EBA/GL/2021/03

10. lipnja 2021.

Revidirane smjernice

o izvješćivanju o značajnim incidentima u skladu s Direktivom PSD2

1. Obveze usklađivanja i izvješćivanja

Status ovih smjernica

1. Ovaj dokument sadrži smjernice izdane u skladu s člankom 16. Uredbe o EBA-i[1]. U skladu s člankom 16. stavkom 3. Uredbe o EBA-i, nadležna tijela i financijske institucije moraju ulagati napore da se usklade s ovim smjernicama.

2. U smjernicama se iznosi EBA-ino stajalište o odgovarajućim nadzornim praksama unutar Europskog sustava financijskog nadzora ili o tome kako bi se pravo Unije trebalo primjenjivati u određenom području. Nadležna tijela određena člankom 4. stavkom 2. Uredbe (EU) br.1093/2010 na koja se smjernice primjenjuju trebala bi se s njima uskladiti tako da ih na odgovarajući način uključe u svoje prakse (npr. izmjenama svojeg pravnog okvira ili nadzornih postupaka), uključujući i u slučajevima kada su smjernice prvenstveno upućene institucijama.

Zahtjevi za izvješćivanje

3. U skladu s člankom 16. stavkom 3. Uredbe (EU) 1093/2010 nadležna tijela moraju obavijestiti EBA-u o tome jesu li usklađena ili se namjeravaju uskladiti s ovim smjernicama, odnosno o razlozima neusklađenosti do (07.11.2021). U slučaju izostanka obavijesti unutar tog roka, EBA će smatrati da nadležna tijela nisu usklađena. Obavijesti se dostavljaju slanjem ispunjenog obrasca koji se nalazi na internetskim stranicama EBA-e s naznakom „EBA/GL/2021/03”. Obavijesti bi trebale slati osobe s odgovarajućom nadležnošću za izvješćivanje o usklađenosti u ime svojih nadležnih tijela. Svaka se promjena statusa usklađenosti isto tako mora prijaviti EBA-i.

4. Obavijesti će se objaviti na internetskim stranicama EBA-e u skladu s člankom 16. stavkom 3.

[1] Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ (SL L 331, 15.12.2010., str. 12.).

2. Predmet, područje primjene i definicije

Predmet

5. Smjernice su izrađene na temelju obveze EBA-e iz članka 96. stavka 3. Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ (Direktiva PSD2).

6. Točnije, smjernicama se određuju kriteriji koje pružatelji platnih usluga trebaju upotrijebiti za klasifikaciju značajnih operativnih ili sigurnosnih incidenata te format i procedure kojih se trebaju pridržavati kako bi o takvim incidentima obavijestili nadležno tijelo u matičnoj državi članici u skladu s člankom 96. stavkom 1. prethodno navedene direktive.

7. Osim toga, smjernicama se određuje način na koji ta nadležna tijela trebaju ocijeniti relevantnost incidenta i pojedinosti iz izvješća o incidentima koja, u skladu s člankom 96. stavkom 2. prethodno navedene direktive, moraju podijeliti s drugim domaćim tijelima.

8. Nadalje, u smjernicama se govori i o dijeljenju relevantnih informacija o prijavljenim incidentima s EBA-om i ESB-om radi promicanja zajedničkog i dosljednog pristupa.

Područje primjene

9. Smjernice se primjenjuju na klasifikaciju i izvješćivanje o značajnim operativnim ili sigurnosnim incidentima u skladu sa člankom 96. Direktive PSD2.

10. Smjernice se primjenjuju na sve incidente obuhvaćene definicijom „značajnog operativnog ili sigurnosnog incidenta”, a to uključuje i vanjske i unutarnje događaje koji mogu biti zlonamjerni ili nenamjerni.

11. Smjernice se primjenjuju i na značajne operativne ili sigurnosne incidente koji potječu izvan Unije (npr. kada incident nastane u matičnom društvu ili društvu kćeri s poslovnim nastanom izvan Unije), a utječu na platne usluge koje pruža pružatelj platnih usluga koji se nalazi u Uniji bilo izravno (uslugu povezanu s plaćanjem pruža zahvaćeno društvo izvan Unije) ili neizravno (sposobnost pružatelja platnih usluga da nastavi s aktivnošću plaćanja ugrožena je na neki drugi način zbog incidenta).

12. Ove se smjernice također primjenjuju na značajne incidente koji utječu na funkcije koje su pružatelji platnih usluga eksternalizirali trećim stranama.

Adresati

13. Prva grupa smjernica (4. poglavlje) odnosi se na pružatelje platnih usluga kako su definirani u članku 4. Stavku 11. Direktive PSD2 i kako se na njih upućuje u članku 4. stavku 1. Uredbe (EU) 1093/2010.

14. Druga i treća grupa smjernica (5. i 6. poglavlje) odnose se na nadležna tijela kako su definirana u članku 4. stavku 2. točki i. Uredbe (EU) br. 1093/2010.

Definicije

15. Ako nije drugačije naznačeno, pojmovi upotrijebljeni i utvrđeni u Direktivi PSD2 imaju isto značenje u ovim smjernicama. Osim toga, za potrebe ovih smjernica primjenjuju se sljedeće definicije:

Operativni ili sigurnosni incident	Jedan događaj ili niz povezanih događaja koje nije planirao pružatelj platnih usluga, a koji imaju ili će vjerojatno imati negativan učinak na cjelovitost, dostupnost, povjerljivost, i/ili autentičnost usluga povezanih s plaćanjem.
Cjelovitost	Svojstvo čuvanja točnosti i potpunosti imovine (uključujući podatke).
Dostupnost	Svojstvo dostupnosti i mogućnosti korištenja uslugama povezanim s plaćanjem korisnicima platnih usluga, u skladu s prihvatljivim razinama koje je unaprijed odredio pružatelj platnih usluga.
Povjerljivost	Svojstvo da informacije nisu dostupne ili otkrivene neovlaštenim fizičkim osobama, subjektima ili procesima.
Autentičnost	Svojstvo izvora da je upravo ono što tvrdi da jest.
Usluge povezane s plaćanjem	Bilo koja poslovna aktivnost u smislu članka 4. stavka 3. Direktive PSD2 i sva tehnička podrška potrebna za ispravno pružanje platnih usluga.

