EBA/GL/2021/03

10. jún 2021

Revidované usmernenia

k oznamovaniu závažných incidentov podľa druhej smernice o platobných službách

1. Povinnosť dodržiavania usmernení a oznamovacia povinnosť

Status týchto usmernení

1. Tento dokument obsahuje usmernenia vydané podľa článku 16 nariadenia o Európskom orgáne pre bankovníctvo (ďalej len „EBA“)[1]. V súlade s článkom 16 ods. 3 nariadenia o EBA musia príslušné orgány a finančné inštitúcie vynaložiť všetko úsilie na dodržanie týchto usmernení.

2. V týchto usmerneniach sa uvádza stanovisko EBA k náležitým postupom dohľadu v rámci Európskeho systému finančného dohľadu alebo k spôsobu, akým sa má uplatňovať právo Únie v konkrétnej oblasti. Príslušné orgány vymedzené v článku 4 ods. 2 nariadenia o EBA, na ktoré sa usmernenia vzťahujú, ich majú dodržiavať tak, že ich primeraným spôsobom začlenia do svojich postupov (napríklad zmenou svojho právneho rámca alebo procesov dohľadu) vrátane prípadov, keď sú usmernenia určené predovšetkým inštitúciám.

Požiadavky na oznamovanie

3. Podľa článku 16 ods. 3 nariadenia o EBA musia príslušné orgány oznámiť EBA, či tieto usmernenia dodržiavajú alebo majú v úmysle dodržať, alebo musia uviesť dôvody ich nedodržania do (07.11.2021). Ak to príslušné orgány do tohto termínu neoznámia, EBA ich bude považovať za orgány, ktoré nedodržiavajú tieto usmernenia. Oznámenia je potrebné zaslať prostredníctvom formulára dostupného na webovom sídle EBA s uvedením referenčného čísla „EBA/GL/2021/03“. Oznámenia majú predkladať osoby s náležitým oprávnením na oznamovanie dodržiavania súladu v mene svojich príslušných orgánov. Akúkoľvek zmenu stavu dodržiavania usmernení treba takisto oznámiť EBA.

4. Oznámenia budú uverejnené na webovom sídle orgánu EBA v súlade s článkom 16 ods. 3 uvedeného nariadenia.

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12).

2. Predmet úpravy, rozsah pôsobnosti a vymedzenie pojmov

Predmet úpravy

5. Tieto usmernenia vychádzajú z mandátu udeleného orgánu EBA v článku 96 ods. 3 smernice Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES (ďalej len „druhá smernica o platobných službách“).

6. V týchto usmerneniach sa stanovujú najmä kritériá na klasifikáciu závažných prevádzkových alebo bezpečnostných incidentov poskytovateľov platobných služieb, ako aj formát a postupy, ktoré majú dodržiavať pri oznamovaní takýchto incidentov príslušnému orgánu v domovskom členskom štáte, podľa článku 96 ods. 1 druhej smernice o platobných službách.

7. Okrem toho sa tieto usmernenia zaoberajú spôsobom, akým by mali príslušné orgány posudzovať relevantnosť incidentu, a podrobné informácie uvedené v hláseniach o incidentoch, ktoré podľa článku 96 ods. 2 uvedenej smernice súčasne oznamujú aj iným vnútroštátnym orgánom.

8. Tieto usmernenia sa venujú aj súčasnému poskytovaniu relevantných podrobných informácií o oznámených incidentoch orgánu EBA a Európskej centrálnej banke (ďalej len „ECB“) s cieľom podporiť spoločný a jednotný prístup.

Rozsah uplatňovania

9. Tieto usmernenia sa uplatňujú v súvislosti s klasifikáciou a oznamovaním závažných prevádzkových alebo bezpečnostných incidentov v súlade s článkom 96 druhej smernice o platobných službách.

10. Vzťahujú sa na všetky incidenty zahrnuté do vymedzenia pojmu „závažný prevádzkový alebo bezpečnostný incident“, ktorý sa týka možných úmyselných alebo náhodných externých aj interných udalostí.

11. Tieto usmernenia sa uplatňujú aj v prípadoch, ak závažný prevádzkový alebo bezpečnostný incident vznikne mimo Únie (napríklad ak incident vznikne v materskej spoločnosti alebo dcérskej spoločnosti so sídlom mimo Únie) a ovplyvní platobné služby poskytované poskytovateľom platobných služieb so sídlom v Únii, a to buď priamo (službu súvisiacu s platbou vykonáva dotknutá spoločnosť mimo Únie), alebo nepriamo (v dôsledku incidentu je

iným spôsobom ohrozená kapacita poskytovateľa platobných služieb naďalej vykonávať svoju platobnú činnosť).

12. Tieto usmernenia sa uplatňujú aj v prípadoch závažných incidentov ovplyvňujúcich funkcie, ktoré poskytovatelia platobných služieb zadali externým tretím stranám.

Adresáti

13. Prvý súbor usmernení (oddiel 4) je určený poskytovateľom platobných služieb, ktorí sú vymedzení v článku 4 bode 11 druhej smernice o platobných službách a ako je to uvedené v článku 4 ods. 1 nariadenia (EÚ) č. 1093/2010.

14. Druhý a tretí súbor usmernení (oddiely 5 a 6) sú určené príslušným orgánom, ktoré sú vymedzené v článku 4 ods. 2 písm. i) nariadenia (EÚ) č. 1093/2010.

Vymedzenie pojmov

15. Pokiaľ nie je uvedené inak, pojmy používané a vymedzené v druhej smernici o platobných službách majú v týchto usmerneniach rovnaký význam. Na účely týchto usmernení sa okrem toho uplatňuje toto vymedzenie pojmov:

Prevádzkový alebo bezpečnostný incident	Ojedinelá udalosť alebo rad navzájom súvisiacich udalostí, ktoré poskytovateľ platobných služieb neplánoval a ktoré majú alebo pravdepodobne budú mať nepriaznivý vplyv na integritu, dostupnosť, dôvernosť a/alebo hodnovernosť služieb súvisiacich s platbami.
Integrita	Vlastnosť, ktorá znamená, že je zabezpečená presnosť a úplnosť aktív (vrátane údajov).
Dostupnosť	Vlastnosť, ktorá znamená, že služby súvisiace s platbami sú prístupné používateľom platobných služieb a títo používatelia ich môžu využívať, a to podľa prípustných úrovní vopred vymedzených poskytovateľom platobných služieb.
Dôvernosť	Vlastnosť, ktorá znamená, že informácie sa nezverejnia ani nesprístupnia neoprávneným osobám, subjektom či procesom.
Hodnovernosť	Vlastnosť, ktorá znamená, že zdroj je naozaj tým, za čo sa vydáva.
Služby súvisiace s platbami	Každá ekonomická činnosť v zmysle článku 4 bodu 3 druhej smernice o platobných službách a všetky potrebné odborné podporné úlohy na správne poskytovanie platobných služieb.

3. Vykonávanie

Dátum začiatku uplatňovania

16. Tieto usmernenia sa uplatňujú od 1. januára 2022.

Zrušenie

17. S účinnosťou od 1. januára 2022 sa rušia tieto usmernenia:

Usmernenia k oznamovaniu závažných incidentov podľa smernice (EÚ) 2015/2366 o platobných službách (PSD2) (EBA/GL/2017/10)

4. Usmernenia určené poskytovateľom platobných služieb k oznamovaniu závažných prevádzkových alebo bezpečnostných incidentov príslušnému orgánu v domovskom členskom štáte

Usmernenie 1: Klasifikácia závažného incidentu

1.1. Poskytovatelia platobných služieb by mali klasifikovať ako závažné také prevádzkové alebo bezpečnostné incidenty, ktoré spĺňajú

a. jedno alebo viaceré kritériá na „úrovni väčšieho vplyvu“; alebo

b. tri alebo viaceré kritériá na „úrovni menšieho vplyvu“,

ako je to stanovené v usmernení 1.4 a posúdené podľa týchto usmernení.

1.2. Poskytovatelia platobných služieb by mali posúdiť prevádzkový alebo bezpečnostný incident podľa týchto kritérií a ich súvisiacich ukazovateľov:

i. Dotknuté transakcie

Poskytovatelia platobných služieb by mali určiť celkovú hodnotu dotknutých transakcií, ako aj počet ohrozených platieb ako percentuálny podiel bežnej úrovne platobných transakcií vykonaných v rámci dotknutých platobných služieb.

ii. Dotknutí používatelia platobných služieb

Poskytovatelia platobných služieb by mali určiť počet dotknutých používateľov platobných služieb, a to v absolútnom vyjadrení, ako aj percentuálnom pomere k celkovému počtu používateľov platobných služieb.

iii. Porušenie bezpečnosti siete alebo informačných systémov

Poskytovatelia platobných služieb by mali určiť, či nejaké škodlivé konanie oslabilo bezpečnosť siete alebo informačných systémov súvisiacich s poskytovaním platobných služieb.

iv. Výpadok služby

Poskytovatelia platobných služieb by mali určiť časové obdobie, počas ktorého bude služba pre používateľa platobnej služby pravdepodobne nedostupná alebo počas ktorého nebude môcť poskytovateľ platobnej služby vykonať platobný príkaz v zmysle článku 4 bodu 13 druhej smernice o platobných službách.

v. Hospodársky vplyv

Poskytovatelia platobných služieb by mali holisticky určiť finančné náklady spojené s incidentom a zohľadniť absolútne vyjadrenie a v prípade potreby aj relatívny význam týchto nákladov, pokiaľ ide o veľkosť poskytovateľa platobných služieb (t. j. vzhľadom na kapitál Tier 1 poskytovateľa platobných služieb).

vi. Vysoká miera vnútornej eskalácie

Poskytovatelia platobných služieb by mali určiť, či tento incident bol alebo pravdepodobne bude nahlásený vedúcim pracovníkom.

vii. Iní potenciálne dotknutí poskytovatelia platobných služieb alebo relevantné infraštruktúry

Poskytovatelia platobných služieb by mali určiť pravdepodobné systémové vplyvy incidentu, t. j. jeho potenciál zasiahnuť okrem pôvodne dotknutého poskytovateľa platobných služieb aj iných poskytovateľov platobných služieb, infraštruktúry finančných trhov a/alebo platobné schémy.

viii. Poškodenie dobrého mena

Poskytovatelia platobných služieb by mali určiť, ako môže incident ohroziť dôveru používateľov v samotného poskytovateľa platobných služieb, a vo všeobecnosti súvisiacu službu alebo trh ako taký.

1.3. Poskytovatelia platobných služieb by mali vypočítať hodnotu ukazovateľov podľa tejto metodiky:

i. Dotknuté transakcie:

Vo všeobecnosti platí, že poskytovatelia platobných služieb by mali pod pojmom „dotknutá transakcia“ chápať všetky domáce a cezhraničné transakcie, ktoré boli alebo pravdepodobne budú priamo či nepriamo dotknuté incidentom, a najmä tie transakcie, ktoré nebolo možné iniciovať alebo spracovať, transakcie, v prípade ktorých bol zmenený obsah platobnej správy, a transakcie, pre ktoré bol príkaz vystavený podvodne (či už prostriedky boli, alebo neboli získané späť) alebo keď incident nejakým iným spôsobom zabráni riadnemu vykonaniu alebo mu prekáža.

V prípade prevádzkových incidentov ovplyvňujúcich schopnosť iniciovať a/alebo spracovať transakcie by poskytovatelia platobných služieb mali oznamovať len incidenty trvajúce dlhšie než hodinu. Trvanie incidentu by sa malo merať od chvíle, keď sa incident stane, do chvíle, keď sa obnovia bežné činnosti/operácie na úroveň služby, ktorá bola poskytovaná pred incidentom.

