EBA/GL/2021/03

10. června 2021

# Revidované obecné pokyny

# k oznamování významných incidentů podle směrnice PSD2

# 1. Soulad a oznamovací povinnost

## Status těchto obecných pokynů

1. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení o orgánu EBA[1]. V souladu s čl. 16 odst. 3 nařízení o orgánu EBA musí příslušné orgány a finanční instituce vynaložit 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 bodu 2 nařízení o orgánu EBA, na které se tyto obecné pokyny vztahují, by se jimi měly řídit a začlenit je do svých postupů (např. pozměněním svého 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 o orgánu EBA musí příslušné orgány do (07.11.2021) 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 předložena na formuláři, který je k dispozici na internetových stránkách orgánu EBA, s označením „EBA/GL/2021/03“. Oznámení by měly předložit osoby s příslušným oprávněním oznamovat, zda se jejich příslušné orgány těmito obecnými pokyny řídí nebo hodlají řídit. Jakoukoli změnu stavu dodržování obecných 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, oblast působnosti a definice

## Předmět

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

6. Tyto obecné pokyny zejména blíže vymezují kritéria pro klasifikaci významných operačních a bezpečnostních incidentů poskytovateli platebních služeb, jakož i formát a postupy, které by měli dodržovat při oznamování těchto incidentů příslušnému orgánu v domovském členském státě podle čl. 96 odst. 1 směrnice PSD2.

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, kterou budou podle čl. 96 odst. 2 směrnice PSD2 sdílet s ostatními vnitrostátními orgány.

8. Tyto obecné pokyny se rovněž zabývají sdílením příslušných podrobných informací o oznámených incidentech s orgánem EBA a Evropskou centrální bankou (ECB) s cílem podpořit společný a jednotný přístup.

## Oblast působnosti

9. Tyto obecné pokyny se použijí v souvislosti s klasifikací a oznamováním významných operačních nebo bezpečnostních incidentů podle článku 96 směrnice PSD2.

10. Tyto obecné pokyny se vztahují na všechny incidenty zahrnuté 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 nebo v dceřiné společnosti usazené mimo Unii) a přímo (dotčená společnost se sídlem mimo Unii provádí službu související s platbami) nebo nepřímo (v důsledku incidentu je jiným způsobem ohrožena způsobilost poskytovatele platebních služeb vykonávat jeho platební činnost) ovlivní platební služby poskytované poskytovatelem platebních služeb se sídlem v Unii.

12. Tyto obecné pokyny se vztahují také na významné incidenty ovlivňující funkce při externím zajišťování služeb nebo činností (outsourcing) poskytovatelem platebních služeb třetím stranám.

## Adresáti

13. První soubor obecných pokynů (oddíl 4) je určen poskytovatelům platebních služeb vymezeným v čl. 4 bodu 11 směrnice PSD2 a uvedeným v čl. 4 bodu 1 nařízení (EU) č. 1093/2010.

14. Druhý a třetí soubor obecných pokynů (oddíly 5 a 6) je určen příslušným orgánům ve smyslu čl. 4 bodu 2 podbodu i) nařízení (EU) č. 1093/2010.

## Definice

15. Není-li stanoveno jinak, mají pojmy v těchto obecných pokynech stejný význam jako pojmy používané a vymezené ve směrnici PSD2. Kromě toho se pro účely těchto obecných pokynů použijí 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 a/nebo autenticitu služeb souvisejících s platbami |
| integrita | zajištění správnosti a úplnosti aktiv (včetně údajů) |
| dostupnost | vlastnost služeb souvisejících s platbami spočívající v tom, že jsou plně přístupné a použitelné uživateli platebních služeb podle přijatelných úrovní předem stanovených poskytovatelem platebních služeb |
| důvěrnost | skutečnost, že se informace nezpřístupňují ani nesdělují neoprávněným osobám či subjektům nebo pro neautorizované účely |
| autenticita | vlastnost zajišťující, že zdroj je tím, za co se vydává |
| služby související s platbami | Jakákoliv podnikatelská (obchodní) činnost ve smyslu čl. 4 bodu 3 směrnice PSD2 a všechny technické podpůrné úkoly nezbytné pro správné poskytování platebních služeb |

# 3. Provádění

## Datum použití

16. Tyto obecné pokyny se použijí ode dne 1. ledna 2022.

## Zrušení

17. S účinností od 1. ledna 2022 se zrušují tyto obecné pokyny:

*Obecné pokyny k oznamování významných incidentů podle směrnice (EU) 2015/2366 (PSD2) (EBA/GL/2017/10).*

# 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“

vymezených v obecném pokynu 1.4 a na základě posouzení stanoveného v těchto obecných pokynech.

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

*i. Dotčené transakce*

Poskytovatelé platebních služeb by měli určit celkovou hodnotu dotčených transakcí i počet ohrožených plateb vyjádřený jako procentní 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 procentní podíl z celkového počtu uživatelů platebních služeb.

*iii. Narušení zabezpečení sítě nebo informačních systémů*

Poskytovatelé platebních služeb by měli určit, zda nějaká škodlivá činnost neohrozila zabezpečení sítě nebo informačních systémů souvisejících s poskytováním platebních služeb.

*iv. Délka výpadku služby*

Poskytovatelé platebních služeb by měli určit dobu, po kterou bude služba uživateli platební služby pravděpodobně nedostupná nebo po kterou nemůže poskytovatel platebních služeb splnit platební příkaz ve smyslu čl. 4 bodu 13 směrnice PSD2.

*v. 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).

*vi. Vysoká úroveň interní eskalace*

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

*vii. 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 platební schémata.

*viii. 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 vypočítat hodnotu ukazatelů pomocí této 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 peněžní prostředky byly či nebyly získány zpět), nebo tam, kde incident jinak brání nebo zamezuje řádnému provedení.

U operačních incidentů ovlivňujících schopnost iniciovat a/nebo zpracovávat transakce by poskytovatelé platebních služeb měli hlásit pouze incidenty trvající déle než jednu hodinu. Doba trvání incidentu by měla být měřena od okamžiku, kdy k incidentu dojde, do okamžiku, kdy jsou obnoveny běžné činnosti/operace na takovou úroveň služby, na které byla poskytována před incidentem.

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 pro výpočet. V případě, že poskytovatelé platebních služeb tento údaj nepovažují za vypovídající (např. kvůli sezónnosti), měli by místo toho použít jinou, více vypovídající metriku a sdělit příslušnému orgánu odpovídající odůvodnění tohoto přístupu v příslušném poli formuláře (viz příloha).

*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. Pro určení počtu uživatelů platebních služeb, kteří by bývali mohli platební službu využívat během trvání incidentu, by poskytovatelé platebních služeb měli použít odhady vycházející z dřívější činnosti.

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 dotčený 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.

U operačních incidentů ovlivňujících schopnost iniciovat nebo zpracovávat transakce by poskytovatelé platebních služeb měli hlásit pouze incidenty, které mají dopad na uživatele platebních služeb a trvají déle než jednu hodinu. Doba trvání incidentu by měla být měřena od okamžiku, kdy k incidentu dojde, do okamžiku, kdy jsou obnoveny běžné činnosti/operace na takovou úroveň služby, na které byla poskytována před incidentem.

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 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. Narušení zabezpečení sítě nebo informačních systémů*

Poskytovatelé platebních služeb by měli určit, zda nějaká škodlivá činnost neohrozila dostupnost, autenticitu, integritu nebo důvěrnost sítě nebo informačních systémů (včetně dat) souvisejících s poskytováním platebních služeb.

*iv. Délka výpadku služby*

Poskytovatelé platebních služeb by měli zohlednit dobu, po kterou trvá nebo pravděpodobně bude trvat výpadek jakékoliv úkolu, procesu nebo kanálu vztahujícího se k poskytování platebních služeb, který tudíž znemožňuje i) iniciování a/nebo provedení platební služby nebo ii) přístup k platebnímu účtu. Poskytovatelé platebních služeb by měli určit délku výpadku služby od okamžiku, kdy výpadek začne, přičemž by měli 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 určit délku výpadku služby od okamžiku, kdy byl výpadek zjištěn.

v. *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 peněžní prostředky nebo aktiva, náklady na výměnu hardwaru nebo softwaru, další náklady na forenzní analýzy nebo náklady na nápravu škod, poplatky v důsledku nedodržení smluvních závazků, 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.

vi. *Vysoká úroveň interní eskalace*

Poskytovatelé platebních služeb by měli zvážit, zda v důsledku dopadu na služby související s platbami byl nebo pravděpodobně bude vedoucí orgán, jak je definován v obecných pokynech orgánu EBA pro řízení rizik v oblasti IKT a bezpečnosti, informován o incidentu v souladu s obecným pokynem 60 písm. d) obecných pokynů orgánu EBA pro řízení rizik v oblasti IKT a bezpečnosti mimo jakýkoli postup pravidelného oznamování a průběžně po celou dobu trvání incidentu. Dále by poskytovatelé platebních služeb měli zohlednit, zda v důsledku dopadu incidentu na služby související s platbami byl nebo pravděpodobně bude vyhlášen krizový režim.