3. Provedba

Datum primjene

16. Ove se smjernice primjenjuju od 1. siječnja 2022.

Stavljanje izvan snage

17. Sljedeće se smjernice stavljaju izvan snage s učinkom od 1. siječnja 2022.:

Smjernice o izvješćivanju o značajnim incidentima u skladu s Direktivom (EU) 2015/2366 (PSD2) (EBA/GL/2017/10)

4. Smjernice koje se odnose na pružatelje platnih usluga u vezi s izvješćivanjem nadležnog tijela u matičnoj državi članici o značajnim operativnim ili sigurnosnim incidentima

Smjernica 1.: klasifikacija značajnog incidenta

1.1. Pružatelji platnih usluga trebaju klasificirati kao značajne one operativne ili sigurnosne incidente koji ispunjavaju

a. jedan ili više kriterija na „višoj razini utjecaja” ili

b. tri ili više kriterija na „nižoj razini utjecaja”

kako je određeno u smjernici 1.4., i to nakon ocjenjivanja utvrđenog ovim smjernicama.

1.2. Pružatelji platnih usluga trebaju ocijeniti operativni ili sigurnosni incident u odnosu na sljedeće kriterije i njihove temeljne pokazatelje:

i. Zahvaćene transakcije

Pružatelji platnih usluga trebaju utvrditi ukupnu vrijednost zahvaćenih transakcija, kao i postotni udio kompromitiranih plaćanja u redovnom volumenu platnih transakcija provedenih zahvaćenim platnim uslugama.

ii. Zahvaćeni korisnici platnih usluga

Pružatelji platnih usluga trebaju utvrditi apsolutni broj zahvaćenih korisnika platnih usluga te njihov postotni udio u ukupnom broju korisnika platnih usluga.

iii. Povreda sigurnosti mrežnih ili informacijskih sustava

Pružatelji platnih usluga trebaju utvrditi je li zlonamjernom radnjom ugrožena sigurnost mrežnih ili informacijskih sustava povezanih s pružanjem platnih usluga.

iv. Razdoblje prekida rada usluge

Pružatelji platnih usluga trebaju utvrditi razdoblje u kojem će usluga vjerojatno biti nedostupna korisniku platnih usluga, odnosno pružatelj platnih usluga neće moći izvršiti nalog za plaćanje u smislu članka 4. stavka 13. Direktive PSD2.

v. Ekonomski učinak

Pružatelji platnih usluga trebaju cjelovito utvrditi financijske troškove povezane s incidentom i uzeti u obzir i apsolutni iznos i, kada je primjenjivo, relativan značaj tih troškova u odnosu na veličinu pružatelja platnih usluga (tj. osnovni kapital pružatelja platnih usluga).

vi. Visoka razina unutarnje eskalacije

Pružatelji platnih usluga trebaju utvrditi jesu li njihovi članovi uprave već obaviješteni o tom incidentu ili ne, odnosno hoće li vjerojatno o njemu biti obaviješteni.

vii. Potencijalno zahvaćeni drugi pružatelji platnih usluga ili relevantne infrastrukture

Pružatelji platnih usluga trebaju odrediti posljedice koje će incident vjerojatno imati za sustav, tj. njegov potencijal da se proširi s izvorno zahvaćenog pružatelja platnih usluga na druge pružatelje platnih usluga, infrastrukture financijskog tržišta i/ili platne sheme.

viii. Učinak na reputaciju

Pružatelji platnih usluga trebaju utvrditi na koje sve načine incident može ugroziti povjerenje korisnika u samog pružatelja platnih usluga i općenito u temeljnu uslugu ili tržište kao cjelinu.

1.3. Pružatelji platnih usluga trebaju izračunati vrijednost pokazatelja u skladu sa sljedećom metodologijom:

i. Zahvaćene transakcije:

Opće je pravilo da pružatelji platnih usluga trebaju smatrati da su „zahvaćene transakcije" sve domaće i prekogranične transakcije na koje je incident izravno ili neizravno utjecao ili će vjerojatno izravno ili neizravno utjecati, a osobito one transakcije koje se nije moglo inicirati ili obraditi, one s promijenjenim sadržajem poruke o plaćanju i one koje su inicirane s namjerom prijevare (neovisno o tome jesu li novčana sredstva vraćena ili ne) ili one čija je ispravna provedba na bilo koji drugi način spriječena ili ugrožena incidentom.

Za operativne incidente koji utječu na sposobnost iniciranja i/ili obrade transakcija, pružatelji platnih usluga trebaju prijaviti samo incidente dulje od jednog sata. Trajanje incidenta treba mjeriti od trenutka nastanka incidenta do trenutka kada su redovne aktivnosti/poslovanje vraćeni na istu razinu usluge koja je pružena prije incidenta.

Nadalje, pružatelji platnih usluga trebaju smatrati da je „redovan volumen platnih transakcija" godišnji dnevni prosjek domaćih i prekograničnih platnih transakcija izvršenih istim platnim uslugama koje su zahvaćene incidentom, pri čemu prethodna godina služi kao referentno razdoblje za izračune. Ako pružatelji platnih usluga smatraju da dobivena brojka nije reprezentativna (npr. zbog sezonskog utjecaja), umjesto tog izračuna trebaju upotrijebiti drugi, reprezentativniji izračun i obavijestiti nadležno tijelo o osnovnim razlozima za taj pristup u odgovarajućem polju obrasca (vidjeti Prilog).

ii. Zahvaćeni korisnici platnih usluga

Pružatelji platnih usluga trebaju smatrati da su „zahvaćeni korisnici platnih usluga" svi klijenti (domaći ili inozemni, potrošači ili poduzeća) koji imaju ugovor sa zahvaćenim pružateljem

platnih usluga kojim im se odobrava pristup zahvaćenoj platnoj usluzi i koji su pretrpjeli ili će vjerojatno pretrpjeti posljedice incidenta. Pružatelji platnih usluga trebaju na temelju prošle aktivnosti procijeniti broj korisnika platnih usluga koji su se možda koristili platnom uslugom tijekom trajanja incidenta.

U slučaju grupa, svaki pružatelj platnih usluga treba uzeti u obzir samo svoje korisnike platnih usluga. Ako pružatelj platnih usluga nudi operativne usluge drugim subjektima, taj pružatelj platnih usluga treba uzeti u obzir samo svoje korisnike platnih usluga (ako postoje), a pružatelji platnih usluga koji su korisnici tih operativnih usluga trebaju ocijeniti incident u odnosu na vlastite korisnike platnih usluga.

Za operativne incidente koji utječu na sposobnost iniciranja i/ili obrade transakcija, pružatelji platnih usluga trebaju prijaviti samo incidente koji utječu na korisnike platnih usluga dulje od jednog sata. Trajanje incidenta treba mjeriti od trenutka nastanka incidenta do trenutka kada su redovne aktivnosti/poslovanje vraćeni na istu razinu usluge koja je pružena prije incidenta.