Poskytovatelia platobných služieb by mali okrem toho chápať bežnú úroveň platobných transakcií ako ročný denný priemer domácich a cezhraničných platobných transakcií vykonávaných tými istými platobnými službami, ktoré boli dotknuté incidentom, pričom pri výpočte sa za referenčné obdobie považuje predchádzajúci rok. V prípade, že poskytovatelia platobných služieb nepovažujú tento údaj za reprezentatívny (napríklad z dôvodu

sezónnosti), mali by použiť inú, reprezentatívnejšiu metriku a príslušnému orgánu oznámiť zdôvodnenie tohto prístupu v zodpovedajúcej časti vzorového formulára (pozri prílohu).

ii. Dotknutí používatelia platobných služieb

Poskytovatelia platobných služieb by mali pod pojmom „dotknutí používatelia platobných služieb“ rozumieť všetkých zákazníkov (domácich alebo zahraničných, spotrebiteľov alebo spoločnosti), ktorí majú zmluvu s dotknutým poskytovateľom platobných služieb, ktorá im zaručuje prístup k dotknutej platobnej službe, a ktorí utrpeli alebo pravdepodobne utrpia škody v dôsledku incidentu. Poskytovatelia platobných služieb by sa mali pri určovaní počtu používateľov platobných služieb, ktorí počas trvania incidentu mohli používať platobnú službu, vrátiť k odhadom vyplývajúcim z minulej činnosti.

V prípade skupín by mal každý poskytovateľ platobných služieb vziať do úvahy iba vlastných používateľov platobných služieb. V prípade, že poskytovateľ platobných služieb ponúka prevádzkové služby ostatným, mal by vziať do úvahy iba vlastných používateľov platobných služieb (ak existujú), a poskytovatelia platobných služieb, ktorí sú príjemcami týchto prevádzkových služieb, by mali posúdiť incident vo vzťahu k vlastným používateľom platobných služieb.

V prípade prevádzkových incidentov ovplyvňujúcich schopnosť iniciovať a/alebo spracovať transakcie by poskytovatelia platobných služieb mali oznamovať len incidenty, ktoré ovplyvňujú používateľov platobných služieb dlhšie než hodinu. Trvanie incidentu by sa malo merať od chvíle, keď sa incident stane, do chvíle, keď sa obnovia bežné činnosti/operácie na úroveň služby, ktorá bola poskytovaná pred incidentom.

Poskytovatelia platobných služieb by mali okrem toho za celkový počet používateľov platobných služieb považovať súhrnný údaj o domácich a cezhraničných používateľoch platobných služieb, s ktorými sú zmluvne viazaní v čase incidentu (alebo najnovší dostupný údaj) a ktorí majú prístup k dotknutej platobnej službe, a to bez ohľadu na ich veľkosť alebo na to, či sa považujú za aktívnych alebo pasívnych používateľov platobných služieb.

iii. Porušenie bezpečnosti siete alebo informačných systémov

Poskytovatelia platobných služieb by mali určiť, či nejaké škodlivé konanie oslabilo dostupnosť, hodnovernosť, integritu alebo dôvernosť siete alebo informačných systémov (vrátane údajov) súvisiacich s poskytovaním platobných služieb.

iv. Výpadok služby

Poskytovatelia platobných služieb by mali zohľadniť časové obdobie, počas ktorého sa zaznamenal alebo pravdepodobne zaznamená výpadok úlohy, procesu alebo kanálu v súvislosti s poskytovaním platobných služieb, a tým sa zabráni i) iniciovaniu a/alebo vykonaniu platobnej služby a/alebo ii) prístupu k platobnému účtu. Poskytovatelia platobných služieb by mali počítať čas výpadku služby od chvíle jeho začatia a mali by zohľadniť časové intervaly, počas ktorých vykonávajú svoje činnosti potrebné na realizáciu platobných služieb, a v prípade potreby aj obdobia, keď majú zatvorené a keď sa vykonáva

údržba. Ak poskytovatelia platobných služieb nie sú schopní určiť, kedy sa výpadok služby začal, mali by výnimočne čas výpadku služby počítať od chvíle zistenia výpadku.

v. Hospodársky vplyv

Poskytovatelia platobných služieb by mali zohľadniť náklady, ktoré je možné priamo spojiť s incidentom, ale aj tie, ktoré sa ho týkajú nepriamo. Poskytovatelia platobných služieb by mali okrem iného zohľadniť vyvlastnené finančné prostriedky alebo aktíva, reprodukčnú obstarávaciu cenu hardvéru alebo softvéru, ďalšie forenzné náklady alebo náklady na nápravu, poplatky za nedodržanie zmluvných povinností, sankcie, externé záväzky a straty príjmov. Pokiaľ ide o nepriame náklady, poskytovatelia platobných služieb by mali zohľadniť iba tie z nich, ktoré sú už známe alebo veľmi pravdepodobne vzniknú.

vi. *Vysoká miera vnútornej eskalácie*

Poskytovatelia platobných služieb by mali zohľadniť, či v dôsledku vplyvu na služby súvisiace s platbami riadiaci orgán, ako je vymedzený v usmerneniach EBA o riadení rizika v oblasti informačných a komunikačných technológií (ďalej len „IKT“) a bezpečnosti, bol alebo pravdepodobne bude, v súlade s usmernením 60 d) usmernení EBA o riadení rizika v oblasti IKT a bezpečnosti, informovaný o incidente mimo akéhokoľvek postupu pravidelného oznamovania a priebežne počas celého trvania incidentu. Poskytovatelia platobných služieb by mali okrem toho zohľadniť, či sa v dôsledku vplyvu incidentu na služby súvisiace s platbami spustil alebo pravdepodobne spustí krízový režim.

vii. *Iní potenciálne dotknutí poskytovatelia platobných služieb alebo relevantné infraštruktúry*

Poskytovatelia platobných služieb by mali posúdiť vplyv incidentu na finančný trh, pod ktorým sa rozumejú infraštruktúry finančných trhov a/alebo platobné schémy, ktoré to, ako aj ostatných poskytovateľov platobných služieb podporujú. Poskytovatelia platobných služieb by mali posúdiť, či sa incident zopakoval alebo je pravdepodobné, že sa zopakuje v prípade ostatných poskytovateľov platobných služieb, či mal vplyv alebo pravdepodobne bude mať vplyv na bezproblémové fungovanie infraštruktúr finančných trhov a či ohrozil alebo pravdepodobne ohrozí riadnu prevádzku finančného systému ako celku. Poskytovatelia platobných služieb by nemali zabúdať na rôzne rozmery incidentu, ako napríklad to, či sú dotknuté súčasti/dotknutý softvér proprietárne alebo všeobecne dostupné, či je ohrozená sieť interná alebo externá a či poskytovateľ platobných služieb prestal alebo pravdepodobne prestane plniť svoje povinnosti v rámci infraštruktúr finančných trhov, ktorých je členom.

viii. *Poškodenie dobrého mena*

Poskytovatelia platobných služieb by mali zvážiť úroveň viditeľnosti, ktorú podľa ich najlepšieho vedomia incident dosiahol alebo pravdepodobne dosiahne na trhu. Poskytovatelia platobných služieb by mali zvážiť pravdepodobnosť, že incident spôsobí spoločnosti ujmu, čo je dobrým ukazovateľom schopnosti poškodiť ich dobré meno. Poskytovatelia platobných služieb by mali zohľadniť, i) či sa používatelia platobných služieb a/alebo iní poskytovatelia platobných služieb sťažovali na nepriaznivý vplyv incidentu; ii) či

incident ovplyvnil viditeľný proces súvisiaci s platobnou službou a či preto pravdepodobne získa alebo už získal pozornosť médií (do úvahy treba brať nielen tradičné médiá, ako sú noviny, ale aj blogy, sociálne siete atď.); iii) či neboli alebo pravdepodobne nebudú dodržané zmluvné povinnosti, čo povedie k zverejneniu právnych krokov voči poskytovateľovi platobných služieb; iv) či neboli splnené regulačné požiadavky, čo povedie k opatreniam dohľadu alebo sankciám, ktoré sú alebo pravdepodobne budú verejne dostupné a v) či sa podobný druh incidentu stal už predtým.

1.4. Poskytovatelia platobných služieb by mali posúdiť incident tak, že pre každé kritérium určia, či sa pred vyriešením incidentu dosiahli alebo pravdepodobne dosiahnu relevantné prahové hodnoty uvedené v tabuľke 1.

Tabuľka 1: Prahové hodnoty

Kritériá	Úroveň menšieho vplyvu	Úroveň väčšieho vplyvu
Dotknuté transakcie	> 10 % bežnej úrovne transakcií (v zmysle počtu transakcií) poskytovateľa platobných služieb **a** trvanie incidentu > 1 hodina* **alebo** > 500 000 EUR **a** trvanie incidentu > 1 hodina*	> 25% bežnej úrovne transakcií (v zmysle počtu transakcií) poskytovateľa platobných služieb **alebo** > 15 000 000 EUR
Dotknutí používatelia platobných služieb	> 5 000 **a** trvanie incidentu > 1 hodina* **alebo** > 10 % používateľov platobných služieb poskytovateľa platobných služieb **a** trvanie incidentu > 1 hodina*	> 50 000 **alebo** > 25% používateľov platobných služieb poskytovateľa platobných služieb
Výpadok služby	> 2 hodiny	Neuvádza sa
Porušenie bezpečnosti siete alebo informačných systémov	Áno	Neuvádza sa
Hospodársky vplyv	Neuvádza sa	> max (0,1 % kapitálu Tier 1**, 200 000 EUR) **alebo** > 5 000 000 EUR
Vysoká miera vnútornej eskalácie	Áno	Áno a pravdepodobne sa spustí krízový režim (alebo ekvivalentný)

Iní potenciálne dotknutí poskytovatelia platobných služieb alebo relevantné infraštruktúry	Áno	Neuvádza sa
Poškodenie dobrého mena	Áno	Neuvádza sa

* Prahová hodnota týkajúca sa trvania incidentu dlhšie než jednu hodinu sa uplatňuje len na prevádzkové incidenty, ktoré ovplyvňujú schopnosť poskytovateľa platobných služieb iniciovať a/alebo spracovať transakcie.

**Kapitál Tier 1 sa vymedzuje v článku 25 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012.

1.5. Poskytovatelia platobných služieb by mali používať odhady, ak nemajú k dispozícii skutočné údaje, o ktoré by sa mohlo oprieť ich posúdenie, či sa daná prahová hodnota dosiahla alebo sa pravdepodobne dosiahne pred vyriešením incidentu (napríklad by sa to mohlo stať počas úvodnej fázy vyšetrovania).

1.6. Poskytovatelia platobných služieb by mali toto posúdenie vykonávať počas trvania incidentu nepretržite, aby mohli zistiť všetky možné zmeny stavu smerom nahor (z nezávažného na závažný) aj nadol (zo závažného na nezávažný). Každá zmena klasifikácie incidentu zo závažného na nezávažný by sa mala bezodkladne oznámiť príslušnému orgánu v súlade s požiadavkou usmernenia 2.21.

Usmernenie 2: Postup oznamovania

2.1. Poskytovatelia platobných služieb by mali zhromaždiť všetky relevantné informácie, vypracovať oznámenie o incidente vyplnením vzorového formulára uvedeného v prílohe a predložiť ho príslušnému orgánu v domovskom členskom štáte. Poskytovatelia platobných služieb by mali vyplniť všetky polia vzorového formulára podľa pokynov uvedených v prílohe.

2.2. Poskytovatelia platobných služieb by mali použiť rovnaký vzorový formulár pri predkladaní úvodnej, priebežnej a záverečnej správy týkajúcej sa toho istého incidentu. Poskytovatelia platobných služieb by preto mali postupne vypĺňať jeden vzorový formulár s prípadnými aktualizáciami informácií poskytnutých v predchádzajúcich správach.

2.3. Poskytovatelia platobných služieb by okrem toho mali príslušnému orgánu v domovskom členskom štáte v prípade potreby predložiť kópiu informácií poskytnutých (alebo informácií, ktoré sa poskytnú) vlastným používateľom, podľa článku 96 ods. 1 druhého pododseku druhej smernice o platobných službách, a to hneď ako sú informácie k dispozícii.

2.4. Poskytovatelia platobných služieb by mali na požiadanie príslušného orgánu v domovskom členskom štáte poskytnúť všetky ďalšie dokumenty, ktoré dopĺňajú informácie predložené v rámci štandardného vzorového formulára. Poskytovatelia platobných služieb by mali odpovedať na všetky žiadosti príslušného orgánu v domovskom členskom štáte a poskytnúť ďalšie informácie alebo objasnenia týkajúce sa už predloženej dokumentácie.

2.5. Všetky ďalšie informácie obsiahnuté v dokumentoch, ktoré poskytovatelia platobných služieb poskytnú príslušnému orgánu, či už z iniciatívy poskytovateľa platobných služieb, alebo na požiadanie príslušného orgánu v súlade s usmernením 2.4, by mal poskytovateľ platobných služieb uviesť vo vzorovom formulári podľa usmernenia 2.1.

