernetickým útokům, nebo když se návrh nebo provádění bezpečnostních zásad či fyzická ostraha projeví jako nevhodné.

Příčina incidentu: uveďte příčinu incidentu nebo v případě, že dosud není známa, nejpravděpodobnější možnou příčinu. Je možné zaškrtnout více políček.

Probíhá šetření: příčina dosud nebyla stanovena.

Externí útok: zdroj příčiny pochází zvnějšku a úmyslně cílí na poskytovatele platebních služeb (např. útoky prostřednictvím malwaru).

Interní útok: zdroj příčiny pochází zevnitř a úmyslně cílí na poskytovatele platebních služeb (např. interní podvod).

Druh útoku:

Distribuované odepření služby / odepření služby (D/DoS): pokus znepřístupnit on-line službu tím, že dojde k jejímu zahlcení provozem z více zdrojů.

Nákaza interních systémů: škodlivá činnost, která napadá počítačové systémy ve snaze ukrást prostor na pevném disku nebo čas procesoru, získat přístup k soukromým informacím, poškodit data, rozeslat kontaktům nevyžádanou poštu atd.

Cílený průnik: neoprávněná špionáž, špehování a krádež informací prostřednictvím kybernetického prostoru.

Jiné: jakýkoliv jiný druh útok, k němuž u poskytovatele platebních služeb mohlo přímo či prostřednictvím poskytovatele služeb dojít. Toto políčko by mělo být zaškrtnuto zejména, pokud došlo k útoku, který se zaměřil na proces autorizace a ověření. Podrobnosti se uvedou ve volném textovém poli.

Externí události: příčina souvisí s událostmi, které se obecně nacházejí mimo kontrolu dotyčné organizace (např. přírodní katastrofy, právní problémy, obchodní problémy a závislost na službách).

Lidská chyba: incident byl způsoben neúmyslnou chybou člověka, ať už v rámci postupu při provádění platby (např. nahrání chybného dávkového souboru plateb do platebního systému), nebo v souvislosti s ním (např. náhodné odpojení od elektrického proudu a pozastavení platební činnosti).

Selhání procesu: příčinou incidentu byl chybný návrh nebo provedení platebního procesu, kontrol procesu a/nebo podpůrných procesů (např. proces změny / migrace dat, testování, konfigurace, kapacita, monitorování).

Selhání systému: příčina incidentu souvisí s nevhodným návrhem, provedením, složkami, specifikacemi, integrací nebo složitostí systémů, které platební činnost podporují.
Jiné: žádná z výše uvedených možností není příčinou. Další podrobnosti se uvedou ve volném textovém poli.

Dotkl se vás incident přímo nebo nepřímo prostřednictvím poskytovatele služeb?: incident se může zaměřit na poskytovatele platebních služeb přímo, nebo ho může ovlivnit nepřímo prostřednictvím třetí strany. V případě nepřímého dopadu uveďte jméno poskytovatelů služeb.

B 4 – Dopad incidentu

Případné dotčené **budovy (adresy):** je-li dotčena fyzická budova, uveďte její adresu.

Dotčené obchodní kanály: uveďte kanál nebo kanály pro spojení s uživateli platebních služeb dotčené incidentem. Je možné zaškrtnout více políček.

Pobočky: provozovna (s výjimkou ústředí), která je součástí poskytovatele platebních služeb, nemá právní subjektivitu a přímo vykonává některé nebo všechny transakce, které jsou součástí obchodní činnosti poskytovatele platebních služeb. Všechna místa výkonu obchodní činnosti zřízená v tomtéž členském státě poskytovatelem platebních služeb s ústředím v jiném členském státě by měla být považována za jedinou pobočku.
Elektronické bankovnictví: využívání počítačů k provádění finančních transakcí přes internet.
Telefonní bankovnictví: používání telefonů k provádění finančních transakcí.
Mobilní bankovnictví: používání zvláštní bankovní aplikace v chytrém telefonu nebo v podobném zařízení k provádění finančních transakcí.
Bankomaty: elektromechanická zařízení, která umožňují uživatelům platebních služeb výběr hotovosti z jejich účtů a/nebo přístup k dalším službám.
Místo prodeje: fyzický prostor obchodníka, kde je iniciována platební transakce.
Jiné: dotčeným obchodním kanálem není žádná z výše uvedených možností. Další podrobnosti se uvedou ve volném textovém poli.