Nadalje, pružatelji platnih usluga trebaju smatrati da je ukupan broj korisnika platnih usluga zbroj domaćih i prekograničnih korisnika platnih usluga s kojima su ugovorno vezani u trenutku incidenta (ili, kao alternativa, njihov najnoviji dostupan broj) i koji su imali pristup zahvaćenoj platnoj usluzi neovisno o njihovoj veličini i neovisno o tome smatraju li se aktivnim ili pasivnim korisnicima platnih usluga.

iii. Povreda sigurnosti mrežnih ili informacijskih sustava

Pružatelji platnih usluga trebaju utvrditi je li neka zlonamjerna radnja ugrozila dostupnost, autentičnost, cjelovitost ili povjerljivost mrežnih ili informacijskih sustava (uključujući podatke) povezanih s pružanjem platnih usluga.

iv. Razdoblje prekida rada usluge

Pružatelji platnih usluga trebaju razmotriti koliko traje ili će vjerojatno trajati prekid bilo kojeg zadatka, procesa ili kanala povezanog s pružanjem platnih usluga koji će spriječiti i. iniciranje i/ili izvršavanje platne usluge i/ili ii. pristup računu za plaćanje. Pružatelji platnih usluga trebaju računati razdoblje prekida rada usluge od trenutka u kojem prekid počinje te trebaju uzeti u obzir vremenska razdoblja kada su otvoreni za poslovanje, a koja su potrebna za izvršavanje platnih usluga, kao i vrijeme zatvaranja i razdoblja održavanja ako je to relevantno i primjenjivo. Ako pružatelji platnih usluga ne mogu utvrditi kada je počelo razdoblje prekida rada usluge, iznimno trebaju računati razdoblje prekida rada usluge od trenutka u kojem je prekid rada otkriven.

v. Ekonomski učinak

Pružatelji platnih usluga trebaju razmotriti troškove koji se mogu izravno povezati s incidentom i one koji su neizravno povezani s incidentom. Pružatelji platnih usluga trebaju, među ostalim, uzeti u obzir oduzeta novčana sredstva ili imovinu, troškove zamjene hardvera ili softvera, druge troškove forenzičnih ili korektivnih radnji, naknade zbog neispunjenja ugovornih obveza, kazne, vanjske obveze i izgubljene prihode. Pružatelji platnih usluga

trebaju uzeti u obzir samo one neizravne troškove koji su već poznati ili za koje je vrlo vjerojatno da će nastati.

vi. *Visoka razina unutarnje eskalacije*

Pružatelji platnih usluga trebaju razmotriti je li, zbog utjecaja incidenta na usluge povezane s plaćanjem, upravljačko tijelo, kako je definirano Smjernicama EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima, obaviješteno ili će vjerojatno biti obaviješteno, u skladu sa smjernicom 60. točkom (d) Smjernica EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima, o incidentu izvan bilo kojeg postupka periodičnog izvješćivanja te redovito tijekom trajanja incidenta. Nadalje, pružatelji platnih usluga trebaju razmotriti je li, zbog utjecaja incidenta na usluge povezane s plaćanjem, već aktivirano krizno stanje, odnosno je li vjerojatno da će se ono aktivirati.

vii. *Potencijalno zahvaćeni drugi pružatelji platnih usluga ili relevantne infrastrukture*

Pružatelji platnih usluga trebaju procijeniti utjecaj incidenta na financijsko tržište, koje obuhvaća infrastrukture financijskog tržišta i/ili platne sheme koje im pružaju potporu te druge pružatelje platnih usluga. Pružatelji platnih usluga osobito trebaju ocijeniti je li se incident već proširio na druge pružatelje platnih usluga, odnosno hoće li do toga vjerojatno doći, je li utjecao ili će vjerojatno utjecati na neometano funkcioniranje infrastruktura financijskog tržišta te je li ugrozio ili će vjerojatno ugroziti pravilno funkcioniranje financijskog sustava kao cjeline. Pružatelji platnih usluga trebaju imati na umu različita pitanja, primjerice: jesu li zahvaćena komponenta/softver zaštićeni autorskim pravom ili javno dostupni, je li kompromitirana mreža unutarnja ili vanjska i je li pružatelj platnih usluga prestao ili će vjerojatno prestati ispunjavati svoje obveze u infrastrukturama financijskog tržišta u kojima je član.

viii. *Učinak na reputaciju*

Pružatelji platnih usluga trebaju razmotriti mjeru u kojoj je incident, prema njihovu saznanju, postao ili je vjerojatno da će postati vidljiv na tržištu. Pružatelji platnih usluga osobito trebaju razmotriti vjerojatnost da će incident prouzročiti štetu društvu, što je dobar indikator potencijalnog utjecaja na njihovu reputaciju. Pružatelji platnih usluga trebaju razmotriti i. jesu li se korisnici platnih usluga i/ili drugi pružatelji platnih usluga žalili na negativan učinak incidenta; ii. je li incident utjecao na vidljivi proces povezan s platnim uslugama te je stoga vjerojatno da će biti ili već je medijski pokriven (uzimajući u obzir ne samo tradicionalne medije, kao što su novine, nego i blogove, društvene mreže itd.); iii. je li došlo do propusta u ispunjavanju ugovornih obveza ili je vjerojatno da će do njega doći, što za posljedicu ima pokretanje pravnih radnji protiv pružatelja platnih usluga; iv. je li došlo do propusta u ispunjavanju regulatornih obveza, što je dovelo do toga da su nadzorne mjere ili sankcije javno objavljene ili će vjerojatno biti javno objavljene; te v. je li se i prije dogodila slična vrsta incidenta.

1.4. Pružatelji platnih usluga trebaju procijeniti incident tako da za svaki kriterij utvrde jesu li već dosegnuti relevantni pragovi iz tablice 1., odnosno je li vjerojatno da će biti dosegnuti prije nego što se incident riješi.

Tablica 1.: Pragovi

Kriteriji	Niža razina utjecaja	Viša razina utjecaja
Zahvaćene transakcije	> 10 % redovnog volumena transakcija pružatelja platnih usluga (u smislu broja transakcija) **i** trajanje incidenta > 1 sat* **ili** > 500 000 EUR **i** trajanje incidenta > 1 sat*	> 25 % redovnog volumena transakcija pružatelja platnih usluga (u smislu broja transakcija) **ili** > 15 000 000 EUR
Zahvaćeni korisnici platnih usluga	> 5 000 **i** trajanje incidenta > 1 sat* **ili** > 10 % korisnika platnih usluga pružatelja platnih usluga **i** trajanje incidenta > 1 sat*	> 50 000 **ili** > 25 % korisnika platnih usluga pružatelja platnih usluga
Razdoblje prekida rada usluge	> 2 sata	Nije primjenjivo
Povreda sigurnosti mrežnih ili informacijskih sustava	Da	Nije primjenjivo
Ekonomski učinak	Nije primjenjivo	> maks. (0,1 % osnovnog kapitala**, 200 000 EUR) **ili** > 5 000 000 EUR
Visoka razina unutarnje eskalacije	Da	Da i vjerojatno je da će se aktivirati krizno stanje (ili njegov ekvivalent)
Potencijalno zahvaćeni drugi pružatelji platnih usluga ili relevantne infrastrukture	Da	Nije primjenjivo
Učinak na reputaciju	Da	Nije primjenjivo

* Prag koji se odnosi na trajanje incidenta u razdoblju duljem od jednog sata primjenjuje se samo na operativne incidente koji utječu na sposobnost pružatelja platnih usluga da inicira i/ili obrađuje transakcije.