2.6. Poskytovatelia platobných služieb by mali za každých okolností zachovávať dôvernosť a integritu informácií, ktoré si vymieňajú, a riadne sa autentifikovať voči príslušnému orgánu v domovskom členskom štáte.

Úvodná správa

2.7. Poskytovatelia platobných služieb by mali predložiť príslušnému orgánu v domovskom členskom štáte úvodnú správu, keď bol prevádzkový alebo bezpečnostný incident klasifikovaný ako závažný. Príslušné orgány by mali bezodkladne oznámiť prijatie úvodnej správy a prideliť incidentu jedinečný referenčný kód, ktorý ho jednoznačne identifikuje. Poskytovatelia platobných služieb by mali uviesť tento referenčný kód, keď predkladajú aktualizáciu úvodnej správy alebo priebežnej a záverečnej správy týkajúcej sa toho istého incidentu, pokiaľ nepredkladajú priebežnú a záverečnú správu spoločne s úvodnou správou.

2.8. Poskytovatelia platobných služieb by mali odoslať úvodnú správu príslušnému orgánu do štyroch hodín od chvíle, keď bol prevádzkový alebo bezpečnostný incident klasifikovaný ako závažný. Pokiaľ je známe, že kanály príslušného orgánu na odovzdávanie oznámení nebudú v danom čase dostupné alebo v prevádzke, poskytovatelia platobných služieb by mali odoslať úvodnú správu čo najskôr po opätovnom sprístupnení/sprevádzkovaní kanálov.

2.9. Poskytovatelia platobných služieb by mali klasifikovať incident v súlade s usmerneniami 1.1 a 1.4 čo najskôr, ale najneskôr 24 hodín po jeho zistení, a bezodkladne po získaní informácií potrebných na klasifikáciu incidentu. Ak je na klasifikáciu incidentu potrebný dlhší čas, poskytovatelia platobných služieb by mali vysvetliť dôvody v úvodnej správe predloženej príslušnému orgánu.

2.10. Poskytovatelia platobných služieb by mali predložiť príslušnému orgánu v domovskom členskom štáte úvodnú správu aj v prípade, ak sa klasifikácia incidentu zmenila z pôvodne nezávažného na závažný. V tomto konkrétnom prípade by mali poskytovatelia platobných služieb odoslať úvodnú správu príslušnému orgánu ihneď po zistení zmeny stavu, alebo pokiaľ je známe, že kanály príslušného orgánu na odovzdávanie oznámení nebudú v danom čase dostupné alebo v prevádzke, čo najskôr po ich opätovnom sprístupnení/sprevádzkovaní.

2.11. Poskytovatelia platobných služieb by mali v úvodných správach uviesť informácie z hlavičky (t. j. oddielu A vzorového formulára), čiže niektoré základné charakteristiky incidentu a jeho očakávané dôsledky na základe informácií, ktoré sú dostupné ihneď po tom, čo bol incident klasifikovaný ako závažný. Poskytovatelia platobných služieb by mali použiť odhady, ak nemajú k dispozícii skutočné údaje.

Priebežná správa

2.12. Poskytovatelia platobných služieb by mali predložiť priebežnú správu po obnovení bežných činností a návrate ekonomickej činnosti do normálneho stavu, o čom v správe informujú príslušný orgán. Poskytovatelia platobných služieb by mali za návrat ekonomickej činnosti do normálneho stavu považovať situáciu, keď je činnosť/prevádzka obnovená na rovnakú úroveň služieb/podmienok, akú vymedzil poskytovateľ platobných služieb alebo aká sa stanovila v dohode o úrovni poskytovaných služieb (časy spracovania, kapacita, bezpečnostné požiadavky atď.), a keď sa už neuplatňujú pohotovostné opatrenia. Priebežná správa by mala obsahovať podrobnejší opis incidentu a jeho dôsledkov (oddiel B vzorového formulára).

2.13. Ak bežné činnosti zatiaľ neboli obnovené, poskytovatelia platobných služieb by mali predložiť príslušnému orgánu priebežnú správu do troch pracovných dní od predloženia úvodnej správy.

2.14. Poskytovatelia platobných služieb by mali aktualizovať informácie už poskytnuté v oddieloch A a B vzorového formulára v prípadoch, keď od predloženia predchádzajúcej správy zistia závažné zmeny (napríklad incident eskaloval alebo sa zmiernil, identifikujú sa nové príčiny alebo sa prijmú opatrenia na riešenie problému). Zahŕňa to prípad, keď incident nebol vyriešený do troch pracovných dní, čo by si vyžadovalo, aby poskytovatelia platobných služieb predložili ďalšiu priebežnú správu. Poskytovatelia platobných služieb by mali v každom prípade predložiť ďalšiu priebežnú správu na žiadosť príslušného orgánu v domovskom členskom štáte.

2.15. Tak ako v prípade úvodných správ, ak nemajú poskytovatelia platobných služieb k dispozícii skutočné údaje, mali by použiť odhady.

2.16. Ak sa ekonomická činnosť vráti do normálneho stavu do štyroch hodín, odkedy bol incident klasifikovaný ako závažný, poskytovatelia platobných služieb by mali zároveň predložiť úvodnú aj priebežnú správu (t. j. vyplniť oddiely A a B vzorového formulára) v rámci uvedenej štvorhodinovej lehoty.

Záverečná správa

2.17. Poskytovatelia platobných služieb by mali záverečnú správu predložiť po vykonaní analýzy hlavných príčin (bez ohľadu na to, či už boli vykonané zmierňovacie opatrenia alebo zistená konečná hlavná príčina), a keď sú k dispozícii skutočné údaje, ktoré nahradia potenciálne odhady.

2.18. Poskytovatelia platobných služieb by mali záverečnú správu doručiť príslušnému orgánu maximálne do 20 pracovných dní od návratu ekonomickej činnosti do normálneho stavu. Poskytovatelia platobných služieb, ktorí potrebujú predĺženie tejto lehoty (napríklad ak ešte nie sú k dispozícii skutočné údaje o vplyve alebo ešte neboli zistené hlavné príčiny), by sa mali

obrátiť na príslušný orgán ešte pred uplynutím termínu a poskytnúť primerané odôvodnenie oneskorenia, ako aj nový odhadovaný dátum predloženia záverečnej správy.

2.19. Ak sú poskytovatelia platobných služieb schopní predložiť všetky potrebné informácie v záverečnej správe (t. j. oddiel C vzorového formulára) do štyroch hodín, odkedy bol incident klasifikovaný ako závažný, mali by vynaložiť úsilie o spoločné poskytnutie informácií týkajúcich sa úvodnej, priebežnej aj záverečnej správy.

2.20. Poskytovatelia platobných služieb by mali vo svojej záverečnej správe uviesť úplné informácie, t. j. i) skutočné údaje o vplyve namiesto odhadov (ako aj ostatné potrebné aktualizácie v oddieloch A a B vzorového formulára) a ii) oddiel C vzorového formulára, ktorý obsahuje hlavné príčiny, ak sú už známe, a súhrn prijatých opatrení alebo opatrení, ktoré sa plánujú prijať, na odstránenie problému a zabránenie opätovnému výskytu problému v budúcnosti.

2.21. Poskytovatelia platobných služieb by mali záverečnú správu odoslať aj vtedy, ak na základe priebežného posudzovania incidentu zistili, že oznámený incident už nespĺňa kritériá, na základe ktorých sa má považovať za závažný, a pred vyriešením ich pravdepodobne ani spĺňať nebude. V takom prípade by poskytovatelia platobných služieb mali odoslať záverečnú správu čo najskôr po zistení tejto okolnosti, v každom prípade do lehoty na predloženie nasledujúcej správy. V tejto konkrétnej situácii by mali poskytovatelia platobných služieb namiesto vyplnenia oddielu C vzorového formulára začiarknuť políčko „incident preklasifikovaný na nezávažný“ a poskytnúť vysvetlenie dôvodov na túto zmenu klasifikácie.

Usmernenie 3: Delegované a konsolidované oznamovanie

3.1. Ak to príslušný orgán povoľuje, poskytovatelia platobných služieb, ktorí chcú delegovať oznamovacie povinnosti podľa druhej smernice o platobných službách na tretiu stranu, by mali informovať príslušný orgán v domovskom členskom štáte a zabezpečiť splnenie týchto podmienok:

a. Rozdelenie povinností jednotlivých strán sa jednoznačne vymedzuje vo formálnej zmluve a v prípade potreby v existujúcich interných ustanoveniach skupiny, ktoré upravujú delegované oznamovanie medzi poskytovateľom platobných služieb a treťou stranou. Konkrétne sa v nich jednoznačne uvádza, že bez ohľadu na možné delegovanie oznamovacích povinností je za splnenie požiadaviek stanovených v článku 96 druhej smernice o platobných službách a za obsah informácií poskytnutých príslušnému orgánu v domovskom členskom štáte v plnej miere zodpovedný dotknutý poskytovateľ platobných služieb.

b. Delegovanie je v súlade s požiadavkami na externé zabezpečovanie činností v prípade dôležitých prevádzkových funkcií, ako je to stanovené:

i. v článku 19 ods. 6 druhej smernice o platobných službách, pokiaľ ide o platobné inštitúcie a inštitúcie elektronických peňazí, ktorý sa uplatňuje *mutatis mutandis* v súlade s článkom 3 smernice 2009/110/ES; alebo

ii. v usmerneniach orgánu EBA o dohodách o outsourcingu (EBA/GL/2019/02), ktoré sa týkajú všetkých poskytovateľov platobných služieb.

c. Informácie sa predkladajú príslušnému orgánu v domovskom členskom štáte vopred a v každom prípade sa dodržia termíny a postupy stanovené príslušným orgánom, ak existujú.

d. Riadne sa zabezpečí dôvernosť citlivých údajov, ako aj kvalita, jednotnosť, integrita a spoľahlivosť informácií, ktoré sa majú poskytnúť príslušnému orgánu.

3.2. Poskytovatelia platobných služieb, ktorí chcú povoliť určenej tretej strane konsolidované plnenie oznamovacích povinností (t. j. predloženie jednej správy týkajúcej sa viacerých poskytovateľov platobných služieb, v prípade ktorých sa vyskytol rovnaký závažný prevádzkový alebo bezpečnostný incident), by mali informovať príslušný orgán v domovskom členskom štáte a poskytnúť mu kontaktné informácie uvedené v časti „Dotknutí poskytovatelia platobných služieb“ vzorového formulára a zabezpečiť, aby boli splnené tieto podmienky:

a. začleniť toto ustanovenie do zmluvy o delegovaní oznamovania;

b. podmieniť konsolidované oznamovanie tým, že incident je spôsobený narušením služieb poskytovaných treťou stranou;

c. obmedziť konsolidované oznamovanie iba na poskytovateľov platobných služieb so sídlom v rovnakom členskom štáte;

d. poskytnúť zoznam všetkých poskytovateľov platobných služieb dotknutých incidentom;

e. zabezpečiť, aby závažnosť incidentu pre každého dotknutého poskytovateľa platobných služieb posudzovala tretia strana a do konsolidovanej správy zahrnula iba tých poskytovateľov platobných služieb, pre ktorých je incident klasifikovaný ako závažný; okrem toho zabezpečiť, aby v prípade pochybností bol poskytovateľ platobných služieb zahrnutý do konsolidovanej správy, pokiaľ neexistuje žiadny dôkaz potvrdzujúci opačnú situáciu;

f. zabezpečiť, aby v prípade polí vzorového formulára, do ktorých nie je možné uviesť spoločnú odpoveď (napríklad oddiely B2, B4 alebo C3 vzorového formulára), tretia strana i) vyplnila tieto polia jednotlivo za každého dotknutého poskytovateľa platobných služieb a ďalej uviedla identitu každého poskytovateľa platobných

služieb, na ktorého sa informácie vzťahujú, alebo ii) použila kumulatívne pozorované alebo odhadované hodnoty za poskytovateľov platobných služieb;

g. tretia strana vždy informuje poskytovateľa platobných služieb o všetkých relevantných skutočnostiach týkajúcich sa incidentu a o všetkej komunikácii, ktorú môže tretia strana viesť s príslušným orgánom, ako aj o jej obsahu, ale len v takej miere, aby nedošlo k žiadnemu porušeniu požiadaviek na zachovanie dôvernosti informácií týkajúcich sa iných poskytovateľov platobných služieb.