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

Poskytovatelé platebních služeb by měli posoudit dopad incidentu na finanční trh, kterým se rozumí infrastruktury finančního trhu a/nebo platební schémata, která jej podporují , a na ostatní poskytovatele platebních služeb. Poskytovatelé platebních služeb by měli zejména posoudit, zda se incident projevil nebo se pravděpodobně projeví u jiných poskytovatelů platebních služeb, zda ovlivnil nebo pravděpodobně ovlivní hladké fungování infrastruktur finančního trhu a zda ohrozil nebo pravděpodobně ohrozí řádné fungování finančního systému jako celku. Poskytovatelé platebních služeb by měli zohlednit různé aspekty, například to, zda je dotčená složka / dotčený software soukromý nebo všeobecně dostupný, 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.

viii. *Dopad na dobrou pověst*

Poskytovatelé platebních služeb by měli zvážit úroveň viditelnosti, které incident podle jejich nejlepšího vědomí na trhu dosáhl nebo pravděpodobně dosáhne. Poskytovatelé platebních služeb by měli zvážit zejména pravděpodobnost, že incident způsobí společnosti škodu, což je dobrý ukazatel jeho potenciálního dopadu na jejich pověst. Poskytovatelé platebních služeb by měli vzít v úvahu, zda i) si uživatelé platebních služeb nebo jiní

poskytovatelé platebních služeb stěžovali na nepříznivý dopad incidentu; ii) incident ovlivnil viditelný proces související s platební službou, a je tedy pravděpodobné, že se mu dostane nebo se mu již dostalo mediálního pokrytí (s přihlédnutím nejen k tradičním sdělovacím prostředkům, jako jsou noviny, ale také k blogům, sociálním sítím atd.); iii) došlo nebo pravděpodobně dojde k nedodržení smluvních závazků, což má za následek zveřejnění právních kroků vůči poskytovateli platebních služeb; iv) nebyly dodrženy požadavky regulace, což má za následek uložení dohledových opatřen nebo sankcí, které byly nebo pravděpodobně budou zveřejněny; a v) k podobnému 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 č. 1.

Tabulka č. 1: Prahové hodnoty

| Kritérium | Nižší úroveň dopadu | Vyšší úroveň dopadu |
|---|---|---|
| Dotčené transakce | > 10 % běžné úrovně transakcí dotčeného poskytovatele platebních služeb (z hlediska počtu transakcí)<br>**a**<br>doba trvání incidentu > 1 hodina*<br><br>**nebo**<br><br>> 500 000 EUR<br>**a**<br>doba trvání incidentu > 1 hodina* | > 25% běžné úrovně transakcí dotčeného poskytovatele platebních služeb (z hlediska počtu transakcí)<br><br>**nebo**<br><br>> 15 000 000 EUR |
| Dotčení uživatelé platebních služeb | > 5 000<br>**a**<br>doba trvání incidentu > 1 hodina*<br><br>**nebo**<br><br>> 10 % uživatelů platebních služeb dotčeného poskytovatele platebních služeb<br>**a**<br>doba trvání incidentu > 1 hodina* | > 50 000<br><br>**nebo**<br><br>> 25% uživatelů platebních služeb dotčeného poskytovatele platebních služeb |
| Délka výpadku služby | > 2 hodiny | neuplatňuje se |
| Narušení zabezpečení sítě nebo informačních systémů | ano | neuplatňuje se |
| Ekonomický dopad | neuplatňuje se | > max. (0,1 % kapitálu tier 1**, 200 000 EUR)<br>**nebo**<br>> 5 000 000 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 | neuplatňuje se |
| Dopad na dobrou pověst | ano | neuplatňuje se |

* Prahová hodnota týkající se doby trvání incidentu po dobu delší než jedna hodina se vztahuje pouze na operační incidenty, které ovlivňují schopnost poskytovatele platebních služeb iniciovat a/nebo zpracovávat transakce.

**Kapitál tier 1 ve smyslu 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 použít odhady, pokud nemají k dispozici skutečné údaje, které by podpořily jejich úsudek o tom, zda je nebo pravděpodobně bude dosaženo dané prahové hodnoty před vyřešením incidentu (např. k tomu může dojít ve fázi počátečního šetření).

1.6. Poskytovatelé platebních služeb by měli toto hodnocení 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). Jakákoli změna klasifikace incidentu z významného na nevýznamný by měla být sdělena příslušnému orgánu v souladu s požadavkem obecného pokynu 2.21 a bez zbytečného odkladu.

## Obecný pokyn 2: Postup oznamování

2.1. Poskytovatelé platebních služeb by měli shromáždit všechny relevantní informace, vypracovat zprávu o incidentu vyplněním formuláře uvedeného v příloze a zprávu předložit příslušnému orgánu v domovském členském státě. Poskytovatelé platebních služeb by měli všechna pole formuláře vyplnit podle instrukcí uvedených v příloze.

2.2. Poskytovatelé platebních služeb by měli při předkládání úvodních, průběžných a závěrečných zpráv týkajících se stejného incidentu používat stejný formulář. Poskytovatelé platebních služeb by proto měli postupně vyplňovat pouze jeden formulář a v případě potřeby aktualizovat informace poskytnuté v předchozích zprávách.

2.3. Poskytovatelé platebních služeb by případně měli příslušnému orgánu ve svém domovském členském státě dále předložit kopii informací, které byly (nebo budou) poskytnuty uživatelům v souladu s čl. 96 odst. 1 druhým pododstavcem směrnice PSD2, a to jakmile budou tyto informace k dispozici.

2.4. Poskytovatelé platebních služeb by měli na žádost příslušného orgánu v domovském členském státě poskytnout jakékoli další dokumenty, které doplňují informace předložené ve standardizovaném formuláři. Poskytovatelé platebních služeb by měli odpovědět na

případné žádosti od příslušného orgánu v domovském členském státě o poskytnutí dalších informací nebo objasnění již předložené dokumentace.

2.5. Veškeré další informace obsažené v dokumentech, které poskytovatelé platebních služeb poskytli příslušnému orgánu, a to buď z podnětu poskytovatele platebních služeb, nebo na žádost příslušného orgánu v souladu s obecným pokynem 2.4, by měl poskytovatel platebních služeb zohlednit ve formuláři podle obecného pokynu 2.1.

2.6. Poskytovatelé platebních služeb by měli vždy zachovávat důvěrnost a integritu vyměňovaných informací a řádně prokazovat svou totožnost příslušnému orgánu v jejich domovském členském státě.

## Úvodní zpráva

2.7. Poskytovatelé platebních služeb by měli příslušnému orgánu v domovském členském státě poté, co byl významný operační nebo bezpečnostní incident klasifikován jako významný, předložit úvodní zprávu. Příslušné orgány by měly bez zbytečného odkladu potvrdit přijetí úvodní zprávy a přidělit incidentu jedinečný referenční kód, který jej jednoznačně identifikuje. Poskytovatelé platebních služeb by měli tento referenční kód uvádět při předkládání aktualizací k úvodní zprávě, nebo při předkládání průběžných a závěrečných zpráv týkajících se téhož incidentu, pokud nejsou průběžné a závěrečné zprávy předloženy společně s úvodní zprávou.

2.8. Poskytovatelé platebních služeb by měli příslušnému orgánu zaslat úvodní zprávu do čtyř hodin od okamžiku, kdy byl operační nebo bezpečnostní incident klasifikován jako významný. Pokud je známo, že kanály příslušného orgánu pro oznamování nejsou v té době dostupné nebo funkční, měli by poskytovatelé platebních služeb zaslat úvodní zprávu, jakmile budou opět dostupné/funkční.