**Osnovni kapital u smislu članka 25. Uredbe (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012.

1.5. Pružatelji platnih usluga trebaju pribjeći procjenama ako nemaju stvarnih podataka kojima mogu poduprijeti svoje prosudbe o tome je li predmetni prag dosegnut, odnosno je li vjerojatno da će se dosegnuti prije nego što se incident riješi (npr. to se može dogoditi u početnoj fazi istrage).

1.6. Pružatelji platnih usluga trebaju provoditi tu procjenu kontinuirano tijekom cjelokupnog trajanja incidenta kako bi otkrili sve potencijalne promjene statusa bilo prema višoj razini (incident koji nije značajan u značajan incident) ili nižoj razini (značajan incident u incident koji nije značajan). O svakoj reklasifikaciji incidenta iz značajnog u incident koji nije značajan treba bez odgode obavijestiti nadležno tijelo u skladu sa zahtjevom iz smjernice 2.21.

Smjernica 2.: postupak obavješćivanja

2.1. Pružatelji platnih usluga trebaju prikupiti sve relevantne informacije, pripremiti izvješće o incidentu s pomoću obrasca iz Priloga i podnijeti ga nadležnom tijelu u matičnoj državi članici. Pružatelji platnih usluga trebaju ispuniti sva polja obrasca pridržavajući se uputa navedenih u Prilogu.

2.2. Pružatelji platnih usluga trebaju upotrijebiti isti obrazac prilikom podnošenja početnog, prijelaznog i konačnog izvješća povezanih s istim incidentom. Pružatelji platnih usluga trebaju stoga postupno ispuniti samo jedan obrazac te, ako je to primjenjivo, ažurirati informacije pružene u prethodnim izvješćima.

2.3. Nadalje, ako je to primjenjivo, pružatelji platnih usluga trebaju nadležnom tijelu u svojoj matičnoj državi članici podnijeti primjerak obavijesti koja je dostavljena (ili će biti dostavljena) njihovim korisnicima, kako je predviđeno odredbama drugog podstavka stavka 1. članka 96. Direktive PSD2 čim ona postane dostupna.

2.4. Pružatelji platnih usluga trebaju na zahtjev nadležnog tijela u matičnoj državi članici dostaviti sve dodatne dokumente kojima se nadopunjuju informacije dostavljene u standardiziranom obrascu. Pružatelji platnih usluga trebaju pružiti odgovor na bilo koji zahtjev nadležnog tijela u matičnoj državi članici za pružanje dodatnih informacija ili objašnjenja o već podnesenoj dokumentaciji.

2.5. U obrascu iz smjernice 2.1. pružatelji platnih usluga trebaju navesti sve dodatne informacije navedene u dokumentima koje pružatelji platnih usluga dostavljaju nadležnom tijelu na inicijativu pružatelja platnih usluga ili na zahtjev nadležnog tijela u skladu sa smjernicom 2.4.

2.6. Pružatelji platnih usluga trebaju u svakom trenutku čuvati povjerljivost i cjelovitost informacija koje razmjenjuju s nadležnim tijelom u svojoj matičnoj državi članici te se trebaju i ispravno autentificirati nadležnom tijelu u matičnoj državi članici.

Početno izvješće

2.7. Pružatelji platnih usluga trebaju podnijeti početno izvješće nadležnom tijelu u matičnoj državi članici čim se neki operativni ili sigurnosni incident klasificira kao značajan. Nadležna tijela trebaju bez nepotrebne odgode potvrditi primitak početnog izvješća i dodijeliti jedinstvenu referentnu oznaku kojom se nedvosmisleno identificira incident. Pružatelji platnih usluga tu referentnu oznaku trebaju navesti prilikom dostavljanja ažuriranog početnog izvješća ili

ažuriranih prijelaznih ili konačnih izvješća povezanih s istim incidentom ako prijelazna i konačna izvješća nisu već podnesena zajedno s početnim izvješćem.

2.8. Pružatelji platnih usluga trebaju podnijeti početno izvješće nadležnom tijelu u roku od četiri sata od trenutka kad je operativni ili sigurnosni incident klasificiran kao značajan. Ako je poznato da kanali za izvješćivanje nadležnog tijela nisu dostupni ili funkcionalni u tom trenutku, pružatelji platnih usluga trebaju poslati početno izvješće čim kanali ponovno postanu dostupni/funkcionalni.

2.9. Pružatelji platnih usluga trebaju pravodobno klasificirati incident u skladu sa smjernicama 1.1. i 1.4. nakon otkrivanja incidenta, ali najkasnije 24 sata nakon otkrivanja incidenta, te bez nepotrebne odgode nakon što pružatelju platnih usluga postanu dostupne informacije potrebne za klasifikaciju incidenta. Ako je za klasifikaciju incidenta potrebno dulje vrijeme, pružatelji platnih usluga u početnom izvješću podnesenom nadležnom tijelu trebaju objasniti razloge za to.

2.10. Osim toga, pružatelji platnih usluga trebaju podnijeti početno izvješće nadležnom tijelu u matičnoj državi članici kada se incident koji prethodno nije bio značajan reklasificira kao značajan incident. U tom slučaju, pružatelji platnih usluga trebaju poslati početno izvješće nadležnom tijelu neposredno nakon što se utvrdi promjena statusa ili, ako se zna da kanali za izvješćivanje nadležnog tijela nisu dostupni ili funkcionalni u danom trenutku, čim oni ponovno postanu dostupni/funkcionalni.

2.11. Pružatelji platnih usluga svojim početnim izvješćima također trebaju obuhvatiti informacije u zaglavlju (tj. dio A obrasca) te u njima opisati neke osnovne značajke incidenta i njegove očekivane posljedice na temelju informacija dostupnih odmah nakon što je klasificiran kao značajan. Pružatelji platnih usluga trebaju pribjeći procjenama kada im nisu dostupni stvarni podaci.