3.3. Poskytovatelia platobných služieb by nemali delegovať svoje oznamovacie povinnosti, kým neinformujú príslušný orgán v domovskom členskom štáte alebo potom, čo im bolo oznámené, že dohoda o externom zabezpečovaní činností nespĺňa požiadavky uvedené v usmernení 3.1 písm. b).

3.4. Poskytovatelia platobných služieb, ktorí chcú zrušiť delegovanie oznamovacích povinností, by mali toto rozhodnutie oznámiť príslušnému orgánu v domovskom členskom štáte v súlade s termínmi a postupmi stanovenými týmto príslušným orgánom. Poskytovatelia platobných služieb by mali informovať príslušný orgán v domovskom členskom štáte aj o každom dôležitom vývoji, ktorý by mohol ovplyvniť určenú tretiu stranu a jej schopnosť plniť oznamovacie povinnosti.

3.5. Poskytovatelia platobných služieb by mali vecne plniť svoje oznamovacie povinnosti bez toho, aby sa obracali na externú pomoc vždy, keď určená tretia strana neinformuje príslušný orgán v domovskom členskom štáte o závažnom prevádzkovom alebo bezpečnostnom incidente podľa článku 96 druhej smernice o platobných službách a podľa týchto usmernení. Poskytovatelia platobných služieb by okrem toho mali zabezpečiť, aby sa incident neoznámil dvakrát, a to individuálne uvedeným poskytovateľom platobných služieb a potom znova treťou stranou.

3.6. Poskytovatelia platobných služieb by mali zabezpečiť, aby v situácii, keď je incident spôsobený narušením služieb poskytovaných poskytovateľom technických služieb (alebo infraštruktúry), čo ovplyvňuje viacerých poskytovateľov platobných služieb, v rámci delegovaného oznamovania sa uvádzajú individuálne údaje poskytovateľa platobných služieb (okrem prípadu konsolidovaného oznamovania).

Usmernenie 4: Prevádzková a bezpečnostná politika

4.1. Poskytovatelia platobných služieb by mali zabezpečiť, aby sa v ich všeobecnej prevádzkovej a bezpečnostnej politike jednoznačne vymedzovali všetky povinnosti v prípade oznamovania incidentov podľa druhej smernice o platobných službách, ako aj procesy, ktoré boli zavedené na splnenie požiadaviek vymedzených v týchto usmerneniach.

5. Usmernenia určené príslušným orgánom ku kritériám na posudzovanie relevantnosti incidentu a podrobných informácií v hláseniach o incidentoch, ktoré sa majú súčasne oznamovať iným vnútroštátnym orgánom

Usmernenie 5: Posúdenie relevantnosti incidentu

5.1. Príslušné orgány v domovskom členskom štáte by mali posúdiť relevantnosť závažného prevádzkového alebo bezpečnostného incidentu pre iné vnútroštátne orgány na základe vlastného odborného stanoviska a pomocou týchto kritérií, ktoré slúžia ako prvotné ukazovatele dôležitosti príslušného incidentu:

a. Príčiny incidentu patria do rozsahu regulačnej právomoci iného vnútroštátneho orgánu (t. j. do jeho oblasti pôsobnosti).
b. Dôsledky incidentu majú vplyv na ciele iného vnútroštátneho orgánu (napríklad zabezpečenie finančnej stability).
c. Incident ovplyvní alebo by mohol vo veľkom rozsahu ovplyvniť používateľov platobných služieb.
d. Incident získa alebo pravdepodobne získa rozsiahlu pozornosť médií.

5.2. Príslušné orgány v domovskom členskom štáte by mali toto posúdenie vykonávať priebežne počas trvania incidentu, aby mohli identifikovať akékoľvek možné zmeny, v dôsledku ktorých by sa incident, ktorý sa pôvodne nepovažoval za dôležitý, mohol preklasifikovať na dôležitý.

Usmernenie 6: Informácie, ktoré sa majú poskytovať

6.1. Bez ohľadu na ďalšiu zákonnú požiadavku, ktorá sa týka poskytovania informácií o incidente iným vnútroštátnym orgánom, by mali príslušné orgány poskytnúť informácie o závažných prevádzkových alebo bezpečnostných incidentoch relevantným vnútroštátnym orgánom identifikovaným na základe uplatňovania usmernenia 5.1 minimálne v čase prijatia úvodnej správy (alebo správy, ktorá podnecuje poskytnutie informácií) a po tom, čo sú informované, že ekonomická činnosť sa vrátila do normálneho stavu (t. j. priebežnej správy).

6.2. Príslušné orgány by mali predložiť relevantným vnútroštátnym orgánom informácie potrebné na vytvorenie jasného obrazu o tom, čo sa stalo, a o možných dôsledkoch. S týmto cieľom by

mali poskytovať minimálne informácie predkladané poskytovateľom platobných služieb v týchto poliach vzorového formulára (v úvodnej alebo priebežnej správe):

- dátum a čas, kedy je incident klasifikovaný ako závažný,
- dátum a čas zistenia incidentu,
- dátum a čas začatia incidentu,
- dátum a čas obnovenia po incidente alebo očakávaného obnovenia po incidente,
- stručný opis incidentu (vrátane podrobného opisu častí, ktoré neobsahujú citlivé informácie),
- stručný opis prijatých alebo plánovaných opatrení na obnovu po incidente,
- opis možného vplyvu incidentu na ostatných poskytovateľov platobných služieb a/alebo infraštruktúry,
- opis (ak existuje) mediálneho pokrytia,
- príčina incidentu.

6.3. Príslušné orgány by pred poskytnutím akýchkoľvek informácií o incidente relevantným vnútroštátnym orgánom mali podľa potreby vykonať riadnu anonymizáciu a vynechať všetky informácie, na ktoré by sa mohli vzťahovať obmedzenia súvisiace so zachovaním dôvernosti alebo s právami duševného vlastníctva. Príslušné orgány by však mali relevantným vnútroštátnym orgánom poskytnúť názov a adresu poskytovateľa platobných služieb podávajúceho správu, ak sú uvedené vnútroštátne orgány schopné zabezpečiť zachovanie dôvernosti informácií.

6.4. Príslušné orgány by mali za každých okolností zachovávať dôverný charakter a integritu uložených a poskytovaných informácií a riadne sa autentifikovať voči relevantným vnútroštátnym orgánom. Bez toho, aby boli dotknuté platné právne predpisy Únie a vnútroštátne požiadavky, by príslušné orgány mali so všetkými informáciami získanými na základe týchto usmernení zaobchádzať predovšetkým v súlade s povinnosťou zachovať služobné tajomstvo, ktoré je vymedzené v druhej smernici o platobných službách.

6. Usmernenia určené príslušným orgánom ku kritériám na posudzovanie relevantných podrobných informácií v hláseniach o incidentoch, ktoré sa majú poskytovať orgánu EBA a ECB, ako aj k formátu a postupom ich oznamovania

Usmernenie 7: Informácie, ktoré sa majú poskytovať

7.1. Príslušné orgány by mali vždy poskytnúť orgánu EBA a ECB všetky správy prijaté od (alebo v mene) poskytovateľov platobných služieb dotknutých závažným prevádzkovým alebo bezpečnostným incidentom, s použitím štandardného súboru dostupného na webovom sídle orgánu EBA.

Usmernenie 8: Komunikácia

8.1. Príslušné orgány by mali za každých okolností zachovávať dôverný charakter a integritu uložených a poskytovaných informácií a riadne sa autentifikovať voči orgánu EBA a ECB. Bez toho, aby boli dotknuté platné právne predpisy Únie a vnútroštátne požiadavky, by príslušné orgány mali so všetkými informáciami získanými na základe týchto usmernení zaobchádzať predovšetkým v súlade s povinnosťou zachovať služobné tajomstvo, ktoré je vymedzené v druhej smernici o platobných službách.

8.2. S cieľom zabrániť omeškaniam pri prenose informácií súvisiacich s incidentom orgánu EBA/ECB a prispieť k minimalizácii rizík narušenia prevádzky by príslušné orgány mali podporovať vhodné komunikačné prostriedky.

Príloha – Vzorový formulár oznámení pre poskytovateľov platobných služieb

Úvodná správa

Úvodná správa	do 4 hodín, odkedy je incident klasifikovaný ako závažný	Obnoviť rozbaľovacie výbery
Dátum správy *(DD/MM/RRRR)*		Čas *(HH.MM)*
Referenčný kód incidentu		

A – Úvodná správa						
A1 – VŠEOBECNÉ ÚDAJE						
Typ výkazu						
Typ výkazu						
Dotknutý poskytovateľ platobných služieb						
Názov poskytovateľa platobných služieb						
Vnútroštátne identifikačné číslo poskytovateľa platobných služieb						
Vedúci skupiny, ak sa uplatňuje						
Krajina/krajiny dotknuté incidentom	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ LI ☐ GR ☐ HR ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Hlavná kontaktná osoba		E-mail		Telefón		
Sekundárna kontaktná osoba		E-mail		Telefón		
Oznamujúci subjekt (tento oddiel vyplňte, ak oznamujúci subjekt nie je dotknutým poskytovateľom platobných služieb v prípade delegovaného oznamovania)						
Názov nahlasujúceho subjektu						
Vnútroštátne identifikačné číslo						
Hlavná kontaktná osoba		E-mail		Telefón		
Sekundárna kontaktná osoba		E-mail		Telefón		
A2 – ZISTENIE INCIDENTU a KLASIFIKÁCIA						
Dátum a čas zistenia incidentu *(DD/MM/RRRR HH.MM)*						
Dátum a čas, kedy je incident klasifikovaný ako závažný *(DD/MM/RRRR HH.MM)*						
Incident zistil			Ak „Iné", uveďte:			
Typ incidentu						
Kritériá vedúce k správe o závažnom incidente	☐ Dotknuté transakcie	☐ Dotknutí používatelia platobných služieb	☐ Výpadok služby	☐ Porušenie bezpečnosti siete alebo informačných	☐ Hospodársky vplyv	☐ Vysoká miera vnútornej eskalácie	☐ Iní potenciálne dotknutí poskytovatelia platobných služieb alebo relevantné infraštruktúry	☐ Poškodenie dobrého
Stručný a všeobecný opis incidentu						
Prípadný vplyv v iných členských štátoch EÚ						
Oznamovanie iným orgánom			Ak „Áno", uveďte:			
Dôvody oneskoreného predloženia úvodnej správy						

Priebežná správa

Správa o závažnom incidente

Priebežná správa	maximálne 3 pracovné dni od predloženia úvodnej správy	Obnoviť rozbaľovacie výbery

Dátum správy *(DD/MM/RRRR)* | Čas *(HH.MM)*

Referenčný kód incidentu

B – Priebežná správa

B1 – VŠEOBECNÉ ÚDAJE

Podrobnejší opis incidentu:		
Aký je konkrétny problém?		
Ako sa incident začal?		
Ako sa vyvíjal?		
Aké sú dôsledky (najmä pre používateľov platobných služieb)?		
Bol incident oznámený používateľom platobných služieb?		Ak „Áno", uveďte:
Súviselo to s predchádzajúcim incidentom (predchádzajúcimi incidentmi)?		Ak „Áno", uveďte:
Boli dotknutí alebo donútení zapojiť sa iní poskytovatelia služieb/tretie strany?		Ak „Áno", uveďte:
Začalo sa krízové riadenie (interné a/alebo externé)?		Ak „Áno", uveďte:
Dátum a čas začatia incidentu (ak sa už identifikoval) *(DD/MM/RRRR HH.MM)*		
Dátum a čas obnovenia po incidente alebo očakávaného obnovenia po incidente *(DD/MM/RRRR HH.MM)*		
Dotknuté oblasti funkcií	☐ Autentifikácia/autorizácia ☐ Priame preplatenie ☐ Komunikácia ☐ Nepriame preplatenie ☐ Zúčtovanie ☐ Ostatné	Ak „Iné", uveďte:
Zmeny vykonané na predchádzajúcich správach		

B2 – KLASIFIKÁCIA INCIDENTU/INFORMÁCIE O INCIDENTE

Dotknuté transakcie[2]	Úroveň vplyvu		
	Počet dotknutých transakcií		
	Ako % bežného počtu transakcií		
	Hodnota dotknutých transakcií v EUR		
	Trvanie incidentu (uplatňuje sa iba pre prevádzkové incidenty)		
	Poznámky:		
Dotknutí používatelia platobných služieb[3]	Úroveň vplyvu		
	Počet dotknutých používateľov platobných služieb		
	Ako % celkového počtu používateľov platobných služieb		
Porušenie bezpečnosti siete alebo informačných systémov		Opíšte, ako boli sieť alebo informačné systémy dotknuté	
Výpadok služby	Celkový výpadok služby:	Dni: Hodiny: Minúty:	
Hospodársky vplyv	Úroveň vplyvu		
	Priame náklady v EUR		
	Nepriame náklady v EUR		
Vysoká miera vnútornej eskalácie		Opíšte úroveň vnútornej eskalácie incidentu a uveďte, či sa v jej dôsledku spustil alebo sa pravdepodobne spustí krízový režim (alebo ekvivalentný), a ak áno, opíšte ho	
Iní potenciálne dotknutí poskytovatelia platobných služieb alebo relevantné infraštruktúry		Opíšte, ako mohol tento incident ovplyvniť iných poskytovateľov platobných služieb a/alebo infraštruktúry	
Poškodenie dobrého mena		Opíšte, ako mohol incident ovplyvniť dobré meno poskytovateľa platobných služieb (napríklad medializácia, zverejnenie právnych krokov alebo porušení práva...)	