2.9. Poskytovatelé platebních služeb by měli incident klasifikovat v souladu s obecnými pokyny 1.1 a 1.4 včas po zjištění incidentu, nejpozději však do 24 hodin po jeho zjištění, a bez zbytečného odkladu poté, co má poskytovatel platebních služeb k dispozici informace potřebné ke klasifikaci incidentu . Pokud je ke klasifikaci incidentu zapotřebí delší doba, měli by poskytovatelé platebních služeb v úvodní zprávě předložené příslušnému orgánu vysvětlit důvody.

2.10. Poskytovatelé platebních služeb by měli úvodní zprávu předložit také příslušnému orgánu v domovském členském státě v okamžiku, kdy je klasifikace incidentu změněna z nevýznamného incidentu na 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 příslušného orgánu pro oznamování nejsou v té době dostupné nebo funkční, jakmile budou tyto kanály opět dostupné nebo funkční.

2.11. Poskytovatelé platebních služeb by měli ve svých úvodních zprávách (tj. v oddíle A formuláře) poskytnout informace z nadpisu, a to včetně základní charakteristiky incidentu

a jeho předpokládaných důsledků na základě informací dostupných okamžitě poté, co byl incident klasifikován jako významný. V případě, že skutečné údaje nejsou k dispozici, měli by poskytovatelé platebních služeb použít odhady.

### Průběžná zpráva

2.12. Poskytovatelé platebních služeb by měli předložit průběžnou zprávu po obnovení běžné činnosti a návratu k normálnímu provozu a příslušný orgán o této skutečnosti informovat. Poskytovatelé platebních služeb by měli za návrat k normálnímu provozu považovat situaci, kdy se činnost/provoz navrátí na stejnou úroveň služeb/podmínek, která je stanovena poskytovatelem platebních služeb nebo vymezena externě dohodou o úrovni služeb z hlediska doby zpracování, kapacity, bezpečnostních požadavků atd., a kdy již nejsou zavedena opatření pro nepředvídané události. Průběžná zpráva by měla obsahovat podrobnější popis incidentu a jeho následků (oddíl B formuláře).

2.13. Pokud dosud nedošlo k obnovení běžných činností, měli by poskytovatelé platebních služeb předložit příslušnému orgánu průběžnou zprávu do tří pracovních dnů od předložení úvodní zprávy.

2.14. Poskytovatelé platebních služeb by měli aktualizovat informace již poskytnuté v oddílech A a B formuláře, pokud od předložení předchozí zprávy zjistí nové významné změny (např. zda došlo k eskalaci nebo ke zmírnění incidentu, nově zjištěné příčiny nebo opatření přijatá k vyřešení problému). To zahrnuje i případ, kdy incident nebyl vyřešen do tří pracovních dnů, což by vyžadovalo, aby poskytovatelé platebních služeb předložili další průběžnou zprávu. Poskytovatelé platebních služeb by každopádně měli další průběžnou zprávu předložit na žádost příslušného orgánu v domovském členském státě.

2.15. Stejně jako v případě počátečních zpráv, pokud nejsou k dispozici skutečné údaje, měli by poskytovatelé platebních služeb použít odhady.

2.16. Jestliže dojde k návratu k normálnímu provozu do čtyř hodin od okamžiku, kdy byl incident klasifikován jako významný, poskytovatelé platebních služeb by měli usilovat o současné předložení úvodní i průběžné zprávy (tj. vyplnit oddíly A a B formuláře) během uvedené čtyřhodinové lhůty.

### Závěrečná zpráva

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

2.18. Poskytovatelé platebních služeb by měli závěrečnou zprávu předložit příslušnému orgánu maximálně do dvaceti pracovních dnů od návratu k normálnímu provozu. Poskytovatelé platebních služeb, kteří potřebují tuto lhůtu prodloužit (např. v případě, že ještě nejsou

k dispozici skutečné údaje o dopadu nebo zatím nebyly zjištěny hlavní příčiny), by měli kontaktovat příslušný orgán před uplynutím této lhůty a sdělit mu odpovídající důvody zpoždění, jakož i nové předpokládané datum předložení závěrečné zprávy.

2.19. Jsou-li poskytovatelé platebních služeb schopni poskytnout veškeré informace vyžadované v závěrečné zprávě (tj. v oddíle C formuláře) během uvedené čtyřhodinové lhůty poté, co byl incident klasifikován jako významný, měli by usilovat o předložení informací vztahujících se k úvodní, průběžné a závěrečné zprávě najednou.

2.20. Poskytovatelé platebních služeb by měli v závěrečné zprávě uvést úplné informace, tj. i) skutečné údaje o dopadu namísto odhadů (jakož i případné další potřebné aktualizace v oddílech A a B formuláře) a ii) oddíl C formuláře, který uvádí hlavní příčinu, pokud je již známa, a shrnutí opatření přijatých nebo plánovaných k odstranění problému a zabránění jeho opakovaní v budoucnu.

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

## Obecný pokyn 3: Delegované a konsolidované oznamování

3.1. Jestliže to příslušný orgán povolí, poskytovatelé platebních služeb, kteří chtějí delegovat oznamovací povinnosti podle směrnice PSD2 na třetí stranu, by měli informovat příslušný orgán v domovském členském státě a zajistit splnění těchto podmínek:

a. Formální smlouva nebo případně stávající interní ujednání v rámci skupiny, které upravují oznamování delegované poskytovatelem platebních služeb na třetí stranu, jednoznačně vymezují rozdělení povinností všech stran. Zejména jasně stanoví, že bez ohledu na možné delegování oznamovací povinnosti dotčený poskytovatel platebních služeb zůstává plně odpovědný za splnění požadavků stanovených v článku 96 směrnice PSD2 a za obsah informací poskytnutých příslušnému orgánu v domovském členském státě.

b. Delegování oznamovací povinnosti splňuje požadavky na outsourcing důležitých provozních funkcí stanovených v:

i. čl. 19 odst. 6 směrnice PSD2 ve vztahu k platebním institucím a institucím elektronických peněz, které se použijí obdobně v souladu s článkem 3 směrnice 2009/110/ES; nebo v

ii. obecných pokynech orgánu EBA k outsourcingu (EBA/GL/2019/02) ve vztahu ke všem poskytovatelům platebních služeb.

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

d. Je řádně zajištěna důvěrnost citlivých údajů a kvalita, konzistentnost, 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 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 těchto podmínek:

a. zahrnout toto ustanovení do smlouvy, na jejímž základě dochází k delegování oznamování;

b. podmínit konsolidované oznamování tím, že incident je způsoben narušením služeb poskytovaných třetí stranou;

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

d. uvést seznam všech poskytovatelů platebních služeb, kterých se incident týká;

e. zajistit, aby třetí strana posoudila významnost incidentu u každého dotčeného poskytovatele platebních služeb a do konsolidované zprávy zahrnula pouze ty poskytovatele platebních služeb, u nichž je incident klasifikován jako významný; a zajistit, aby v případě pochybností byl do konsolidované zprávy poskytovatel platebních služeb zahrnut, pokud neexistují důkazy potvrzující opak;

f. zajistit, aby v případě, že formulář obsahuje pole, u nichž není možná společná odpověď (např. oddíly B2, B4 nebo C3 formuláře), třetí strana buď i) vyplnila pole pro každého poskytovatele platebních služeb zvlášť, přičemž dále uvedla totožnost každého poskytovatele platebních služeb, kterého se informace týkají; nebo ii) použila kumulativní hodnoty zjištěné nebo odhadované pro poskytovatele platebních služeb;

g. třetí strana musí za všech okolností informovat poskytovatele platebních služeb o všech relevantních informacích týkajících se incidentu a veškerých interakcích, které mohou mít s příslušným orgánem, a o obsahu incidentu, avšak pouze

v takovém rozsahu, aby nedošlo k porušení důvěrnosti, pokud jde o informace, které se týkají jiných poskytovatelů platebních služeb.

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

3.4. Poskytovatelé platebních služeb, kteří mají v úmyslu odvolat delegování oznamovací povinnosti, by měli toto rozhodnutí sdělit příslušnému orgánu v domovském členském státě v souladu s lhůtami a postupy jím stanovenými. Poskytovatelé platebních služeb by měli příslušný orgán v domovském členském státě rovněž informovat o jakémkoli podstatném vývoji, který má vliv na určenou třetí stranu a její schopnost plnit oznamovací povinnost.