Prijelazno izvješće

2.12. Nakon oporavka redovnih aktivnosti i ponovne uspostave redovitog poslovanja, pružatelji platnih usluga trebaju dostaviti prijelazno izvješće kako bi nadležno tijelo obavijestili o toj okolnosti. Pružatelji platnih usluga trebaju smatrati da je redovito poslovanje ponovno uspostavljeno kada se aktivnosti/poslovanje vrate na istu razinu usluge/uvjeta koju je odredio pružatelj platnih usluga ili koja je utvrđena izvana sporazumom o razini usluga (u pogledu vremena obrade, kapaciteta, sigurnosnih zahtjeva itd.) i kada se više ne provode izvanredne mjere. Prijelazno izvješće treba sadržavati detaljniji opis incidenta i njegovih posljedica (dio B obrasca).

2.13. Ako redovne aktivnosti još nisu oporavljene, pružatelji platnih usluga nadležnom tijelu trebaju dostaviti prijelazno izvješće u roku od tri radna dana od podnošenja početnog izvješća.

2.14. Pružatelji platnih usluga trebaju ažurirati informacije koje su već navedene u dijelovima A i B obrasca kada saznaju za značajne promjene do kojih je došlo nakon podnošenja prethodnog izvješća (npr. je li incident eskalirao ili se smanjio, jesu li otkriveni novi uzroci ili su poduzete radnje za rješavanje problema). To uključuje slučaj kada incident nije riješen u roku od tri radna dana, zbog čega bi pružatelji platnih usluga morali podnijeti dodatno prijelazno izvješće. Pružatelji platnih usluga u svakom slučaju trebaju podnijeti dodatno prijelazno izvješće na zahtjev nadležnog tijela u matičnoj državi članici.

2.15. Kao i u slučaju početnih izvješća, kada nisu dostupni stvarni podaci, pružatelji platnih usluga trebaju pribjeći procjenama.

2.16. Ako se redovito poslovanje ponovno uspostavi unutar četiri sata od trenutka kada je incident klasificiran kao značajan, pružatelji platnih usluga trebaju nastojati istodobno podnijeti početno i prijelazno izvješće (tj. ispuniti dijelove A i B obrasca) u tom roku od četiri sata.

Konačno izvješće

2.17. Pružatelji platnih usluga trebaju podnijeti konačno izvješće nakon analize temeljnog uzroka (neovisno o tome jesu li već provedene mjere za ublažavanje ili je otkriven konačni temeljni uzrok) i nakon što postanu dostupni stvarni podaci kojima se mogu zamijeniti eventualne procjene.

2.18. Pružatelji platnih usluga trebaju podnijeti konačno izvješće nadležnom tijelu najkasnije dvadeset radnih dana nakon što se procijeni da je redovito poslovanje ponovno uspostavljeno. Pružatelji platnih usluga kojima je potrebno produženje tog roka (npr. ako još uvijek nema dostupnih stvarnih podataka o utjecaju ili ako nisu otkriveni temeljni uzroci) trebaju se obratiti nadležnom tijelu prije isteka roka i navesti prikladno opravdanje za odgodu, kao i novi procijenjeni datum konačnog izvješća.

2.19. Pružatelji platnih usluga trebaju nastojati zajedno pružiti informacije povezane s početnim, prijelaznim i konačnim izvješćem ako sve informacije koje se zahtijevaju u konačnom izvješću (tj. dijelu C obrasca) mogu pružiti u roku od četiri sata od trenutka kada je incident klasificiran kao značajan.

2.20. Pružatelji platnih usluga trebaju nastojati u svojem konačnom izvješću navesti cjelovite informacije, odnosno: i. stvarne podatke o utjecaju umjesto procjena (kao i sva druga ažuriranja potrebna u dijelovima A i B obrasca) te ii. informacije iz dijela C obrasca, koje obuhvaćaju temeljni uzrok, ako je već poznat, i sažetak mjera koje su usvojene ili se namjeravaju usvojiti radi uklanjanja problema i sprečavanja njegove ponovne pojave u budućnosti.

2.21. Osim toga, pružatelji platnih usluga trebaju poslati konačno izvješće kada, kao rezultat kontinuirane procjene incidenta, utvrde da već prijavljeni incident više ne ispunjava kriterije za klasifikaciju kao značajni incident te se ne očekuje da će ih ispunjavati do rješenja incidenta. U tom slučaju pružatelji platnih usluga trebaju poslati konačno izvješće čim se

otkrije ta okolnost, a u svakom slučaju prije isteka roka za podnošenje sljedećeg izvješća. Pružatelji platnih usluga u toj situaciji umjesto ispunjavanja dijela C obrasca trebaju označiti kvačicom okvir „incident reklasificiran u incident koji nije značajan" i objasniti razloge kojima se opravdava promjena klasifikacije.

Smjernica 3.: delegirano i konsolidirano izvješćivanje

3.1. Kada to dopusti nadležno tijelo, pružatelji platnih usluga koji svoje obveze izvješćivanja u skladu s Direktivom PSD2 žele delegirati trećoj strani o tome trebaju obavijestiti nadležno tijelo u matičnoj državi članici i osigurati ispunjenje sljedećih uvjeta:

a. Službenim ugovorom ili, ako je primjenjivo, postojećim internim sporazumom unutar grupe na kojem se temelji delegiranje izvješćivanja između pružatelja platnih usluga i treće strane nedvosmisleno se određuje raspodjela odgovornosti svih strana. U njemu se osobito navodi da, neovisno o potencijalnim delegiranim obvezama izvješćivanja, zahvaćeni pružatelj platnih usluga i dalje u potpunosti snosi odgovornost za ispunjavanje zahtjeva utvrđenih člankom 96. Direktive PSD2, kao i za sadržaj informacija podnesenih nadležnom tijelu u matičnoj državi članici.

b. Delegiranje je u skladu sa zahtjevima za eksternalizaciju važnih operativnih funkcija utvrđenima u:

i. članku 19. stavku 6. Direktive PSD2 za institucije za platni promet i institucije za elektronički novac, koji je primjenjiv *mutatis mutandis* u skladu s člankom 3. Direktive 2009/110/EZ; ili

ii. Smjernicama EBA-e o eksternalizaciji (EBA/GL/2019/02) u odnosu na sve pružatelje platnih usluga.

c. Informacije se podnose nadležnom tijelu u matičnoj državi članici unaprijed, a u svakom slučaju unutar rokova i u skladu s postupcima koje je odredilo nadležno tijelo, gdje je to primjenjivo.

d. Pravilno su osigurane povjerljivost osjetljivih podataka te kvaliteta, dosljednost, cjelovitost i pouzdanost informacija koje će se podnijeti nadležnom tijelu.