B 3 – OPIS INCIDENTU

Typ incidentu		
Príčina incidentu	☐ Vyšetruje sa ☐ Škodlivé konanie ☐ Zlyhanie procesu ☐ Zlyhanie systému ☐ Chyba spôsobená človekom ☐ Externé udalosti ☐ Ostatné	Ak „Iné", uveďte:
Ovplyvnil vás incident priamo alebo nepriamo prostredníctvom poskytovateľa služieb?		Ak nepriamo, uveďte názov poskytovateľa služieb:

B 4 – VPLYV INCIDENTU

Celkový vplyv	☐ Integrita ☐ Dostupnosť	☐ Dôvernosť ☐ Hodnovernosť	
Dotknuté obchodné kanály	☐ Pobočky ☐ Elektronické bankovníctvo ☐ Elektronický obchod	☐ Telefónbanking ☐ Mobilné bankovníctvo ☐ Bankomaty	☐ Miesto predaja ☐ Ostatné
	Ak „Iné", uveďte:		
Dotknuté platobné služby	☐ Vloženie peňažných prostriedkov na platobný účet ☐ Výber peňažných prostriedkov z platobného účtu ☐ Operácie potrebné na prevádzku platobného účtu ☐ Získanie platobných nástrojov	☐ Úhrady ☐ Inkasá ☐ Platby kartou ☐ Vydávanie platobných nástrojov	☐ Poukázanie peňazí ☐ Platobné iniciačné ☐ Služby informovania o účte

B5 – ZMIERNENIE INCIDENTU

Ktoré činnosti/opatrenia boli zatiaľ uskutočnené alebo sa plánujú na obnovenie po incidente?	
Bol aktivovaný plán na zabezpečenie kontinuity činností a/alebo plán na obnovenie činnosti po havárii?	
Ak áno, kedy? *(DD/MM/RRRR, HH.MM)*	
Ak áno, opíšte ich	

Záverečná správa

Správa o závažnom incidente			
Zvoľte typ správy:		do 20 pracovných dní od predloženia priebežnej správy	Obnoviť rozbaľovacie výbery
Opíšte: (uplatňuje sa na incidenty preklasifikované na nezávažné)			
Dátum správy *(DD/MM/RRRR)*		Čas *(HH.MM)*	
Referenčný kód incidentu			

C – Záverečná správa						
Ak nebola odoslaná žiadna priebežná správa, vyplňte aj oddiel B						
C1 – VŠEOBECNÉ ÚDAJE						
Aktualizácia informácií z úvodnej správy a priebežnej správy (priebežných správ)						
Zmeny vykonané na predchádzajúcich správach						
Nejaké ďalšie relevantné informácie						
Uplatňujú sa všetky pôvodné kontroly?						
Ak „Nie", uveďte, ktoré kontroly sa neobnovili a aké ďalšie obdobie je potrebné na ich obnovenie						
C2 – ANALÝZA HLAVNÝCH PRÍČIN A NÁSLEDNÉ ČINNOSTI						
Aká bola hlavná príčina (ak je už známa)?	☐ Škodlivé konanie	☐ Zlyhanie procesu	☐ Zlyhanie systému	☐ Chyba spôsobená	☐ Externé udalosti	☐ Ostatné
Uveďte:	☐ Škodlivý kód ☐ Zhromažďovanie informácií ☐ Narušenia ☐ Útok typu distribuovaného odmietnutia služby/útok ☐ Premyslené interné akcie ☐ Premyslené externé fyzické poškodenie ☐ Bezpečnosť informačného obsahu ☐ Podvodné akcie ☐ Ostatné	☐ Nedostatočné monitorovanie a kontrola ☐ Problémy komunikácie ☐ Nesprávna činnosť ☐ Neprimerané riadenie zmien ☐ Neprimeranosť interných postupov a dokumentácie ☐ Otázky obnovy ☐ Ostatné	☐ Zlyhanie ☐ Zlyhanie siete ☐ Otázky databázy ☐ Zlyhanie softvéru/aplikácie ☐ Fyzické ☐ Ostatné	☐ Nezamýšľané ☐ Nečinnosť ☐ Nedostatočné zdroje ☐ Ostatné	☐ Zlyhanie dodávateľa/poskytovateľa technických služieb ☐ Vyššia moc ☐ Ostatné	
	Ak „Iné", uveďte:					
Ďalšie relevantné informácie o hlavnej príčine						
Hlavné nápravné opatrenia/opatrenia uskutočnené alebo plánované na zabránenie zopakovaniu incidentu v budúcnosti, ak sú už známe						
C3 – DOPLŇUJÚCE INFORMÁCIE						
Boli informácie o incidente oznámené ostatným poskytovateľom platobných služieb na informačné účely?	Ak „Áno", uveďte podrobnosti:					
Boli voči poskytovateľovi platobných služieb podniknuté právne kroky?	Ak „Áno", uveďte podrobnosti:					
Posúdenie účinnosti prijatých opatrení	Uveďte podrobnosti:					

POKYNY NA VYPLNENIE VZOROVÉHO FORMULÁRA

Poskytovatelia platobných služieb by mali vyplniť príslušný oddiel vzorového formulára v závislosti od fázy oznamovania, v ktorej sa nachádzajú: oddiel A pre úvodnú správu, oddiel B pre priebežné správy a oddiel C pre záverečnú správu. Poskytovatelia platobných služieb by mali použiť rovnaký vzorový formulár pri predkladaní úvodnej, priebežnej a záverečnej správy týkajúcej sa toho istého incidentu. Všetky polia sú povinné, ak nie je jednoznačne uvedené inak.

Nadpis

Úvodná správa: je to prvé oznámenie, ktoré poskytovateľ platobných služieb predkladá príslušnému orgánu v domovskom členskom štáte.

Priebežná správa: obsahuje podrobnejší opis incidentu a jeho dôsledkov. Je to aktualizácia úvodnej správy (a prípadne predchádzajúcej priebežnej správy) o tom istom incidente.

Záverečná správa: je to posledná správa, ktorú poskytovateľ platobných služieb zašle o incidente, keďže i) sa už vykonala analýza hlavných príčin a odhady sa môžu nahradiť reálnymi údajmi, alebo ii) incident sa už nepovažuje za závažný a je potrebné ho preklasifikovať.

Incident preklasifikovaný na nezávažný: incident už nespĺňa kritériá na to, aby sa považoval za závažný, a neočakáva sa, že ich bude do vyriešenia spĺňať. Poskytovatelia platobných služieb by mali vysvetliť dôvody tohto preklasifikovania.

Dátum a čas predloženia správy: presný dátum a čas predloženia správy príslušnému orgánu.

Referenčný kód incidentu (uplatniteľné pre priebežnú a záverečnú správu, ako aj pre aktualizácie úvodnej správy): referenčný kód vydaný príslušným orgánom v čase úvodnej správy na jednoznačnú identifikáciu incidentu. Každý príslušný orgán by mal zahrnúť ako predčíslie dvojmiestny ISO kód[2] svojho príslušného členského štátu.

A - Úvodná správa

A 1 - Všeobecné údaje

Typ správy:

Individuálna: správa sa týka jedného poskytovateľa platobných služieb.

Konsolidovaná: správa sa týka viacerých poskytovateľov platobných služieb v tom istom členskom štáte, ktorí sú dotknutí rovnakým závažným prevádzkovým alebo bezpečnostným incidentom a ktorí využívajú konsolidované oznamovanie. Polia v časti „Dotknutí poskytovatelia platobných služieb“ by sa mali ponechať prázdne (s výnimkou poľa „Krajina/krajiny dotknuté incidentom“) a v príslušnej tabuľke (Konsolidovaná správa – Zoznam poskytovateľov platobných služieb) by mal byť uvedený zoznam poskytovateľov platobných služieb, ktorí sú zahrnutí do správy.

Dotknutý poskytovateľ platobných služieb: je poskytovateľ platobných služieb, u ktorého došlo k incidentu.

Názov poskytovateľa platobných služieb: celý názov poskytovateľa platobných služieb, na ktorého sa vzťahuje postup oznamovania, ako je uvedený v platnom oficiálnom vnútroštátnom registri poskytovateľov platobných služieb.

Vnútroštátne identifikačné číslo poskytovateľa platobných služieb: jedinečné vnútroštátne identifikačné číslo, ktoré príslušný orgán v domovskom členskom štáte používa vo svojom vnútroštátnom registri na jednoznačnú identifikáciu poskytovateľa platobných služieb.

Vedúci skupiny: v prípade skupín subjektov, ako sú vymedzené v článku 4 bode 40 druhej smernice o platobných službách, uveďte názov vedúceho subjektu.

Krajina/krajiny dotknuté incidentom: krajina alebo krajiny, kde sa prejavil vplyv incidentu (dotknutých je napríklad niekoľko vetiev poskytovateľa platobných služieb so sídlom v rôznych

[2] Dvojmiestne abecedné kódy krajín podľa normy ISO-3166 sú dostupné na adrese https://www.iso.org/iso-3166-country-codes.html.

krajinách), bez ohľadu na závažnosť incidentu v inej krajine/krajinách. Môže, ale nemusí to byť domovský členský štát.

Primárna kontaktná osoba: meno a priezvisko osoby zodpovednej za oznámenie incidentu alebo v prípade, ak v mene dotknutého poskytovateľa platobných služieb incident oznamuje tretí poskytovateľ služieb, meno a priezvisko osoby zodpovednej za riadenie incidentov/útvaru pre riadenie rizika alebo podobnú oblasť u dotknutého poskytovateľa platobných služieb.

E-mail: e-mailová adresa, na ktorú je možné v prípade potreby zasielať žiadosti o ďalšie objasnenia. Môže to byť osobná alebo podniková e-mailová adresa.

Telefón: telefónne číslo, na ktoré je možné v prípade potreby smerovať žiadosti o ďalšie objasnenie. Môže to byť osobné alebo podnikové telefónne číslo.

Sekundárna kontaktná osoba: meno a priezvisko druhej osoby, na ktorú sa môže obrátiť príslušný orgán s otázkami o incidente, keď primárna kontaktná osoba nie je k dispozícii. Ak v mene dotknutého poskytovateľa platobných služieb poskytuje oznámenie tretí poskytovateľ služieb, meno a priezvisko druhej osoby zodpovednej za riadenie incidentov/útvaru pre riadenie rizika alebo podobnú oblasť u dotknutého poskytovateľa platobných služieb.

E-mail: e-mailová adresa druhej kontaktnej osoby, na ktorú je možné v prípade potreby zasielať žiadosti o ďalšie objasnenia. Môže to byť osobná alebo podniková e-mailová adresa.

Telefón: telefónne číslo druhej kontaktnej osoby, na ktoré je možné zavolať a v prípade potreby požiadať o ďalšie objasnenia. Môže to byť osobné alebo podnikové telefónne číslo.

Oznamujúci subjekt: tento oddiel by sa mal vyplniť v prípade, že tretia strana plní oznamovacie povinnosti v mene dotknutého poskytovateľa platobných služieb.

Názov oznamujúceho subjektu: celý názov subjektu, ktorý oznamuje incident, ako je uvedený v platnom oficiálnom vnútroštátnom obchodnom registri.