3.5. Jestliže určená třetí strana neinformovala příslušný orgán v domovském členském státě o významném operačním nebo bezpečnostním incidentu v souladu s článkem 96 směrnice PSD2 a s těmito obecnými pokyny, měli by poskytovatelé platebních služeb věcně splnit svoji oznamovací povinnost bez vnější pomoci. Poskytovatelé platebních služeb by měli rovněž zajistit, aby incident nebyl oznámen dvakrát, a to individuálně dotčeným poskytovatelem platebních služeb a ještě jednou touto třetí stranou.

3.6. Poskytovatelé platebních služeb by měli zajistit, aby v situaci, kdy je incident způsoben narušením služeb zajišťovaných poskytovatelem technických služeb (nebo infrastrukturou), které má dopad na více poskytovatelů platebních služeb, odkazovalo delegované oznamování na jednotlivé údaje konkrétního poskytovatele platebních služeb (s výjimkou konsolidovaného oznamování).

## 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 PSD2, jakož i procesy zavedené s cílem splnit požadavky uvedené v těchto obecných pokynech.

# 5. Obecné pokyny určené příslušným orgánům týkající se kritérií pro posuzování závažnosti incidentu a podrobných informací uvedených ve zprávách o incidentech poskytovaných ostatním 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 ostatní vnitrostátní orgány na základě vlastního odborného posouzení a s použitím těchto kritérií, které slouží jako primární ukazatele významnosti uvedeného incidentu:

a. Příčiny incidentu spadají do regulační kompetence 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 ovlivnit uživatele platebních služeb ve velkém rozsahu.
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 ostatními vnitrostátními orgány, by příslušné orgány měly poskytnout informace o významných operačních nebo bezpečnostních incidentech alespoň relevantním vnitrostátním orgánům určeným na základě obecného pokynu 5.1, a to po obdržení úvodní zprávy (nebo případné zprávy, která dala podnět ke sdílení informací) a poté, kdy jsou informovány o tom, že došlo k návratu k normálnímu provozu (tj. v průběžné zprávě).

6.2. Příslušné orgány by měly relevantním vnitrostátním orgánům předložit informace potřebné k tomu, aby si vytvořily jasnou představu o tom, co se stalo, a o možných důsledcích. Za

tímto účelem by měly poskytnout alespoň informace uvedené poskytovatelem platebních služeb v těchto polích formuláře (v úvodní nebo průběžné zprávě):

- datum a čas klasifikace incidentu jako významného,
- 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 se incident mohl dotknout jiných poskytovatelů platebních služeb a/nebo infrastruktur,
- popis (případného) mediálního pokrytí,
- příčina incidentu.

6.3. Před poskytnutím informací vztahujících se k incidentu relevantním 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 relevantním vnitrostátním orgánům sdělit název a adresu poskytovatele platebních služeb, který oznámení učinil, pokud dotčené vnitrostátní orgány mohou zaručit, že s informacemi bude nakládáno jako s důvěrnými.

6.4. Příslušné orgány by měly vždy zachovávat důvěrnost a integritu uchovávaných a vyměňovaných informací a rovněž řádně prokazovat svou totožnost relevantním vnitrostátním orgánům. 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 služební tajemství, která je vymezena ve směrnici PSD2.

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

## 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 prostřednictvím standardizovaného souboru dostupného na internetových stránkách orgánu EBA.

## Obecný pokyn 8: Komunikace

8.1. Příslušné orgány by měly vždy zachovávat důvěrnost a integritu uchovávaných a vyměňovaných informací a rovněž řádně prokazovat svou totožnost orgánu EBA a ECB. Aniž by bylo dotčeno platné právo Unie a vnitrostátní požadavky, příslušné orgány by měly se všemi informacemi obdrženými na základě těchto obecných pokynů zacházet zejména v souladu s povinností zachovat služební tajemství, která je vymezena ve směrnici PSD2.

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

# Příloha – Formuláře pro účely oznamování určené poskytovatelům platebních služeb

## Úvodní zpráva

| Úvodní zpráva | do 4 hodin od klasifikace incidentu jako významného | Resetovat výběry v rozbalovacích nabídkách |
|---|---|---|
| Datum zprávy (*DD/MM/RRRR*) | | Čas (*HH:MM*) |
| **Referenční kód incidentu** | | |

| **A – Úvodní zpráva** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **A 1 – OBECNÉ ÚDAJE** | | | | | | | | | | | |
| **Druh zprávy** | | | | | | | | | | | |
| Druh zprávy | | | | | | | | | | | |
| **Dotčený poskytovatel platebních služeb** | | | | | | | | | | | |
| Název poskytovatele platebních služeb | | | | | | | | | | | |
| Vnitrostátní identifikační číslo poskytovatele platebních služeb | | | | | | | | | | | |
| Případný vedoucí skupiny | | | | | | | | | | | |
| Země dotčené incidentem | ☐ AT | ☐ DE | ☐ FR | ☐ IE | ☐ LV | ☐ PT | | | | | |
| | ☐ BE | ☐ DK | ☐ LI | ☐ IS | ☐ MT | ☐ RO | | | | | |
| | ☐ BG | ☐ EE | ☐ GR | ☐ IT | ☐ NL | ☐ SE | | | | | |
| | ☐ CY | ☐ ES | ☐ HR | ☐ LT | ☐ NO | ☐ SI | | | | | |
| | ☐ CZ | ☐ FI | ☐ HU | ☐ LU | ☐ PL | ☐ SK | | | | | |
| Hlavní kontaktní osoba | | | | E-mail | | | Telefon | | | | |
| Další kontaktní osoba | | | | E-mail | | | Telefon | | | | |
| **Oznamující subjekt (tento oddíl se vyplní v případě delegovaného oznamování, jestliže oznamujícím subjektem není dotčený poskytovatel platebních služeb)** | | | | | | | | | | | |
| Název oznamujícího subjektu | | | | | | | | | | | |
| Vnitrostátní identifikační číslo | | | | | | | | | | | |
| Hlavní kontaktní osoba | | | | E-mail | | | Telefon | | | | |
| Další kontaktní osoba | | | | E-mail | | | Telefon | | | | |
| **A 2 – ZJIŠTĚNÍ A KLASIFIKACE INCIDENTU** | | | | | | | | | | | |
| Datum a čas zjištění incidentu (*DD/MM/RRRR HH:MM*) | | | | | | | | | | | |
| Datum a čas klasifikace incidentu (*DD/MM/RRRR HH:MM*) | | | | | | | | | | | |
| Kdo incident zjistil | | | | Je-li zvoleno „Jiné", upřesněte: | | | | | | | |
| Druh incidentu | | | | | | | | | | | |
| Kritéria vedoucí ke zprávě o významném incidentu | ☐ Dotčené transakce | ☐ Dotčení uživatelé platebních služeb | ☐ Délka výpadku služby | ☐ Narušení zabezpečení sítě nebo informačních systémů | ☐ Ekonomický dopad | ☐ Vysoká úroveň interní eskalace | ☐ Ostatní potenciálně dotčení poskytovatelé platebních služeb nebo příslušné infrastruktury | ☐ Dopad na dobrou pověst | | | |
| Stručný a obecný popis incidentu | | | | | | | | | | | |
| Případný dopad v jiných členských státech EU | | | | | | | | | | | |
| Oznamování jiným orgánům | | | | Je-li zvoleno „Ano", upřesněte: | | | | | | | |
| Důvody pro pozdní předložení úvodní zprávy | | | | | | | | | | | |

## Průběžná zpráva

**Zpráva o významném incidentu**

| Průběžná zpráva | maximálně tři pracovní dny od předložení úvodní zprávy | Resetovat výběry v rozbalovacích nabídkách |
|---|---|---|

Datum zprávy (*DD/MM/RRRR*) | Čas (*HH:MM*)