3.2. Pružatelji platnih usluga koji žele određenoj trećoj strani povjeriti ispunjavanje obveza konsolidiranog izvješćivanja (tj. pripremu jedinstvenog izvješća za nekoliko pružatelja platnih usluga zahvaćenih istim značajnim operativnim ili sigurnosnim incidentom) o tome trebaju obavijestiti nadležno tijelo u matičnoj državi članici, navesti podatke za kontakt koji su navedeni u obrascu pod „Zahvaćeni PPU" i osigurati ispunjavanje sljedećih uvjeta:

a. ta odredba mora biti navedena u ugovoru o delegiranom izvješćivanju;

b. mogućnost konsolidiranog izvješćivanja mora ovisiti o tome je li uzrok incidenta prekid usluga koje pruža treća strana;

c. konsolidirano izvješćivanje mora biti ograničeno na pružatelje platnih usluga s poslovnim nastanom u istoj državi članici;

d. mora biti naveden popis svih pružatelja platnih usluga zahvaćenih incidentom;

e. treba osigurati da treća strana procijeni značajnosti incidenta kod svakog zahvaćenog pružatelja platnih usluga i da konsolidiranim izvješćem obuhvati samo one pružatelje platnih usluga kod kojih je incident klasificiran kao značajan; nadalje, treba osigurati da će, u slučaju sumnje, pružatelj platnih usluga biti obuhvaćen konsolidiranim izvješćem pod uvjetom da ne postoje dokazi o tome da ne treba biti obuhvaćen;

f. treba osigurati da, u slučaju polja obrasca u kojima nije moguće dati zajednički odgovor (npr. dijelovi B2, B4 ili C3 obrasca), treća strana i. ispuni ta polja zasebno za svakog zahvaćenog pružatelja platnih usluga i dodatno naznači identitet svakog pružatelja platnih usluga na koje se informacije odnose ili ii. upotrijebi kumulativne vrijednosti zabilježene ili procijenjene za pružatelje platnih usluga;

g. treća strana u svakom trenutku obavješćuje pružatelja platnih usluga o svim relevantnim informacijama o incidentu te o svim interakcijama treće strane s nadležnim tijelom i o sadržaju tih interakcija, ali samo ako se time ne krši povjerljivost informacija koje se odnose na druge pružatelje platnih usluga.

3.3. Pružatelji platnih usluga ne smiju delegirati svoje obveze izvješćivanja prije nego što o tome obavijeste nadležno tijelo u matičnoj državi članici ili nakon što su obaviješteni da ugovor o eksternalizaciji ne ispunjava zahtjeve navedene u smjernici 3.1. točki (b).

3.4. Pružatelji platnih usluga koji žele otkazati delegiranje svojih obveza izvješćivanja trebaju o toj odluci obavijestiti nadležno tijelo u matičnoj državi članici u skladu s rokovima i procedurama koje je odredilo to tijelo. Osim toga, pružatelji platnih usluga trebaju obavijestiti nadležno tijelo u matičnoj državi članici o svim značajnim promjenama koje utječu na imenovanu treću stranu i njezinu sposobnost da ispuni obveze izvješćivanja.

3.5. Pružatelji platnih usluga trebaju u bitnome ispuniti svoje obveze izvješćivanja bez pribjegavanja vanjskoj pomoći svaki put kada imenovana treća strana propusti obavijestiti nadležno tijelo u matičnoj državi članici o značajnom operativnom ili sigurnosnom incidentu u skladu s člankom 96. Direktive PSD2 i ovim smjernicama. Pružatelji platnih usluga također trebaju osigurati da se incident ne prijavi dva puta, tj. da ga jednom prijavi pružatelj platnih usluga i još jednom treća strana.

3.6. Pružatelji platnih usluga trebaju osigurati da se, u situaciji u kojoj je incident uzrokovan poremećajem u uslugama koje pruža pružatelj tehničkih usluga (ili infrastruktura) koji utječe

na više pružatelja platnih usluga, delegirano izvješćivanje odnosi na pojedinačne podatke pružatelja platnih usluga (osim u slučaju konsolidiranog izvješćivanja).

Smjernica 4.: operativna i sigurnosna politika

4.1. Pružatelji platnih usluga trebaju osigurati da su njihovom općom operativnom i sigurnosnom politikom jasno definirane sve odgovornosti za izvješćivanje o incidentima u skladu s Direktivom PSD2, kao i postupci uspostavljeni za ispunjavanje zahtjeva utvrđenih ovim smjernicama.

5. Smjernice koje se odnose na nadležna tijela o kriterijima za procjenu relevantnosti incidenta i pojedinostima iz izvješća o incidentima koje se trebaju podijeliti s drugim domaćim tijelima

Smjernica 5.: Procjena relevantnosti incidenta

5.1. Nadležna tijela u matičnoj državi članici trebaju procijeniti relevantnost značajnog operativnog ili sigurnosnog incidenta za druga domaća tijela na temelju svojeg stručnog mišljenja i sljedećih kriterija koji im služe kao glavni pokazatelji važnosti predmetnog incidenta:

a. Uzroci incidenta obuhvaćeni su zakonskim ovlastima drugog domaćeg tijela (tj. u njegovoj su nadležnosti).
b. Posljedice incidenta imaju utjecaj na ciljeve drugog domaćeg tijela (npr. zaštita financijske stabilnosti).
c. Incident utječe ili bi mogao utjecati na veliki broj korisnika platnih usluga.
d. Vjerojatno je da će incident biti, odnosno da već jest, medijski pokriven u velikoj mjeri.

5.2. Nadležna tijela u matičnoj državi članici trebaju redovito provoditi tu procjenu tijekom trajanja incidenta kako bi utvrdila sve potencijalne promjene zbog kojih bi se incident za koji se prethodno smatralo da nije relevantan mogao pretvoriti u relevantan incident.

Smjernica 6.: informacije koje se trebaju podijeliti

6.1. Neovisno o drugim zakonskim obvezama dijeljenja informacija povezanih s incidentom s drugim domaćim tijelima, nadležna tijela trebaju domaćim tijelima utvrđenima primjenom smjernice 5.1. pružiti, u najmanju ruku, informacije o značajnim operativnim ili sigurnosnim incidentima u trenutku primanja početnog izvješća (ili izvješća koje je potaklo dijeljenje informacija), odnosno primanja obavijesti o ponovnoj uspostavi redovnog poslovanja (tj. prijelaznog izvješća).