Vnútroštátne identifikačné číslo: jedinečné vnútroštátne identifikačné číslo, ktoré sa používa v krajine, kde má sídlo tretia strana, na jednoznačnú identifikáciu subjektu, ktorý oznamuje incident. Ak oznamujúca tretia strana je poskytovateľ platobných služieb, vnútroštátnym identifikačným číslom by malo byť jedinečné vnútroštátne identifikačné číslo poskytovateľa platobných služieb, ktoré používa príslušný orgán v domovskom členskom štáte vo svojom vnútroštátnom registri.

Primárna kontaktná osoba: meno a priezvisko osoby zodpovednej za oznamovanie incidentu.

E-mail: e-mailová adresa, na ktorú je možné v prípade potreby zasielať žiadosti o ďalšie objasnenia. Môže to byť osobná alebo podniková e-mailová adresa.

Telefón: telefónne číslo, na ktoré je možné v prípade potreby smerovať žiadosti o ďalšie objasnenie. Môže to byť osobné alebo podnikové telefónne číslo.

Sekundárna kontaktná osoba: meno a priezvisko druhej osoby v subjekte, ktorý oznamuje incident, na ktorú sa môže obrátiť príslušný orgán, keď primárna kontaktná osoba nie je k dispozícii.

E-mail: e-mailová adresa druhej kontaktnej osoby, na ktorú je možné v prípade potreby zasielať žiadosti o ďalšie objasnenia. Môže to byť osobná alebo podniková e-mailová adresa.

Telefón: telefónne číslo druhej kontaktnej osoby, na ktoré je možné zavolať a v prípade potreby požiadať o ďalšie objasnenia. Môže to byť osobné alebo podnikové telefónne číslo.

A 2 - Zistenie a klasifikácia incidentu

Dátum a čas zistenia incidentu: dátum a čas prvého zistenia incidentu.

Dátum a čas klasifikácie incidentu: dátum a čas, keď bol bezpečnostný alebo prevádzkový incident klasifikovaný ako závažný.

Incident zistil subjekt: uveďte, či incident zistil používateľ platobných služieb v rámci poskytovateľa platobných služieb (napríklad funkcia vnútorného auditu) alebo iná externá strana (napríklad poskytovateľ služieb). Ak to nebol nik z uvedených, vysvetlite to v príslušnom poli.

Typ incidentu: uveďte, či podľa vašich najlepších vedomostí, a ak sú príslušné informácie k dispozícii, ide o prevádzkový alebo bezpečnostný incident.

> **Prevádzkový:** incident vyplývajúci z nevhodných procesov či systémov alebo procesov či systémov, ktoré zlyhali, z ľudskej chyby alebo udalostí vyššej moci, ktoré ovplyvňujú integritu, dostupnosť, dôvernosť a/alebo hodnovernosť služieb súvisiacich s platbami.
>
> **Bezpečnostný:** neoprávnený prístup, neoprávnené použitie, zverejnenie, narušenie, úprava alebo zničenie aktív poskytovateľa platobných služieb, ktoré ovplyvňujú integritu, dostupnosť, dôvernosť a/alebo hodnovernosť služieb súvisiacich s platbami. To sa môže stať, okrem iného, keď u poskytovateľa platobných služieb dôjde k porušeniu bezpečnosti siete alebo informačných systémov.

Kritériá vedúce k správe o závažnom incidente: uveďte, ktoré kritériá viedli k správe o závažnom incidente. Sú viaceré možnosti výberu kritérií: dotknuté transakcie, dotknutí používatelia platobných služieb, výpadok služby, porušenie bezpečnosti siete alebo informačných systémov, hospodársky vplyv, vysoká miera vnútornej eskalácie, iní potenciálne dotknutí poskytovatelia platobných služieb alebo relevantné infraštruktúry a/alebo poškodenie dobrého mena.

Stručný a všeobecný opis incidentu: stručne vysvetlite najdôležitejšie otázky týkajúce sa incidentu, jeho možných príčin, bezprostredných vplyvov atď.

Prípadný vplyv v iných členských štátoch EÚ: vysvetlite stručne, aký vplyv mal incident v inom členskom štáte EÚ (napríklad na používateľov platobných služieb, poskytovateľov platobných služieb a/alebo platobnú infraštruktúru). Ak je to zvládnuteľné v rámci termínov oznamovania, poskytnite preklad do angličtiny.

Oznamovanie iným orgánom: uveďte, či incident bol/bude oznámený iným orgánom v osobitnom rámci oznamovania incidentov, ako je to známe v čase oznamovania. Ak áno, uveďte príslušné orgány.

Dôvody oneskoreného predloženia úvodnej správy: vysvetlite dôvody, prečo ste na klasifikáciu incidentu potrebovali dlhší čas než 24 hodín.

B Priebežná správa

B 1 – Všeobecné údaje

Podrobnejší opis incidentu: opíšte hlavné charakteristiky incidentu a uveďte prinajmenšom informácie o konkrétnom prípade a súvisiacom pozadí, opis, ako sa incident začal a ako sa vyvíjal, a dôsledky najmä pre používateľov platobných služieb atď. Poskytnite aj informácie o prípadnej komunikácii s používateľmi platobných služieb.

Súviselo to s predchádzajúcim incidentom (predchádzajúcimi incidentmi)?: uveďte, či incident súvisí s predchádzajúcimi incidentmi, ak je taká informácia k dispozícii. Ak incident súvisí s predchádzajúcimi incidentmi, uveďte s ktorými.

Boli dotknutí alebo donútení zapojiť sa iní poskytovatelia služieb/tretie strany?: uveďte, či sa incident dotkol alebo donútil zapojiť sa iných poskytovateľov služieb/tretie strany, ak je taká informácia k dispozícii. Ak boli incidentom dotknutí alebo donútení zapojiť sa iní poskytovatelia služieb/tretie strany, uveďte ich zoznam a poskytnite viac informácií.

Začalo sa krízové riadenie (interné a/alebo externé)?: uveďte, či sa začalo krízové riadenie (interné a/alebo externé). Ak sa krízové riadenie začalo, poskytnite viac informácií.

Dátum a čas začatia incidentu: dátum a čas začatia incidentu, ak je známy.

Dátum a čas obnovy alebo očakávanej obnovy po incidente: uveďte dátum a čas, kedy incident bol alebo sa očakáva, že bude opäť pod kontrolou a ekonomická činnosť sa vrátila alebo sa očakáva, že sa vráti do normálneho stavu.

Dotknuté oblasti funkcií: uveďte krok alebo kroky platobného procesu, ktoré boli dotknuté incidentom, ako je autentifikácia/autorizácia, komunikácia, zúčtovanie, priame vyrovnanie, nepriame vyrovnanie a ďalšie.

Autentifikácia/autorizácia: postupy, ktorými sa poskytovateľovi platobných služieb umožňuje overenie identity používateľa platobných služieb alebo platnosti používania konkrétneho platobného nástroja vrátane používania personalizovaných bezpečnostných prvkov používateľa a používateľa platobných služieb (alebo tretej strany konajúcej v jeho mene) poskytujúceho súhlas s prevodom prostriedkov.

Komunikácia: tok informácií na účely identifikácie, autentifikácie, oznamovania a informovania medzi poskytovateľmi platobných služieb poskytujúcimi služby k účtom a poskytovateľmi služieb iniciovania platieb, poskytovateľmi služieb informovania o účtoch, platiteľmi, príjemcami platieb a inými poskytovateľmi platobných služieb.

Zúčtovanie: proces prevodu, odsúhlasenia a v niektorých prípadoch potvrdenia príkazov na úhradu pred vyrovnaním vrátane započítania príkazov a určenia konečných stavov na vyrovnanie.

Priame vyrovnanie: dokončenie transakcie alebo spracovania s cieľom zbaviť účastníkov povinností počas prevodu prostriedkov, ak túto činnosť vykonáva samotný dotknutý poskytovateľ platobných služieb.

Nepriame vyrovnanie: dokončenie transakcie alebo spracovania s cieľom zbaviť účastníkov povinností počas prevodu prostriedkov, ak túto činnosť vykonáva iný poskytovateľ platobných služieb v mene dotknutého poskytovateľa platobných služieb.

Iná: dotknutá oblasť funkcie je iná ako boli uvedené. Ďalšie podrobnosti uveďte do poľa s voľným textom.

Zmeny vykonané na predchádzajúcich správach: uveďte vykonané zmeny informácií poskytnutých v predchádzajúcich správach týkajúcich sa toho istého incidentu (napríklad v úvodnej správe alebo prípadne v priebežnej správe).

B 2 – Klasifikácia incidentu/informácie o incidente

Dotknuté transakcie: Poskytovatelia platobných služieb by mali uviesť, aké prahové úrovne incident dosiahol alebo pravdepodobne dosiahne (ak existujú), ako aj súvisiace údaje: počet dotknutých transakcií, percentuálny podiel dotknutých transakcií vo vzťahu k počtu platobných transakcií vykonávaných tými istými platobnými službami, ktoré boli dotknuté incidentom, a celková hodnota transakcií. Poskytovatelia platobných služieb by mali uviesť konkrétne hodnoty týchto premenných, ktorými môžu byť skutočné údaje alebo odhady. Vo všeobecnosti platí, že poskytovatelia platobných služieb by mali pod pojmom „dotknutá transakcia“ chápať všetky domáce a cezhraničné transakcie, ktoré boli alebo pravdepodobne budú priamo či nepriamo dotknuté incidentom, a najmä tie transakcie, ktoré nebolo možné iniciovať alebo spracovať, transakcie, v prípade ktorých bol zmenený obsah platobnej správy, a transakcie, pre ktoré bol príkaz vystavený podvodne (či už prostriedky boli, alebo neboli získané späť). Poskytovatelia platobných služieb by mali okrem toho chápať bežnú úroveň platobných transakcií ako ročný denný priemer domácich a cezhraničných platobných transakcií vykonávaných tými istými platobnými službami, ktoré boli dotknuté incidentom, pričom za referenčné obdobie výpočtov sa považuje predchádzajúci rok. Ak poskytovatelia platobných služieb nepovažujú tento údaj za reprezentatívny (napríklad z dôvodu sezónnosti), mali by použiť inú, reprezentatívnejšiu metriku a príslušnému orgánu oznámiť zdôvodnenie tohto prístupu v poli „Poznámky“. V prípadoch, keď sú incidentom dotknuté platobné transakcie v menách iných ako euro, pri výpočte prahových hodnôt a oznamovaní hodnoty dotknutých transakcií, by mali poskytovatelia platobných služieb sumu transakcií v mene inej ako euro previesť na euro s použitím denného referenčného výmenného kurzu ECB na deň predchádzajúci dňu predloženia úvodnej správy.

Dotknutí používatelia platobných služieb: Poskytovatelia platobných služieb by mali uviesť, aké prahové úrovne incident dosiahol alebo pravdepodobne dosiahne (ak existujú), ako aj súvisiace údaje: celkový počet používateľov platobných služieb, ktorí boli dotknutí incidentom, a percentuálny podiel dotknutých používateľov platobných služieb vo vzťahu k celkovému počtu používateľov platobných

služieb. Poskytovatelia platobných služieb by mali uviesť konkrétne hodnoty týchto premenných, ktorými môžu byť skutočné údaje alebo odhady. Poskytovatelia platobných služieb by mali pod pojmom „dotknutí používatelia platobných služieb“ rozumieť všetkých zákazníkov (domácich alebo zahraničných, spotrebiteľov alebo spoločnosti), ktorí majú zmluvu s dotknutým poskytovateľom platobných služieb, ktorá im zaručuje prístup k dotknutej platobnej službe, a ktorí utrpeli alebo pravdepodobne utrpia škody v dôsledku incidentu. Poskytovatelia platobných služieb by sa mali pri určovaní počtu používateľov platobných služieb, ktorí počas trvania incidentu mohli používať platobnú službu, vrátiť k odhadom vyplývajúcim z minulej činnosti. V prípade skupín by mal každý poskytovateľ platobných služieb vziať do úvahy iba vlastných používateľov platobných služieb. V prípade, že poskytovateľ platobných služieb ponúka prevádzkové služby ostatným, mal by vziať do úvahy iba vlastných používateľov platobných služieb (ak existujú) a aj poskytovatelia platobných služieb, ktorí sú príjemcami týchto prevádzkových služieb, by mali posúdiť incident vo vzťahu k vlastným používateľom platobných služieb. Poskytovatelia platobných služieb by mali okrem toho za celkový počet používateľov platobných služieb považovať súhrnný údaj o domácich a cezhraničných používateľoch platobných služieb, s ktorými sú zmluvne viazaní v čase incidentu (alebo najnovší dostupný údaj) a ktorí majú prístup k dotknutej platobnej službe, a to bez ohľadu na ich veľkosť alebo na to, či sa považujú za aktívnych alebo pasívnych používateľov platobných služieb.