**Referenční kód incidentu**

**B – Průběžná zpráva**

**B 1 – OBECNÉ ÚDAJE**

| **Podrobnější popis incidentu:** | |
|---|---|
| V čem je konkrétně problém? | |
| Jak incident začal? | |
| Jak se vyvíjel? | |
| Jaké má důsledky (zejména pro uživatele platebních služeb)? | |
| Byli o incidentu informováni uživatelé platebních služeb? | Je-li zvoleno „Ano", upřesněte: |
| Souvisí incident s předchozími incidenty? | Je-li zvoleno „Ano", upřesněte: |
| Byli dotčeni nebo zapojeni další poskytovatelé služeb či třetí strany? | Je-li zvoleno „Ano", upřesněte: |
| Bylo zahájeno krizové řízení (interní a/nebo externí)? | Je-li zvoleno „Ano", upřesněte: |
| Datum a čas vzniku incidentu (je-li již informace k dispozici) *(DD/MM/RRRR HH:MM)* | |
| Datum a čas, kdy došlo nebo podle očekávání dojde k návratu do původního stavu *(DD/MM/RRRR HH:MM)* | |
| Dotčené funkční oblasti | ☐ Ověření/autorizace ☐ Přímé vypořádání ☐ Komunikace ☐ Nepřímé vypořádání ☐ Zúčtování ☐ Jiné — Je-li zvoleno „Jiné", upřesněte: |
| Změny oproti předchozím zprávám | |

**B 2 – KLASIFIKACE INCIDENTU / INFORMACE O INCIDENTU**

| | |
|---|---|
| Dotčené transakce [2] | Úrovni dopadu<br>Počet dotčených transakcí<br>Jako % z běžného počtu transakcí<br>Hodnota dotčených transakcí v eurech<br>Doba trvání incidentu (pouze pro operační incidenty)<br>Poznámky: |
| Dotčení uživatelé platebních služeb [3] | Úrovni dopadu<br>Počet dotčených uživatelů platebních služeb<br>Jako % z celkového počtu uživatelů platebních služeb |
| Narušení zabezpečení sítě nebo informačních systémů | Popište, jak byla dotčena síť nebo informační systémy |
| Délka výpadku služby | Celková délka výpadku služby: Dny: Hodiny: Minuty: |
| Ekonomický dopad | Úrovni dopadu<br>Přímé náklady v eurech<br>Nepřímé náklady v eurech |
| Vysoká úroveň interní eskalace | Popište úroveň interní eskalace incidentu a uveďte, zda incident vedl nebo pravděpodobně povede k vyhlášení krizového (nebo podobného) režimu, a pokud ano, popište jej |
| Ostatní potenciálně dotčení poskytovatelé platebních služeb nebo příslušné infrastruktury | Popište, jak by se incident mohl dotknout jiných poskytovatelů platebních služeb a/nebo infrastruktur |
| Dopad na dobrou pověst | Popište, jak by incident mohl ovlivnit dobrou pověst poskytovatele platebních služeb (např. mediální pokrytí, zveřejnění právních kroků nebo porušení právních předpisů…) |

**B 3 – POPIS INCIDENTU**

| | |
|---|---|
| Druh incidentu | |
| Příčina incidentu | ☐ Probíhá šetření ☐ Škodlivá činnost ☐ Selhání procesu ☐ Selhání systému ☐ Lidské chyby ☐ Externí události ☐ Jiné — Je-li zvoleno „Jiné", upřesněte: |
| Dotkl se vás incident přímo nebo prostřednictvím poskytovatele služeb? | Pokud „nepřímo", uveďte název poskytovatele služeb: |

**B 4 – DOPAD INCIDENTU**

| | | |
|---|---|---|
| Celkový dopad | ☐ Integrita ☐ Dostupnost | ☐ Důvěrnost ☐ Autenticita |
| Dotčené obchodní kanály | ☐ Pobočky ☐ Elektronické bankovnictví ☐ Elektronické obchodování | ☐ Telefonní bankovnictví ☐ Mobilní bankovnictví ☐ Bankomaty |
| | ☐ Místo prodeje ☐ Jiné | |
| | Je-li zvoleno „Jiné", upřesněte: | |
| Dotčené platební služby | ☐ Vložení hotovosti na platební účet ☐ Výběr hotovosti z platebního účtu ☐ Operace nutné k vedení platebního účtu ☐ Pořizování platebních prostředků | ☐ Úhrady ☐ Inkaso ☐ Platby kartou ☐ Vydávání platebních prostředků |
| | ☐ Poukazování ☐ Služby iniciování ☐ Služby informování o účtu | |

**B 5 – ZMÍRNĚNÍ INCIDENTU**

| | |
|---|---|
| Jaká opatření byla doposud přijata nebo jsou plánována s cílem dosáhnout obnovy po incidentu? | |
| Došlo k aktivaci plánu kontinuity činnosti a/nebo plánu obnovy provozu po havárii? | |
| Pokud ano, kdy? *(DD/MM/RRRR, HH:MM)* | |
| Pokud ano, popište je | |

## Závěrečná zpráva

**Zpráva o významném incidentu**

Zvolte druh zprávy:

maximálně dvacet pracovních dnů od předložení průběžné zprávy

Popište:
(pro incidenty, jejichž klasifikace byla změněna na „nevýznamný")

Resetovat výběry v rozbalovacích nabídkách

Datum zprávy (*DD/MM/RRRR*)
**Referenční kód incidentu**

Čas (*HH:MM*)

**C – Závěrečná zpráva**

*Nebyla-li žádná průběžná zpráva zaslána, vyplňte rovněž oddíl B.*

**C 1 – OBECNÉ ÚDAJE**

| | |
|---|---|
| **Aktualizace informací z úvodní zprávy a z průběžných zpráv** | |
| Změny oproti předchozím zprávám | |
| Jakékoli další relevantní informace | |
| **Jsou zavedeny všechny původní kontroly?** | |
| Je-li zvoleno „Ne", uveďte, o které kontroly jde a jaký čas je zapotřebí k jejich obnovení | |

**C 2 – ANALÝZA HLAVNÍCH PŘÍČIN A NÁSLEDNÁ OPATŘENÍ**

| | | | | | | |
|---|---|---|---|---|---|---|
| Co bylo hlavní příčinou (je-li již známa)? | ☐ Škodlivá činnost | ☐ Selhání procesu | ☐ Selhání systému | ☐ Lidská chyba | ☐ Externí událost | ☐ Jiné |
| Upřesněte: | ☐ Škodlivý kód<br>☐ Shromažďování informací<br>☐ Průniky<br>☐ Útok (distribuovaným) odmítnutím služby<br>☐ Úmyslná interní činnost<br>☐ Úmyslné externí fyzické poškození<br>☐ Zabezpečení informačního obsahu<br>☐ Podvodná činnost<br>☐ Jiné | ☐ Nedostatečné monitorování a kontrola<br>☐ Problémy s komunikací<br>☐ Nesprávné operace<br>☐ Nedostatečné řízení změn<br>☐ Nedostatečnost interních postupů a dokumentace<br>☐ Problémy s obnovou<br>☐ Jiné | ☐ Selhání<br>☐ Selhání sítě<br>☐ Problémy<br>☐ Selhání softwaru/aplikace<br>☐ Fyzické<br>☐ Jiné | ☐ Neúmyslná<br>☐ Nečinnost<br>☐ Nedostatečné zdroje<br>☐ Jiné | ☐ Selhání dodavatele / poskytovatele technických služeb<br>☐ Vyšší moc<br>☐ Jiné | |
| | Je-li zvoleno „Jiné", upřesněte: | | | | | |
| Další relevantní informace o hlavní příčině | | | | | | |
| Hlavní nápravná opatření přijatá nebo plánovaná s cílem zabránit opakování incidentu v budoucnu, pokud jsou již tato opatření známa | | | | | | |

**C 3 – DOPLŇUJÍCÍ INFORMACE**

| | |
|---|---|
| Byli o incidentu informováni další poskytovatelé platebních služeb? | Je-li zvoleno „Ano", uveďte podrobnosti: |
| Byly proti poskytovateli platebních služeb učiněny nějaké právní kroky? | Je-li zvoleno „Ano", uveďte podrobnosti: |
| Posouzení účinnosti přijatých opatření | Uveďte podrobnosti: |

## INSTRUKCE K VYPLNĚNÍ FORMULÁŘE

Poskytovatelé platebních služeb by měli vyplnit příslušný oddíl formuláře v závislosti na fázi oznamování, ve které se nacházejí: oddíl A v případě úvodní zprávy, oddíl B v případě průběžných zpráv a oddíl C v případě závěrečné zprávy. Poskytovatelé platebních služeb by měli při předkládání úvodních, průběžných a závěrečných zpráv týkajících se stejného incidentu používat stejný formulář. Není-li výslovně stanoveno jinak, všechna pole jsou povinná.