6.2. Nadležna tijela trebaju drugim relevantnim domaćim tijelima dostaviti informacije potrebne za stvaranje jasne slike o tome što se dogodilo i o mogućim posljedicama. Kako bi ispunila tu obvezu, moraju dostaviti barem informacije koje je pružatelj platnih usluga naveo u sljedećim poljima obrasca (u početnom ili prijelaznom izvješću):

- datum i vrijeme klasifikacije incidenta kao značajnog

- datum i vrijeme otkrivanja incidenta
- datum i vrijeme početka incidenta
- datum i vrijeme kada je incident riješen ili se očekuje da će biti riješen
- kratak opis incidenta (uključujući dijelove detaljnog opisa koji nisu osjetljivi)
- kratak opis mjera koje su poduzete ili se namjeravaju poduzeti za oporavak od incidenta
- opis načina na koji bi incident mogao utjecati na druge pružatelje platnih usluga i/ili infrastrukture
- opis medijske pokrivenosti (ako postoji)
- uzrok incidenta

6.3. Nadležna tijela trebaju, ako je to potrebno, provesti ispravnu anonimizaciju i izostaviti sve informacije koje bi mogle biti podložne ograničenjima u pogledu povjerljivosti ili intelektualnog vlasništva prije nego što bilo koje informacije povezane s incidentom podijele s drugim relevantnim domaćim tijelima. Unatoč tome, nadležna tijela trebaju drugim relevantnim domaćim tijelima dostaviti naziv i adresu izvještajnog pružatelja platnih usluga kada ta domaća tijela mogu jamčiti da će se s informacijama postupati povjerljivo.

6.4. Nadležna tijela trebaju u svakom trenutku čuvati povjerljivost i cjelovitost informacija koje se pohranjuju i razmjenjuju te se ispravno autentificirati u odnosu na druga relevantna domaća tijela. Nadležna tijela posebno trebaju sa svim informacijama primljenima na temelju ovih smjernica postupati u skladu s obvezama čuvanja poslovne tajne utvrđenima u Direktivi PSD2, ne dovodeći u pitanje primjenjivo pravo Unije i nacionalne zahtjeve.

6. Smjernice koje se odnose na nadležna tijela o kriterijima za procjenu relevantnih pojedinosti iz izvješća o incidentima koje se trebaju podijeliti s EBA-om i ESB-om te o formatu i postupcima za obavješćivanje o njima

Smjernica 7.: informacije koje se trebaju podijeliti

7.1. Nadležna tijela uvijek trebaju dostaviti EBA-i i ESB-u sva izvješća primljena od (ili u ime) pružatelja platnih usluga zahvaćenih značajnim operativnim ili sigurnosnim incidentom s pomoću standardizirane datoteke dostupne na internetskim stranicama EBA-e.

Smjernica 8.: komunikacija

8.1. Nadležna tijela trebaju u svakom trenutku čuvati povjerljivost i cjelovitost informacija koje se pohranjuju i razmjenjuju te se ispravno autentificirati u odnosu na EBA-u i ESB. Nadležna tijela posebno trebaju sa svim informacijama primljenima na temelju ovih smjernica postupati u skladu s obvezama čuvanja poslovne tajne utvrđenima u Direktivi PSD2, ne dovodeći u pitanje primjenjivo pravo Unije i nacionalne zahtjeve.

8.2. Kako bi se izbjegla kašnjenja u prijenosu informacija povezanih s incidentom EBA-i/ESB-u i kako bi se pomoglo u smanjenju rizika od prekida poslovanja, nadležna tijela trebaju podržavati odgovarajuća sredstva komunikacije.

Prilog – Obrasci za izvješćivanje za pružatelje platnih usluga

Početno izvješće

Početno izvješće	u roku od četiri sata nakon klasifikacije incidenta kao značajnog		Ponovno postavi opcije padajućeg izbornika
Datum izvješća *(DD/MM/GGGG)*		Vrijeme *(HH:MM)*	
Referentna oznaka incidenta			

A – Početno izvješće											
A 1 – OPĆE INFORMACIJE											
Vrsta izvješća											
Vrsta izvješća											
Zahvaćeni pružatelj platnih usluga (PPU)											
Naziv PPU-a											
Nacionalni identifikacijski broj PPU-a											
Vodeći subjekt grupe, ako je primjenjivo											
Država/države zahvaćena/zahvaćene 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					
Primarna kontakt osoba				E-pošta		Telefon					
Sekundarna kontakt osoba				E-pošta		Telefon					
Izvještajni subjekt (ispunite ovaj dio ako izvještajni subjekt nije zahvaćeni PPU u slučaju delegiranog izvješćivanja)											
Naziv izvještajnog subjekta											
Nacionalni identifikacijski broj											
Primarna kontakt osoba				E-pošta		Telefon					
Sekundarna kontakt osoba				E-pošta		Telefon					
A 2 – OTKRIVANJE INCIDENTA I POČETNA KLASIFIKACIJA											
Datum i vrijeme otkrivanja incidenta *(DD/MM/GGGG HH:MM)*											
Datum i vrijeme klasifikacije incidenta *(DD/MM/GGGG HH:MM)*											
Incident otkrio				Ako ste odabrali „Drugo", navedite:							
Vrsta incidenta											
Kriteriji za izvješće o značajnom incidentu	☐ Zahvaćene transakcije	☐ Zahvaćeni korisnici platnih usluga	☐ Razdoblje prekida rada	☐ Povreda sigurnosti mrežnih ili informacijskih sustava	☐ Ekonomski učinak	☐ Visoka razina unutarnje eskalacije	☐ Potencijalno zahvaćeni drugi PPU-ovi ili relevantne infrastrukture	☐ Učinak na reputaciju			
Kratak i općenit opis incidenta											
Učinak u drugim državama članicama EU-a, ako je primjenjivo											
Izvješćivanje drugih nadležnih tijela				Ako ste odabrali „Da", navedite:							
Razlozi za kašnjenje u podnošenju početnog izvješća											

Prijelazno izvješće

Izvješće o značajnom incidentu

Prijelazno izvješće	najviše tri radna dana od podnošenja početnog izvješća	Ponovno postavi opcije padajućeg izbornika

Datum izvješća *(DD/MM/GGGG)* | Vrijeme *(HH:MM)*

Referentna oznaka incidenta

B – Prijelazno izvješće

B 1 – OPĆE INFORMACIJE

Detaljniji opis incidenta:	
O kakvom je točno problemu riječ?	
Kako je incident započeo?	
Kako se razvijao?	
Koje su njegove posljedice (osobito za korisnike platnih usluga)?	
Jesu li korisnici platnih usluga obaviješteni o incidentu?	Ako ste odabrali „Da", navedite:
Je li povezan s prethodnim incidentom/incidentima?	Ako ste odabrali „Da", navedite:
Jesu li zahvaćeni ili uključeni pružatelji usluga/treće strane?	Ako ste odabrali „Da", navedite:
Je li pokrenuto upravljanje kriznim situacijama (unutarnje i/ili vanjsko)?	Ako ste odabrali „Da", navedite:
Datum i vrijeme početka incidenta (ako su već utvrđeni) *(DD/MM/GGGG HH:MM)*	
Datum i vrijeme kada je incident riješen ili se očekuje da će biti riješen *(DD/MM/GGGG HH:MM)*	
Zahvaćena funkcionalna područja	☐ Autentifikacija/autorizacija ☐ Izravna namira ☐ Komunikacija ☐ Neizravna namira ☐ Obračun ☐ Drugo — Ako ste odabrali „Drugo", navedite:
Izmjene prethodnih izvješća	