Dotčené platební služby: uveďte platební služby, které v důsledku incidentu řádně nefungují. Je možné zaškrtnout více políček.

Vložení hotovosti na platební účet: předání hotovosti poskytovateli platebních služeb za účelem jejího připsání na platební účet.
Výběr hotovosti z platebního účtu: poskytovatel platebních služeb obdrží od uživatele platebních služeb požadavek, aby poskytl hotovost a příslušnou částku strhl z uživatelova platebního účtu.
Operace nutné k vedení platebního účtu: úkony, které je u platebního účtu potřeba provést za účelem jeho aktivace, zrušení a/nebo správy (např. zřízení, zablokování).
Pořizování platebních prostředků: platební služba, kdy poskytovatel platebních služeb uzavře s příjemcem smlouvu o přijímání a zpracování platebních transakcí, což vede k převodu peněžních prostředků příjemci.
Úhrady: platební služba za účelem připsání částky na platební účet příjemce prostřednictvím platební transakce nebo řady platebních transakcí z platebního účtu plátce provedených na základě pokynů plátce poskytovatelem platebních služeb, u něhož má plátce veden platební účet.
Inkaso: platební služba pro odepsání částky transakce z účtu plátce, při níž podnět k platební transakci dává příjemce na základě souhlasu, který plátce udělil příjemci,

poskytovateli platebních služeb příjemce nebo svému vlastnímu poskytovateli platebních služeb.

Platby kartou: platební služba založená na infrastruktuře a obchodních pravidlech systému platebních karet a používaná k provedení platební transakce pomocí karty nebo telekomunikačního, digitálního či informačně-technologického zařízení nebo softwaru, je-li jejím výsledkem transakce uskutečněná debetní nebo kreditní kartou. Karetními platebními transakcemi nejsou transakce založené na jiných druzích platebních služeb.

Vydávání platebních prostředků: platební služba, kdy poskytovatel platebních služeb uzavře s plátcem smlouvu o poskytnutí platebních prostředků, což vede k iniciování a zpracování platebních transakcí plátce.

Poukazování peněz: platební služba, při které dochází k přijetí peněžních prostředků od plátce, bez vytvoření jakéhokoliv platebního účtu na jméno plátce nebo příjemce, výhradně za účelem převodu příslušné částky příjemci nebo jinému poskytovateli platebních služeb jednajícímu jménem příjemce nebo při níž dochází k přijetí těchto peněžních prostředků jménem příjemce a jejich zpřístupnění příjemci.

Služby iniciování platby: služba k iniciování platebního příkazu na žádost uživatele platebních služeb ve vztahu k platebnímu účtu vedenému u jiného poskytovatele platebních služeb.

Služby informování o účtu: platební služby on-line, jejichž cílem je poskytnout konsolidované informace o jednom nebo více platebních účtech uživatele platebních služeb vedených buď u jiného poskytovatele platebních služeb, nebo u více než jednoho poskytovatele platebních služeb.

Jiné: dotčenou platební službou není žádná z výše uvedených možností. Další podrobnosti se uvedou ve volném textovém poli.

Dotčená funkční oblast: uveďte krok nebo kroky platebního procesu, které byly incidentem dotčeny. Je možné zaškrtnout více políček.

Ověření/autorizace: postupy, které poskytovateli platebních služeb umožňují ověřit totožnost uživatele platebních služeb nebo platnost použití konkrétního platebního prostředku, včetně využití osobních bezpečnostních údajů uživatele a udělení souhlasu uživatele platebních služeb (nebo třetí strany jednající jeho jménem) k převedení prostředků nebo cenných papírů.

Komunikace: tok informací za účelem identifikace, ověření, oznamování a informování mezi poskytovatelem platebních služeb, který vede účet, a poskytovateli služby iniciování platby, poskytovateli služby informování o účtu, plátci, příjemci a dalšími poskytovateli platebních služeb.

Zúčtování: proces přenosu, párování a v některých případech potvrzení příkazů k převodům před vypořádáním, včetně započtení příkazů a stanovení konečných pozic pro vypořádání.

Přímé vypořádání: dokončení transakce nebo zpracování, jehož cílem je splnění závazků účastníků převodem peněžních prostředků, jestliže tento úkon provádí sám dotčený poskytovatel platebních služeb.