### Nadpis

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

**Průběžná zpráva:** Obsahuje podrobnější popis incidentu a jeho následků. Jde o aktualizaci úvodní zprávy (a případně předchozí průběžné zprávy) o stejném incidentu.

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

**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 tuto změnu klasifikace.

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

**Referenční kód incidentu (používá se u průběžných zpráv a závěrečné zprávy i aktualizací úvodní zprávy):** referenční kód vydaný příslušným orgánem při předložení první zprávy sloužící k jednoznačné identifikaci incidentu Každý příslušný orgán by měl jako předponu uvést dvoupísmenný kód ISO[2] svého příslušného členského státu.

## A - Úvodní zpráva

### A 1 - Obecné údaje

**Druh zprávy:**

**Individuální:** Zpráva se týká jediného poskytovatele platebních služeb.

**Konsolidovaná:** Zpráva se týká několika poskytovatelů platebních služeb, kterých se dotýká stejný významný operační nebo bezpečnostní incident a kteří používají konsolidované oznamování, ve stejném členském státě. Pole pod nadpisem „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:** poskytovatel platebních služeb, u něhož k incidentu došlo.

**Název poskytovatele platebních služeb:** celý název poskytovatele platebních služeb, jehož se oznámení týká, jak je uveden v příslušném oficiálním vnitrostátním rejstříku platebních poskytovatelů služeb.

**Vnitrostátní identifikační číslo poskytovatele platebních služeb:** jedinečné vnitrostátní identifikační číslo používané příslušným orgánem domovského členského státu v jeho vnitrostátním rejstříku k jednoznačné identifikaci poskytovatele platebních služeb.

**Vedoucí skupiny:** V případě skupin subjektů ve smyslu čl. 4 bodu 40 směrnice PSD2 uveďte název hlavního subjektu.

**Země dotčené incidentem**: země, ve kterých má incident dopad (např. je zasaženo několik poboček poskytovatele platebních služeb se sídlem v různých zemích), bez ohledu na závažnost

[2] Dvoupísmenné kódy zemí podle ISO-3166 naleznete na adrese https://www.iso.org/iso-3166-country-codes.html.

incidentu v jiných zemích. Nemusí se jednat o domovský členský stát.

**Hlavní kontaktní osoba:** jméno a příjmení osoby odpovědné za oznámení incidentu nebo v případě, že oznámení jménem dotčeného poskytovatele platebních služeb provádí třetí poskytovatel služeb, jméno a příjmení odpovědné osoby z oddělení řízení incidentů/rizik nebo osoby odpovědné za podobnou oblast činnosti 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-mailovou adresu.
**Telefon:** telefonní číslo, na které se lze v případě potřeby obracet s žádostmi o bližší vysvětlení. Může se jednat o osobní nebo firemní telefonní číslo.
**Další kontaktní osoba**: jméno a příjmení další osoby, na kterou se může příslušný orgán obrátit s dotazy týkajícími se incidentu, pokud není hlavní kontaktní osoba k dispozici. V případě, že oznámení jménem dotčeného poskytovatele platebních služeb činí třetí poskytovatel služeb, jméno a příjmení další osoby z oddělení řízení incidentů/rizik nebo podobné oblasti činnosti dotčeného poskytovatele platebních služeb.
**E-mail:** e-mailová adresa další 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 další kontaktní osoby, na které se lze v případě potřeby obracet s případnými žádostmi o bližší vysvětlení. Může se jednat o osobní nebo firemní telefonní číslo.

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

**Název oznamujícího subjektu:** celý název subjektu, který incident oznamuje, jak je uveden v příslušném oficiálním vnitrostátním obchodním rejstříku.
**Vnitrostátní identifikační číslo:** jedinečné vnitrostátní identifikační číslo používané v zemi, ve které má sídlo třetí strana, k jednoznačné identifikaci subjektu, který incident oznamuje. Pokud je oznamující třetí stranou poskytovatel platebních služeb, vnitrostátním identifikačním číslem by mělo být jedinečné vnitrostátní identifikační číslo poskytovatele platebních služeb, které používá příslušný orgán domovského členského státu ve svém vnitrostátním rejstříku.
**Hlavní 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-mailovou adresu.
**Telefon:** telefonní číslo, na které se lze v případě potřeby obracet s žádostmi o bližší vysvětlení. Může se jednat o osobní nebo firemní telefonní číslo.
**Další kontaktní osoba**: jméno a příjmení další osoby ze subjektu oznamujícího incident, na kterou se může příslušný orgán obracet, pokud není hlavní kontaktní osoba k dispozici.
**E-mail:** e-mailová adresa další 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 další kontaktní osoby, na které se lze v případě potřeby obracet s případnými žádostmi o bližší vysvětlení. Může se jednat o osobní nebo firemní telefonní číslo.

## A 2 - Zjištění a klasifikace incidentu

**Datum a čas zjištění incidentu:** datum a čas, kdy byl incident poprvé zjištěn.
**Datum a čas klasifikace incidentu**: datum a čas, kdy byl bezpečnostní nebo operační incident klasifikován jako významný.
**Kdo incident zjistil:** uveďte, zda byl incident zjištěn uživatelem platební služby, v rámci poskytovatele platebních služeb (např. funkcí interního auditu) nebo jinou externí stranou (např. poskytovatelem služeb). Pokud se nejedná o žádnou z uvedených možností, vysvětlete v příslušném poli.
**Druh incidentu:** uveďte, zda se podle vašeho nejlepšího vědomí jedná o operační nebo bezpečnostní incident, pokud je tato informace dostupná.

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

**Bezpečnostní:** neoprávněný přístup, používání, zveřejnění, narušení, změna nebo zničení aktiv poskytovatele platebních služeb, což má dopad na integritu, dostupnost, důvěrnost a/nebo autenticitu služeb souvisejících s platbami. K tomu může dojít mimo jiné v případě, že u poskytovatele platebních služeb dojde k narušení bezpečnosti sítě nebo informačních systémů.

**Kritéria vedoucí ke zprávě o významném incidentu:** uveďte, která kritéria vedla k vypracování zprávy o významném incidentu. Existuje vícero možností výběru kritérií: dotčené transakce, dotčení uživatelé platebních služeb, výpadek služby, narušení zabezpečení sítě nebo informačních systémů, ekonomický dopad, vysoká úroveň interní eskalace, ostatní potenciálně dotčení poskytovatelé platebních služeb nebo příslušné infrastruktury a/nebo dopad na dobrou pověst.

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

**Případný dopad v jiných členských státech EU:** stručně vysvětlete, jaký dopad měl incident v jiném členském státě EU (např. na uživatele platebních služeb, poskytovatele platebních služeb a/nebo platební infrastruktury). Je-li to možné, poskytněte v příslušných lhůtách pro oznamování překlad do angličtiny.

**Oznamování jiným orgánům:** uveďte, zda incident byl nebo bude oznámen jiným orgánům na základě samostatných rámců pro oznamování incidentů, pokud je to v době oznamování známo. Pokud ano, uveďte příslušné orgány.

**Důvody pro pozdní předložení úvodní zprávy**: vysvětlete důvody, proč jste ke klasifikaci incidentu potřebovali více než 24 hodin.

## B Průběžná zpráva

### B 1 – Obecné údaje

**Podrobnější popis incidentu:** popište hlavní rysy incidentu, zahrnující alespoň informace o konkrétním problému a příslušných souvislostech, dále to, jak incident začal a jak se vyvíjel, a důsledky, zejména pro uživatele platebních služeb atd. Uveďte také informace o případné komunikaci s uživateli platebních služeb.

**Souvisí incident s předchozími incidenty?:** uveďte, zda incident souvisí s předchozími incidenty, pokud tyto informace máte k dispozici. Pokud incident s předchozími incidenty souvisí, uveďte se kterými.

**Byli dotčeni nebo zapojeni další poskytovatelé služeb či třetí strany?:** uveďte, zda se incident dotkl jiných poskytovatelů služeb či třetích stran nebo do něj byli nějak zapojeni, pokud tyto informace máte k dispozici. Pokud se incident dotkl jiných poskytovatelů služeb či třetích stran nebo do něj byli nějak zapojeni, poskytněte jejich seznam a uveďte další podrobnosti.