Porušenie bezpečnosti siete alebo informačných systémov: Poskytovatelia platobných služieb by mali určiť, či nejaké škodlivé konanie oslabilo dostupnosť, hodnovernosť, integritu alebo dôvernosť siete alebo informačných systémov (vrátane údajov) súvisiacich s poskytovaním platobných služieb.

Výpadok služby: Poskytovatelia platobných služieb by mali uviesť, či sa pri incidente dosiahla alebo pravdepodobne dosiahne prahová hodnota, ako aj súvisiaci údaj: celkovú dĺžku výpadku služby. Poskytovatelia platobných služieb by mali uviesť konkrétne hodnoty tejto premennej, ktorými môžu byť skutočné údaje alebo odhady. Poskytovatelia platobných služieb by mali zohľadniť časové obdobie, počas ktorého sa zaznamenal alebo pravdepodobne zaznamená výpadok úlohy, procesu alebo kanálu v súvislosti s poskytovaním platobných služieb, a tým zabrániť i) iniciovaniu a/alebo vykonaniu platobnej služby, a/alebo ii) prístupu k platobnému účtu. Poskytovatelia platobných služieb by mali počítať čas výpadku služby od chvíle jeho začatia a mali by zohľadniť časové intervaly, počas ktorých vykonávajú svoje činnosti potrebné na realizáciu platobných služieb, a v prípade potreby aj obdobia, keď majú zatvorené a keď sa vykonáva údržba. Ak poskytovatelia platobných služieb nie sú schopní určiť, kedy sa výpadok služby začal, mali by výnimočne čas výpadku služby počítať od chvíle zistenia výpadku.

Hospodársky vplyv: Poskytovatelia platobných služieb by mali uviesť, či sa pri incidente dosiahla alebo pravdepodobne dosiahne prahová hodnota, ako aj súvisiace údaje: priame a nepriame náklady. Poskytovatelia platobných služieb by mali uviesť konkrétne hodnoty týchto premenných, ktorými môžu byť skutočné údaje alebo odhady. Poskytovatelia platobných služieb by mali zohľadniť náklady, ktoré sa incidentu týkajú priamo, ale aj tie, ktoré sa ho týkajú nepriamo. Poskytovatelia platobných služieb by mali okrem iného zohľadniť vyvlastnené finančné prostriedky alebo aktíva, reprodukčnú obstarávaciu cenu hardvéru alebo softvéru, ďalšie forenzné náklady alebo náklady na nápravu, poplatky za nedodržanie zmluvných povinností, sankcie, externé záväzky a straty príjmov. Pokiaľ ide o nepriame náklady, poskytovatelia platobných služieb by mali zohľadniť iba tie z nich, ktoré sú už známe alebo veľmi pravdepodobne vzniknú. V prípadoch, keď sú náklady v menách iných ako euro, pri výpočte prahovej hodnoty a oznamovaní hodnoty hospodárskeho vplyvu by mali poskytovatelia platobných služieb sumu nákladov v mene inej ako euro previesť na euro s použitím denného referenčného výmenného kurzu ECB na deň predchádzajúci dňu predloženia úvodnej správy.

> **Priame náklady:** náklady (v eurách), ktoré priamo spôsobil incident, vrátane nákladov na nápravu incidentu (napríklad vyvlastnené finančné prostriedky alebo aktíva, reprodukčná obstarávacia cenu hardvéru a softvéru, poplatky za nedodržanie zmluvných povinností).

Nepriame náklady: náklady (v eurách), ktoré nepriamo spôsobil incident (napríklad náklady na odškodnenie zákazníka/kompenzáciu pre zákazníka, potenciálne náklady na právne služby).

Vysoká miera vnútornej eskalácie: Poskytovatelia platobných služieb by mali zohľadniť, či v dôsledku vplyvu na služby súvisiace s platbami riadiaci orgán, ako je vymedzený v usmerneniach orgánu EBA o riadení rizika v oblasti IKT a bezpečnosti, bol alebo pravdepodobne bude, v súlade s usmernením 60 d) usmernení EBA o riadení rizika v oblasti IKT a bezpečnosti, informovaný o incidente mimo akéhokoľvek postupu pravidelného oznamovania a priebežne počas celého trvania incidentu. Poskytovatelia platobných služieb by mali okrem toho zohľadniť, či sa v dôsledku vplyvu incidentu na služby súvisiace s platbami spustil alebo pravdepodobne spustí krízový režim.

Iní potenciálne dotknutí poskytovatelia platobných služieb alebo relevantné infraštruktúry: Poskytovatelia platobných služieb by mali posúdiť vplyv incidentu na finančný trh, pod ktorým sa rozumejú infraštruktúry finančných trhov a/alebo platobné schémy, ktoré to, ako aj ostatných poskytovateľov platobných služieb podporujú. Poskytovatelia platobných služieb by mali posúdiť, či sa incident zopakoval alebo je pravdepodobné, že sa zopakuje, v prípade ostatných poskytovateľov platobných služieb, či mal vplyv alebo pravdepodobne bude mať vplyv na bezproblémové fungovanie infraštruktúr finančných trhov a či ohrozil alebo pravdepodobne ohrozí pevnosť finančného systému ako celku. Poskytovatelia platobných služieb by nemali zabúdať na rôzne rozmery incidentu, ako napríklad to, či sú dotknuté súčasti/dotknutý softvér proprietárne alebo všeobecne dostupné, či je ohrozená sieť interná alebo externá a či poskytovateľ platobných služieb prestal alebo pravdepodobne prestane plniť svoje povinnosti v rámci infraštruktúr finančných trhov, ktorých je členom.

Poškodenie dobrého mena: Poskytovatelia platobných služieb by mali zvážiť úroveň viditeľnosti, ktorú podľa ich najlepšieho vedomia incident dosiahol alebo pravdepodobne dosiahne na trhu. Poskytovatelia platobných služieb by mali zvážiť pravdepodobnosť, že incident spôsobí spoločnosti ujmu, čo je dobrým ukazovateľom schopnosti poškodiť ich dobré meno. Poskytovatelia platobných služieb by mali zohľadniť, i) či sa používatelia platobných služieb a/alebo iní poskytovatelia platobných služieb sťažovali na nepriaznivý vplyv incidentu; ii) či incident ovplyvnil viditeľný proces súvisiaci s platobnou službou a či preto pravdepodobne získa alebo už získal pozornosť médií (do úvahy treba brať nielen tradičné médiá, ako sú noviny, ale aj blogy, sociálne siete atď., pričom pozornosť médií v tejto súvislosti neznamená len niekoľko negatívnych komentárov od záujemcov, mala by sa objaviť seriózna správa alebo značný počet negatívnych komentárov/výstrah; iii) či neboli alebo pravdepodobne nebudú dodržané zmluvné povinnosti, čo povedie k zverejneniu právnych krokov voči poskytovateľovi platobných služieb; iv) či neboli splnené regulačné požiadavky, čo povedie k opatreniam dohľadu alebo sankciám, ktoré sú alebo pravdepodobne budú verejne dostupné; alebo v) či sa podobný druh incidentu stal už predtým.

B 3 – Opis incidentu

Typ incidentu: prevádzkový alebo bezpečnostný. Podrobnejšie vysvetlenie je uvedené v príslušnom poli úvodnej správy.

Príčina incidentu: uveďte príčinu incidentu, a ak nie je zatiaľ známa, najpravdepodobnejšiu príčinu. Vybrať možno viaceré možnosti.

Vyšetruje sa: začiarknite toto políčko, ak je príčina v súčasnosti neznáma.

Škodlivé konanie: akcie úmyselne zamerané na poskytovateľov platobných služieb. Ide o škodlivý kód, zhromažďovanie informácií, prieniky, distribuovaný útok na vyradenie služby (DDOS), premyslené interné akcie, premyslené externé fyzické poškodenie, bezpečnosť informačného obsahu, podvodné akcie a ďalšie. Viac podrobností je uvedených v oddiele C2 tohto vzorového formulára.

Zlyhanie procesu: príčinou incidentu bol chybný návrh alebo vykonanie platobného procesu, kontrol procesu a/alebo podporných procesov (napríklad procesu zmeny/migrácie, testovania, konfigurácie, kapacity, monitorovania).

Zlyhanie systému: príčina incidentu súvisí s nedostatočným návrhom, vykonaním, zložkami, špecifikáciami, integráciou alebo zložitosťou systémov, sietí, infraštruktúr a databáz, ktoré podporujú platobnú činnosť.

Ľudské chyby: incident bol spôsobený neúmyselnou chybou človeka, či už v rámci platobného rozkazu (napríklad nahratie nesprávneho hromadného platobného príkazu do systému prevodov finančných prostriedkov), alebo v súvislosti s ním (napríklad náhodný výpadok prúdu a odloženie platobnej činnosti).

Externé udalosti: príčina súvisí s udalosťami, ktoré vo všeobecnosti vznikli mimo priamej kontroly organizácie (napríklad prírodné katastrofy, zlyhanie poskytovateľa technických služieb).

Iné: príčina incidentu je iná, ako boli uvedené. Ďalšie podrobnosti uveďte do poľa s voľným textom.

Ovplyvnil vás incident priamo alebo nepriamo prostredníctvom poskytovateľa služieb?: uveďte, či incident zasiahol poskytovateľa platobných služieb priamo alebo ho ovplyvňuje nepriamo prostredníctvom tretej strany, ak je taká informácia k dispozícii. V prípade nepriameho vplyvu uveďte názov poskytovateľa (poskytovateľov) služieb.

B 4 – Vplyv incidentu

Celkový vplyv: uveďte, ktoré rozmery boli dotknuté prevádzkovým alebo bezpečnostným incidentom. Vybrať možno viaceré možnosti.

Integrita: vlastnosť, ktorá znamená, že je zabezpečená presnosť a úplnosť aktív (vrátane údajov).

Dostupnosť: vlastnosť, ktorá znamená, že služby súvisiace s platbami sú prístupné používateľom platobných služieb a títo používatelia ich môžu využívať, podľa vopred vymedzených prípustných úrovní.

Dôvernosť: vlastnosť, ktorá znamená, že informácie sa nezverejnia ani nesprístupnia neoprávneným osobám, subjektom či procesom.

Hodnovernosť: vlastnosť, ktorá znamená, že zdroj je naozaj tým, za čo sa vydáva.

Dotknuté obchodné kanály: uveďte kanál alebo kanály interakcie s používateľmi platobných služieb, ktoré boli incidentom dotknuté. Možno začiarknuť viacero políčok.

Pobočky: miesto podnikania (iné než ústredie), ktoré je súčasťou poskytovateľa platobných služieb, nemá právnu subjektivitu a vykonáva priamo niektoré alebo všetky transakcie viažuce sa na ekonomickú činnosť poskytovateľa platobných služieb. Všetky miesta podnikania zriadené v tom istom členskom štáte poskytovateľom platobných služieb s ústredím v inom členskom štáte by sa mali považovať za jedinú pobočku.

Elektronické bankovníctvo: používanie počítačov na vykonávanie finančných transakcií cez internet.

Telefónbanking: používanie telefónov na vykonávanie finančných transakcií.

Mobilné bankovníctvo: používanie osobitnej bankovej aplikácie na smartfóne alebo podobnom zariadení určenom na vykonávanie finančných transakcií.

Bankomaty: elektromechanické zariadenia, ktoré umožňujú používateľom platobných služieb vyberať hotovosť zo svojich účtov a/alebo získavať prístup k iným službám.

Miesto predaja: fyzické priestory obchodníka, v ktorých sa iniciuje platobná transakcia.

Elektronický obchod: platobná transakcia sa iniciuje na virtuálnom mieste predaja (napríklad platby iniciované prostredníctvom internetu s použitím prenosu kreditov, platobných kariet, prevodu elektronických peňazí medzi účtami elektronických peňazí).