Nepřímé vypořádání: dokončení transakce nebo zpracování, jehož cílem je splnění závazků účastníků převodem peněžních prostředků, jestliže tento úkon provádí jiný poskytovatel platebních služeb jménem dotčeného poskytovatele platebních služeb.

Jiné: dotčenou funkční oblastí není žádná z výše uvedených možností. Další podrobnosti se uvedou ve volném textovém poli.

Dotčené systémy a složky: uveďte, která část nebo části technologické infrastruktury

poskytovatele platebních služeb byly incidentem dotčeny. Je možné zaškrtnout více políček.

Aplikace/software: programy, operační systémy atd., které podporují poskytování platebních služeb poskytovatelem platebních služeb.

Databáze: datová struktura, která uchovává osobní a platební údaje potřebné k provádění platebních transakcí.

Hardware: fyzické technologické zařízení, na kterém běží procesy a/nebo které uchovává údaje potřebné k tomu, aby poskytovatelé platebních služeb mohli vykonávat svoji činnost související s platbami.

Síť/infrastruktura: veřejné nebo soukromé telekomunikační sítě, které umožňují výměnu údajů a informací během platebního procesu (např. internet).

Jiné: dotčeným systémem a složkou není žádná z výše uvedených možností. Další podrobnosti se uvedou ve volném textovém poli.

Dotčení pracovníci: uveďte, zda incident ovlivnil pracovníky poskytovatele platebních služeb, a pokud ano, uveďte ve volném textovém poli bližší informace.

B 5 – Zmírnění incidentu

Jaká opatření byla doposud přijata nebo jsou plánována s cílem dosáhnout obnovy v případě incidentu?: uveďte podrobné informace o opatřeních, která byla přijata nebo jsou plánována s cílem incident dočasně řešit.

Došlo k aktivaci plánů zachování provozu a/nebo plánů obnovy činnosti po havárii?: uveďte, zda ano či ne, a pokud ano, uveďte nejdůležitější informace o tom, co se stalo (tj. kdy došlo k jejich aktivaci a co bylo náplní těchto plánů).

Zrušil nebo oslabil poskytovatel platebních služeb v důsledku incidentu některé kontroly?: uveďte, zda poskytovatel platebních služeb musel zrušit některé kontroly (např. přestal používat princip čtyř očí) s cílem řešit incident, a pokud ano, pak uveďte bližší informace o souvisejících důvodech pro oslabení nebo zrušení kontrol.

C – Závěrečná zpráva

C 1 – Obecné údaje

Aktualizace informací z průběžné zprávy (shrnutí): uveďte další informace o opatřeních přijatých za účelem obnovy v případě incidentu a s cílem zabránit opakování incidentu, analýzu příčin, získané zkušenosti atd.

Datum a čas uzavření incidentu: uveďte datum a čas, kdy byl incident považován za uzavřený.

Jsou opět zavedeny původní kontroly?: jestliže poskytovatel platebních služeb musel kvůli incidentu zrušit nebo oslabit některé kontroly, uveďte, zda byly tyto kontroly opět zavedeny, a doplňte další informace ve volném textovém poli.

C 2 – Analýza příčin a následná opatření

Co bylo příčinou, je-li již příčina známa?: vysvětlete, co je příčinou incidentu nebo v případě, že příčina ještě není známa, předběžné závěry vyplývající z analýzy příčin. Poskytovatelé platebních služeb mohou v případě potřeby přiložit soubor s podrobnými informacemi.

Hlavní nápravná opatření přijatá nebo plánovaná s cílem zabránit opakování incidentu v budoucnu, pokud jsou již tato opatření známa: popište hlavní opatření, která byla přijata nebo jsou plánována s cílem zabránit budoucímu opakování incidentu.

C 3 – Doplňující informace

Byli o incidentu informováni další poskytovatelé platebních služeb?: uveďte přehled

poskytovatelů platebních služeb, kteří byli formálně či neformálně kontaktováni s cílem informovat je o incidentu, a uveďte bližší údaje o poskytovatelích platebních služeb, kteří byli informováni, o poskytnutých informacích a souvisejících důvodech pro poskytnutí těchto informací.

Byly proti poskytovateli platebních služeb učiněny nějaké právní kroky?: uveďte, zda do doby vyplnění závěrečné zprávy byly proti poskytovateli platebních služeb v důsledku incidentu podniknuty nějaké právní kroky (např. podání žaloby u soudu nebo odebrání licence).