**Bylo zahájeno krizové řízení (interní a/nebo externí)?:** uveďte, zda bylo zahájeno krizové řízení (interní a/nebo externí). Pokud ano, uveďte další podrobnosti.

**Datum a čas vzniku incidentu:** datum a čas začátku incidentu, je-li to znám.

**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 k normálnímu provozu.

**Dotčené funkční oblasti:** uveďte krok nebo kroky platebního procesu, kterých se incident dotkl, jako je ověření/autorizace, komunikace, zúčtování, přímé vypořádání, nepřímé vypořádání a další.

**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 převodu peněžních prostředků.

**Komunikace:** tok informací za účelem identifikace, ověřování, oznamování a poskytování

informací mezi poskytovateli platebních služeb, kteří vedou účet, poskytovateli služeb iniciování platby, poskytovateli služeb informování o účtu, plátci, příjemci a dalšími poskytovateli platebních služeb.

**Zúčtování:** proces předání, sesouhlasení a v některých případech potvrzení převodních příkazů před vypořádáním, včetně případného 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. Ve volném textovém poli uveďte další podrobnosti.

**Změny oproti předchozím zprávám:** uveďte změny oproti informacím uvedeným v předchozích zprávách týkajících se stejného incidentu (např. v úvodní zprávě, případně v průběžné zprávě).

## B 2 – Klasifikace incidentu / informace o incidentu

**Dotčené transakce:** Poskytovatelé platebních služeb by měli uvést, které prahové hodnoty byly nebo pravděpodobně budou incidentem dosaženy, a související údaje: počet dotčených transakcí, procentní 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. 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 peněžní 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 pro výpočet. Jestliže poskytovatelé platebních služeb tento údaj nepovažují za vypovídající (např. kvůli sezónnosti), měli by místo toho použít jinou, více vypovídající metriku a sdělit příslušnému orgánu odpovídající odůvodnění tohoto přístupu v poli „Poznámky“. V případech, kdy se incident dotýká platebních transakcí v měnách jiných než euro, by měli poskytovatelé platebních služeb při výpočtu prahových hodnot a vykazování hodnoty transakcí, které byly dotčeny, převést částku transakcí v jiné měně než euro na euro pomocí referenčního směnného kurzu ECB pro den předcházející odeslání zprávy o incidentu.

**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 procentní 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. 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 činnosti. 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 dotčený 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 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.

**Narušení zabezpečení sítě nebo informačních systémů:** Poskytovatelé platebních služeb by měli určit, zda nějaká škodlivá činnost neohrozila dostupnost, autenticitu, integritu nebo důvěrnost sítě nebo informačních systémů (včetně dat) souvisejících s poskytováním 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 hodnotu této proměnné, přičemž se může jednat o skutečný údaj, nebo o odhad. Poskytovatelé platebních služeb by měli zohlednit dobu, po kterou trvá nebo pravděpodobně bude trvat výpadek jakéhokoliv úkolu, 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 určit délku výpadku služby od okamžiku, kdy výpadek začne, přičemž by měli 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 určit 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 a nepřímé náklady. Poskytovatelé platebních služeb by měli uvést konkrétní hodnoty těchto proměnných, přičemž se může jednat o skutečné údaje, nebo o odhady. 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 peněžní prostředky nebo aktiva, náklady na výměnu hardwaru nebo softwaru, další náklady na forenzní analýzy nebo náklady na nápravu škod, poplatky v důsledku nedodržení smluvních závazků, 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 případech, kdy jsou náklady v měnách jiných než euro, by při výpočtu prahové hodnoty a vykazování hodnoty ekonomického dopadu měli poskytovatelé platebních služeb převést částku nákladů v měně jiné než euro na euro pomocí referenčního směnného kurzu ECB pro den před předložením zprávy o incidentu.

> **Přímé náklady:** náklady (v eurech) přímo způsobené incidentem, včetně nákladů na nápravu incidentu (např. ztracené peněžní prostředky nebo aktiva, náklady na výměnu hardwaru a softwaru, poplatky z důvodu nedodržení smluvních závazků).
>
> **Nepřímé náklady:** náklady (v eurech) nepřímo způsobené incidentem (např. náklady na odškodnění či náhradu škody klienta, případné právní náklady).

**Vysoká úroveň interní eskalace:** Poskytovatelé platebních služeb by měli zvážit, zda vedoucí orgán, jak je definován v obecných pokynech orgánu EBA pro řízení rizik v oblasti IKT a bezpečnosti, byl nebo pravděpodobně bude v důsledku dopadu na služby související s platbami informován o incidentu v souladu s obecným pokynem 60 písm. d) obecných pokynů orgánu EBA pro řízení rizik v oblasti IKT a bezpečnosti mimo jakýkoli postup pravidelného oznamování a průběžně po celou dobu trvání incidentu. Dále by poskytovatelé platebních služeb měli zohlednit, zda v důsledku dopadu incidentu na služby související s platbami byl nebo pravděpodobně bude vyhlášen krizový režim.

**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 platební schémata, která podporují tyto a ostatní 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 spolehlivost finančního systému jako celku. Poskytovatelé platebních služeb by měli zohlednit různé aspekty, například to, zda jsou dotčená složka / dotčený 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 vzít v úvahu, zda i) si uživatelé platebních služeb nebo jiní poskytovatelé platebních služeb stěžovali na nepříznivý dopad incidentu; ii) incident ovlivnil viditelný proces související s platební službou, a je tedy pravděpodobné, že se mu dostane nebo se mu již dostalo mediálního pokrytí (s přihlédnutím nejen k tradičním sdělovacím prostředkům, jako jsou noviny, ale také k blogům, sociálním sítím atd.; mediální pokrytí v této souvislosti však znamená nejen několik negativních komentářů sledujících, měla by existovat platná zpráva nebo významný počet negativních komentářů či upozornění); iii) smluvní závazky nebyly nebo pravděpodobně nebudou dodrženy, což povede ke zveřejnění právních kroků proti poskytovateli platebních služeb; iv) nebyly dodrženy požadavky regulace, což má za následek uložení opatření v oblasti dohledu nebo sankcí, které byly nebo budou pravděpodobně zveřejněny, nebo v) k podobnému druhu incidentu došlo již dříve.

## B 3 – Popis incidentu

**Druh incidentu**: operační nebo bezpečnostní. Další vysvětlení je uvedeno v příslušném poli v úvodní zprávě.

**Příčina incidentu:** uveďte příčinu incidentu, a pokud ještě není známa, tu, která je nejpravděpodobnější. Lze vybrat více možností.

**Probíhá šetření:** zaškrtněte políčko, jestliže je příčina v současné době neznámá.

**Škodlivá činnost:** činnost úmyslně zaměřená proti poskytovateli platebních služeb. Zahrnuje škodlivý kód, shromažďování informací, průniky, útok (distribuovaným) odmítnutím služby, úmyslnou interní činnost, úmyslné externí fyzické poškození, zabezpečení informačního obsahu, podvodná jednání atd. Více informací naleznete v části C2 tohoto formuláře.

**Selhání procesu:** příčinou incidentu byl chybný návrh nebo provedení platebního procesu, kontrol procesu a/nebo podpůrných procesů (např. proces změny či 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.

**Lidské chyby:** incident byl způsoben neúmyslnou chybou člověka, ať už v rámci provádění platby (např. nahrání chybného hromadného platebního příkazu do platebního systému), nebo v souvislosti s ním (např. neúmyslné odpojení od elektrického proudu a následné odložení platební činnosti).

**Externí události:** příčina souvisí s událostmi, nad kterými dotčená organizace nemá všeobecně přímou kontrolu (např. přírodní katastrofy, selhání poskytovatele technických služeb).

**Jiné:** žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

**Dotkl se vás incident přímo nebo nepřímo prostřednictvím poskytovatele služeb?:** uveďte, zda se incident týkal přímo poskytovatele platebních služeb, nebo se jej dotkl nepřímo prostřednictvím třetí strany, pokud tyto informace máte k dispozici. V případě nepřímého dopadu uveďte název poskytovatele(ů) služeb.

## B 4 – Dopad incidentu

**Celkový dopad:** uveďte, co všechno operační nebo bezpečnostní incident ovlivnil. Lze vybrat více možností.

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

**Dostupnost:** vlastnost služeb souvisejících s platbami spočívající v tom, že jsou plně přístupné a použitelné uživateli platebních služeb podle přijatelných úrovní předem stanovených poskytovatelem platebních služeb.