Iný: dotknutý obchodný kanál je iný ako boli uvedené. Ďalšie podrobnosti uveďte do poľa s voľným textom.

Dotknuté platobné služby: uveďte platobné služby, ktoré v dôsledku incidentu správne nefungujú. Možno začiarknuť viacero políčok.

Vloženie peňažných prostriedkov na platobný účet: odovzdanie peňažných prostriedkov poskytovateľovi platobných služieb, ktorý ich pripíše na platobný účet.

Výber peňažných prostriedkov z platobného účtu: požiadavka na poskytnutie peňažných prostriedkov a zaťaženie platobného účtu zodpovedajúcou sumou, ktorú dostane poskytovateľ platobných služieb od používateľa platobných služieb.

Operácie potrebné na prevádzku platobného účtu: činnosti potrebné na aktivovanie, deaktivovanie a/alebo správu (napríklad otváranie, blokovanie) platobného účtu.

Získanie platobných nástrojov: platobná služba pozostávajúca zo zmluvy medzi poskytovateľom platobných služieb a príjemcom platby na prijatie a spracovanie platobných transakcií, ktorej výsledkom je prevod prostriedkov príjemcovi platby.

Úhrady: platobná služba na uhrádzanie platieb poskytovateľom platobných služieb, u ktorého má platiteľ platobný účet, na platobný účet príjemcu platby prostredníctvom platobnej transakcie alebo série platobných transakcií z platobného účtu platiteľa na základe pokynu platiteľa.

Inkaso: platobná služba na zaťaženie platobného účtu platiteľa v prípade, ak platobnú transakciu v prospech poskytovateľa platobných služieb alebo vlastného poskytovateľa platobných služieb platiteľa iniciuje príjemca platby na základe súhlasu platiteľa vydaného príjemcovi platby.

Platby kartou: platobná služba založená na infraštruktúre a obchodných pravidlách kartovej schémy, ktorej cieľom je vykonať platobnú transakciu kartou, telekomunikačným, digitálnym alebo IT zariadením alebo softvérom, ktorej výsledkom je transakcia uskutočnená debetnou alebo kreditnou kartou. K platobným transakciám viazaným na kartu nepatria transakcie založené na iných druhoch platobných služieb.

Vydávanie platobných nástrojov: platobná služba pozostávajúca zo zmluvy medzi poskytovateľom platobných služieb a platiteľom na poskytnutie platobného nástroja slúžiaceho na iniciovanie a spracovanie platobných transakcií platiteľa.

Poukázanie peňazí: platobná služba, v rámci ktorej sa prostriedky prijmú od platiteľa bez vytvorenia platobného účtu v mene platiteľa alebo príjemcu platby s jediným cieľom previesť zodpovedajúcu sumu príjemcovi platby alebo na iného poskytovateľa platobných služieb konajúceho v mene príjemcu platby, a/alebo v rámci ktorej sa tieto prostriedky získajú v mene príjemcu platby, ktorému sa sprístupnia.

Platobné iniciačné služby: platobné služby na iniciovanie platobného príkazu na žiadosť používateľa platobnej služby vo vzťahu k platobnému účtu u iného poskytovateľa platobných služieb.

Služby informovania o účte: služby online platieb na poskytovanie konsolidovaných informácií o jednom alebo viacerých platobných účtoch používateľa platobných služieb u iného poskytovateľa platobných služieb alebo viacerých poskytovateľov platobných služieb.

B 5 – Zmiernenie incidentu

Aké činnosti/opatrenia boli zatiaľ uskutočnené alebo sa plánujú na obnovenie po incidente?: uveďte podrobné informácie o činnostiach, ktoré boli uskutočnené alebo sa plánujú uskutočniť na dočasné riešenie incidentu.

Boli aktivované plány na zabezpečenie kontinuity činností a/alebo plány na obnovenie činnosti po havárii?: uveďte, či to tak bolo, a ak áno, uveďte najrelevantnejšie podrobnosti o tom, čo sa stalo (t. j. kedy boli aktivované a z čoho pozostávali).

C – Záverečná správa

C 1 – Všeobecné údaje

Aktualizácia informácií z úvodnej správy a priebežnej správy (priebežných správ) (súhrn): uveďte ďalšie informácie o incidente vrátane konkrétnych zmien vykonaných v informáciách poskytnutých v priebežnej správe. Uveďte aj akékoľvek iné relevantné informácie.

Uplatňujú sa všetky pôvodné kontroly?: uveďte, či poskytovateľ platobných služieb zrušil alebo oslabil niektoré kontroly kedykoľvek počas incidentu. Ak áno, uveďte, či sa všetky kontroly opäť uplatňujú, a ak nie, vysvetlite v poli s voľným textom, ktoré kontroly sa neobnovili a aké ďalšie obdobie je potrebné na ich obnovenie.

C 2 – Analýza hlavných príčin a následné činnosti

Aká bola hlavná príčina, ak je už známa?: uveďte, aká je hlavná príčina incidentu, alebo ak nie je zatiaľ známa, najpravdepodobnejšiu príčinu. Vybrať možno viaceré možnosti. (Vezmite do úvahy, že hlavná príčina by sa mala odlišovať od vplyvu incidentu.)

Škodlivé konanie: externé alebo interné akcie úmyselne zamerané na poskytovateľov platobných služieb. Rozdeľujú sa do týchto kategórií:

Škodlivý kód: napríklad vírus, červ, trójsky kôň, sledovací softvér.

Zhromažďovanie informácií: napríklad skenovanie, odpočúvanie (sniffing), sociálne inžinierstvo.

Prieniky: napríklad privilegovaný kompromis účtov, neprivilegovaný kompromis účtov, kompromis aplikácie, bot.

Útok typu distribuovaného odmietnutia služby/útok zahltením servera služby (D/DoS): pokus o zneprístupnenie online služby zahltením služby požiadavkami z viacerých zdrojov.

Premyslené interné akcie: napríklad sabotáž, krádež.

Premyslené externé fyzické poškodenie: napríklad sabotáž, fyzický útok na zariadenia/dátové centrá.

Bezpečnosť informačného obsahu: neoprávnený prístup k informáciám, neoprávnená úprava informácií.

Podvodné akcie: neoprávnené využívanie zdrojov, copyright, masquerade, phishing.

Iná (uveďte): príčina incidentu je iná, ako boli uvedené. Ďalšie podrobnosti uveďte do poľa s voľným textom.

Zlyhanie procesu: príčinou incidentu bol chybný návrh alebo vykonanie platobného procesu, kontrol procesu a/alebo podporných procesov (napríklad procesu zmeny/migrácie, testovania, konfigurácie, kapacity, monitorovania). Rozdeľujú sa do týchto kategórií:

Nedostatočné monitorovanie a kontrola: napríklad v súvislosti s prebiehajúcimi operáciami, dátumami uplynutia platnosti osvedčenia, dátumami uplynutia platnosti licencie, dátumami uplynutia platnosti dočasných úprav, definovanými maximálnymi hodnotami počítadla, úrovňami naplnenia databázy, správou práv používateľov, zásadou duálnej kontroly.

Problémy komunikácie: napríklad medzi účastníkmi trhu alebo v rámci organizácie.

Nesprávna činnosť: napríklad chýbajúca výmena osvedčení, zásobník je plný.

Nedostatočné riadenie zmien: napríklad nezistené chyby v konfigurácii, uvoľnenie vrátane aktualizácií, problémy údržby, neočakávané chyby.

Neprimeranosť interných postupov a dokumentácie: napríklad nedostatočná transparentnosť, pokiaľ ide o funkčnosť, postupy a výskyt zlyhávania, chýbajúca dokumentácia.

Otázky obnovy: napríklad riadenie nepredvídaných udalostí, neprimeraná redundancia.

Iná (uveďte): príčina incidentu je iná, ako boli uvedené. Ďalšie podrobnosti uveďte do poľa s voľným textom.

Zlyhanie systému: príčina incidentu súvisí s nedostatočným návrhom, vykonaním, zložkami, špecifikáciami, integráciou alebo zložitosťou systémov, sietí, infraštruktúr a databáz, ktoré podporujú platobnú činnosť. Rozdeľujú sa do týchto kategórií:

Zlyhanie hardvéru: zlyhanie zariadenia fyzickej technológie, ktoré vykonáva postupy a/alebo ukladá údaje potrebné pre poskytovateľov platobných služieb na vykonávanie ich činnosti spojenej s platbami (napríklad zlyhanie pevných diskov, dátových centier, ďalšej infraštruktúry).

Zlyhanie siete: zlyhanie telekomunikačných sietí, verejných alebo súkromných, ktoré umožňujú výmenu dát a informácií (napríklad cez internet) počas platobného procesu.

Otázky databázy: údajová štruktúra, v ktorej sa ukladajú osobné údaje a informácie o platbách na realizáciu platobných transakcií.

Zlyhanie softvéru/aplikácie: zlyhania programov, operačných systémov atď., ktoré podporujú poskytovanie platobných služieb poskytovateľa platobných služieb (napríklad zlyhania, neznáme funkcie).

Fyzické poškodenie: napríklad neúmyselné poškodenie spôsobené nevhodnými podmienkami, konštrukčnou prácou.

Iné (uveďte podrobnosti): príčina incidentu je iná, ako boli uvedené. Ďalšie podrobnosti uveďte do poľa s voľným textom.

Ľudská chyba: incident bol spôsobený neúmyselnou chybou človeka, či už v rámci platobného rozkazu (napríklad nahratie nesprávneho hromadného platobného príkazu do systému prevodov finančných prostriedkov), alebo v súvislosti s ním (napríklad náhodný výpadok prúdu a odloženie platobnej činnosti). Rozdeľujú sa do týchto kategórií:

Nezamýšľané: napríklad chyby, omyly, opomenutia, nedostatok skúseností a znalostí.

Nečinnosť: napríklad v dôsledku nedostatku zručností, znalostí, skúseností, informovanosti.

Nedostatočné zdroje: napríklad chýbajúce ľudské zdroje, dostupnosť zamestnancov.

Iné (uveďte podrobnosti): príčina incidentu je iná, ako boli uvedené. Ďalšie podrobnosti uveďte do poľa s voľným textom.

Externá udalosť: príčina sa spája s udalosťami spravidla mimo kontroly organizácie. Rozdeľujú sa do týchto kategórií:

Zlyhanie dodávateľa/poskytovateľa technických služieb: napríklad výpadok elektrickej energie, výpadok internetu, právne problémy, obchodné problémy, závislosť od služieb.

Vyššia moc: napríklad zlyhanie elektrickej energie, požiare, prírodné príčiny ako zemetrasenia, silné zrážky, silný vietor.

Iné (uveďte podrobnosti): príčina incidentu je iná, ako boli uvedené. Ďalšie podrobnosti uveďte do poľa s voľným textom.

Iné: príčina incidentu je iná, ako boli uvedené. Ďalšie podrobnosti uveďte do poľa s voľným textom.

Ďalšie relevantné informácie o hlavnej príčine: poskytnite akékoľvek ďalšie podrobnosti o hlavnej príčine vrátane predbežných záverov vyplývajúcich z analýzy hlavnej príčiny.

Hlavné nápravné opatrenia/opatrenia uskutočnené alebo plánované na zabránenie zopakovaniu incidentu v budúcnosti, ak sú známe: opíšte hlavné činnosti, ktoré boli uskutočnené alebo sa plánujú na zabránenie zopakovaniu incidentu v budúcnosti.

C 3 – Doplňujúce informácie

Boli informácie o incidente poskytnuté ostatným poskytovateľom platobných služieb na informačné účely?: Uveďte prehľad poskytovateľov platobných služieb, či už formálne, alebo neformálne, oslovených s cieľom informovať ich o incidente, poskytnite podrobnosti o tom, ktorí poskytovatelia platobných služieb boli informovaní, ktoré informácie im boli oznámené, a aké sú hlavné dôvody na výmenu týchto informácií.

Bol voči poskytovateľovi platobných služieb podaný návrh na začatie konania?: Uveďte, či boli v dôsledku incidentu voči poskytovateľovi platobných služieb v čase vyplnenia záverečnej správy podniknuté právne kroky (napríklad bola vec odovzdaná súdu alebo prišiel o licenciu).

Posúdenie účinnosti prijatých opatrení: uveďte prípadne vlastné posúdenie účinnosti opatrení prijatých počas trvania incidentu vrátane akýchkoľvek poznatkov získaných z incidentu.