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

**Autenticita:** vlastnost zajišťující, že je zdroj tím, za co se vydává.

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

**Pobočky:** provozovna (jiná než ústředí), která je součástí poskytovatele platebních služeb, nemá právní subjektivitu a přímo provádí některé nebo všechny transakce tvořící podstatu činnosti poskytovatele platebních služeb. Má-li poskytovatel platebních služeb ústředí v jednom členském státě a více provozoven v jiném členském státě, považují se všechny tyto provozovny 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:** fyzické prostory obchodníka, ve kterých je iniciována platební transakce.

**Elektronické obchodování:** platební transakce je iniciována na virtuálním místě prodeje (např. pro platby iniciované prostřednictvím internetu pomocí úhrad, platebních karet, převodu elektronických peněz mezi účty elektronických peněz).

**Jiné:** dotčeným obchodním kanálem není žádná z výše uvedených možností. Ve volném textovém poli uveďte další podrobnosti.

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

**Vložení hotovosti na platební účet:** vydání 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 instrukcí 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 schématu 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, při níž se poskytovatel platebních služeb smluvně zavazuje poskytovat plátci platební prostředek za účelem iniciování a zpracování jeho platebních transakcí.
**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:** platební služby 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.

### B 5 – Zmírnění incidentu

**Jaká opatření byla doposud přijata nebo jsou plánována s cílem dosáhnout obnovy po incidentu?:** uveďte podrobnosti o opatřeních, která byla přijata nebo jsou plánována k dočasnému vyřešení incidentu.
**Došlo k aktivaci plánu kontinuity činnosti a/nebo plánu obnovy provozu 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 v čem spočívaly).

## C – Závěrečná zpráva

### C 1 – Obecné údaje

**Aktualizace informací z úvodní zprávy a z průběžných zpráv** (shrnutí): uveďte další informace o incidentu, včetně konkrétních změn oproti informacím uvedeným v průběžné zprávě. Uveďte také jakékoli další relevantní informace.
**Jsou zavedeny všechny původní kontroly?:** uveďte, zda poskytovatel platebních služeb musel kdykoli během incidentu zrušit nebo oslabit některé kontroly. Pokud ano, uveďte, zda jsou všechny kontroly opět zavedeny, a pokud ne, vysvětlete ve volném textovém poli, které kontroly nejsou opět zavedeny, a dobu potřebnou k jejich obnovení.

## C 2 – Analýza hlavních příčin a následná opatření

**Co bylo hlavní příčinou (je-li již známa)?:** uveďte, hlavní příčinu incidentu, , a pokud ještě není známa, tu, která je nejpravděpodobnější. Lze vybrat více možností. (Pamatujte, že hlavní příčinu je třeba odlišit od dopadu incidentu.)

**Škodlivá činnost:** externí nebo interní činnost úmyslně zaměřená proti poskytovateli platebních služeb. Tyto činnosti jsou rozděleny do těchto kategorií:

**Škodlivý kód:** např. virus, červ, trojský kůň, spyware.

**Shromažďování informací:** např. skenování, sniffing, sociální inženýrství.

**Průniky:** např. kompromitovaný privilegovaný účet, kompromitovaný neprivilegovaný účet, kompromitovaná aplikace, bot.

**Útok (distribuovaným) odmítnutím služby:** pokus znepřístupnit on-line službu tím, že dojde k jejímu zahlcení provozem z více zdrojů.

**Úmyslná interní činnost:** např. sabotáž, krádež.

**Úmyslné externí fyzické poškození:** např. sabotáž, fyzický útok na prostory či datová centra.

**Zabezpečení informačního obsahu:** neoprávněný přístup k informacím, neoprávněná změna informací.

**Podvodná jednání:** neautorizované použití zdrojů, porušení autorských práv, útok typu maškaráda, phishing.

**Jiné (specifikujte):** žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

**Selhání procesu:** příčinou incidentu byl chybný návrh nebo provedení platebního procesu, kontrol procesu a/nebo podpůrných procesů (např. proces změny či migrace dat, testování, konfigurace, kapacita, monitorování). Tyto činnosti jsou rozděleny do těchto kategorií:

**Nedostatečné monitorování a kontrola:** např. ve vztahu k probíhajícím operacím, data vypršení platnosti certifikátů, data vypršení platnosti licencí, data vypršení platnosti aktualizací, vymezené maximální hodnoty čítače, úrovně naplnění databáze, správa uživatelských práv, princip dvojí kontroly.

**Problémy s komunikací:** např. mezi účastníky trhu nebo v rámci organizace.

**Nesprávné operace:** např. žádná výměna certifikátů, plná mezipaměť.

**Nedostatečné řízení změn:** např. neidentifikované chyby konfigurace, zavedení včetně aktualizací, problémy týkající se údržby, neočekávané chyby.

**Nedostatečnost interních postupů a dokumentace:** např. nedostatek transparentnosti, pokud jde o funkce, procesy a poruchy, neexistence dokumentace.

**Problémy s obnovou:** např. řízení nepředvídaných událostí, nedostatečná redundance.

**Jiné (specifikujte):** žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

**Selhání systému:** příčina incidentu souvisí s nevhodným návrhem, provedením, složkami, specifikacemi, integrací nebo složitostí systémů, které platební činnost podporují. Tyto činnosti jsou rozděleny do těchto kategorií:

**Selhání hardwaru:** selhání fyzického technologického zařízení, které spouští procesy a/nebo ukládá údaje, které poskytovatelé platebních služeb potřebují k výkonu činnosti související s platbami (např. selhání pevných disků, datových center, jiné infrastruktury).

**Selhání sítě:** selhání telekomunikačních sítí, ať už veřejných, nebo soukromých, které umožňují výměnu dat a informací (např. přes internet) během platebního procesu.

**Problémy s databází:** datová struktura, která uchovává osobní údaje a údaje související s platbami potřebné k provádění platebních transakcí.

**Selhání softwaru/aplikace:** selhání programů, operačních systémů atd., které podporují poskytování platebních služeb poskytovatelem platebních služeb (např. poruchy,

neznámé funkce).

**Fyzické poškození:** např. neúmyslné poškození způsobené nevhodnými podmínkami, stavebními pracemi.

**Jiné (uveďte):** žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

**Lidská chyba:** incident byl způsoben neúmyslnou chybou člověka, ať už v rámci provádění platby (např. nahrání chybného hromadného platebního příkazu do platebního systému), nebo v souvislosti s ním (např. neúmyslné odpojení od elektrického proudu a následné odložení platební činnosti). Tyto činnosti jsou rozděleny do těchto kategorií:

**Neúmyslná činnost:** např. chyby, omyly, opomenutí, nedostatek zkušeností a znalostí.

**Nečinnost:** např. kvůli nedostatku dovedností, znalostí, zkušeností, povědomí.

**Nedostatečné zdroje:** např. nedostatek lidských zdrojů, zaměstnanci nejsou k dispozici.

**Jiné (uveďte):** žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

**Externí událost:** příčina souvisí s událostmi, nad kterými dotčená organizace nemá všeobecně kontrolu. Tyto činnosti jsou rozděleny do těchto kategorií:

**Selhání dodavatele / poskytovatele technických služeb:** např. výpadek elektrického proudu, výpadek internetu, právní problémy, obchodní problémy, závislost na službách.

**Vyšší moc:** např. výpadek elektrického proudu, požár, přírodní příčiny, jako jsou zemětřesení, povodně, silné srážky, silný vítr.

**Jiné (uveďte):** žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

**Jiné:** žádná z výše uvedených možností není příčinou incidentu. Ve volném textovém poli uveďte další podrobnosti.

**Další relevantní informace o hlavní příčině:** uveďte jakékoli další informace o hlavní příčině, včetně předběžných závěrů vyvozených z analýzy hlavních příčin.

**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 opakování incidentu v budoucnu.

## C 3 – Další 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 podrobnosti o poskytovatelích platebních služeb, kteří byli informováni, o poskytnutých informacích a příslušných důvodech pro poskytnutí těchto informací.

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

**Posouzení účinnosti přijatých opatření:** uveďte, je-li k dispozici, sebehodnocení účinnosti opatření přijatých během trvání incidentu, včetně veškerých poučení vyvozených z incidentu.