B 2 – KLASIFIKACIJA INCIDENTA I INFORMACIJE O INCIDENTU

Zahvaćene transakcije [2]	Razini utjecaja Broj zahvaćenih transakcija Kao udio (%) u redovnom broju transakcija Vrijednost zahvaćenih transakcija u EUR Trajanje incidenta (primjenjivo samo na operativne incidente) Komentari:
Zahvaćeni korisnici platnih usluga [3]	Razini utjecaja Broj zahvaćenih korisnika platnih usluga Kao udio (%) u ukupnom broju korisnika platnih usluga
Povreda sigurnosti mrežnih ili informacijskih sustava	Opišite na koji su način zahvaćeni mrežni ili informacijski sustavi
Razdoblje prekida rada usluge	Ukupno razdoblje prekida rada usluge: Dani: Sati: Minute:
Ekonomski učinak	Razini utjecaja Izravni troškovi u EUR Neizravni troškovi u EUR
Visoka razina unutarnje eskalacije	Opišite razinu unutarnje eskalacije incidenta i navedite je li zbog njega aktivirano ili je vjerojatno da će se aktivirati krizno stanje (ili njegov ekvivalent) te ga opišite ako jest
Potencijalno zahvaćeni drugi PPU-ovi ili relevantne infrastrukture	Opišite način na koji bi ovaj incident mogao utjecati na druge PPU-ove i/ili infrastrukture
Učinak na reputaciju	Opišite kako bi incident mogao utjecati na reputaciju PPU-a (npr. pokrivenost u medijima, pokretanje pravnih radnji ili kršenje zakona...)

B 3 – OPIS INCIDENTA

Vrsta incidenta	
Uzrok incidenta	☐ Pod istragom ☐ Zlonamjerna radnja ☐ Pogreška u procesu ☐ Kvar sustava ☐ Ljudske pogreške ☐ Vanjski događaji ☐ Drugo — Ako ste odabrali „Drugo", navedite:
Je li incident na vas utjecao izravno ili neizravno putem pružatelja usluga?	Ako je utjecao neizravno, navedite naziv pružatelja usluga:

B 4 – UČINAK INCIDENTA

Opći učinak	☐ Cjelovitost ☐ Dostupnost	☐ Povjerljivost ☐ Autentičnost
Zahvaćeni komercijalni kanali	☐ Podružnice ☐ E-bankarstvo ☐ E-trgovina	☐ Telefonsko bankarstvo ☐ Mobilno bankarstvo ☐ Bankomati
	Ako ste odabrali „Drugo", navedite:	☐ Prodajno mjesto ☐ Drugo
Zahvaćene platne usluge	☐ Polaganje gotovog novca na račun za plaćanje ☐ Podizanje gotovog novca s računa za plaćanje ☐ Postupci koji su potrebni za vođenje računa za plaćanje ☐ Prihvaćanje platnih instrumenata	☐ Kreditni transferi ☐ Izravna terećenja ☐ Kartična plaćanja ☐ Izdavanje platnih instrumenata
		☐ Novčana pošiljka ☐ Usluge iniciranja ☐ Usluge informiranja o računu

B 5 – UBLAŽAVANJE INCIDENTA

Koje su radnje/mjere dosad poduzete ili planirane za oporavak od incidenta?	
Je li aktiviran plan kontinuiteta poslovanja i/ili plan oporavka informacijskog sustava?	
Ako da, kada? *(DD/MM/GGGG HH:MM)*	
Ako da, opišite	

Konačno izvješće

Izvješće o značajnom incidentu

Odaberite vrstu izvješća:

u roku od dvadeset radnih dana od podnošenja prijelaznog izvješća

Opišite: (primjenjivo za incidente koji su reklasificirani u incidente koji nisu značajni)

Ponovno postavi opcije padajućeg izbornika

Datum izvješća *(DD/MM/GGGG)* | Vrijeme *(HH:MM)*

Referentna oznaka incidenta

C – Konačno izvješće

Ako nije poslano prijelazno izvješće, ispunite i dio B

C 1 – OPĆE INFORMACIJE

Ažuriranje informacija iz početnog izvješća i prijelaznog/prijelaznih izvješća	
Izmjene prethodnih izvješća	
Sve ostale relevantne informacije	
Jesu li ponovno uspostavljene izvorne kontrole? Ako nisu, navedite o kojim se kontrolama radi i dodatni rok potreban za njihovu ponovnu uspostavu	

C 2 – ANALIZA TEMELJNOG UZROKA I DALJNJE MJERE

Što je temeljni uzrok (ako je već poznat)?	Zlonamjerna radnja	Pogreška u procesu	Kvar sustava	Ljudska pogreška	Vanjski događaj	Drugo
Navedite:	Zlonamjerni kod Prikupljanje informacija Upadi Distribuirani / uskraćivanje usluga (D/DoS) Namjerne unutarnje radnje Namjerno vanjsko fizičko oštećenje Sigurnost informacijskog sadržaja Prijevarne radnje Drugo	Manjkavo praćenje i nadzor Problemi u komunikaciji Neispravan rad Neodgovarajuće upravljanje promjenama Neprimjerenost internih procedura i dokumentacije Problemi s oporavkom Drugo	Kvar hardvera Mrežni kvar Problemi s Kvar softvera/aplikacije Fizičko oštećenje Drugo	Nenamjerno Propust u Nedostatni resursi Drugo	Pogreška dobavljača / pružatelj a tehničkih usluga Viša sila Drugo	
	Ako ste odabrali „Drugo", navedite:					
Ostale relevantne informacije o temeljnom uzroku						
Glavne korektivne radnje/mjere koje su poduzete ili planirane za sprečavanje ponavljanja incidenta u budućnosti, ako su već poznate						

C 3 – DODATNE INFORMACIJE

Jesu li drugi PPU-ovi obaviješteni o incidentu?	Ako jesu, navedite dodatne pojedinosti:	
Jesu li poduzete pravne radnje protiv PPU-a?	Ako jesu, navedite dodatne pojedinosti:	
Procjena djelotvornosti poduzetih mjera	Navedite pojedinosti:	

UPUTE ZA ISPUNJAVANJE OBRASCA

Pružatelji platnih usluga (PPU-ovi) trebaju ispuniti odgovarajući dio obrasca ovisno o fazi izvješćivanja u kojoj se nalaze: dio A služi za početno izvješće, dio B za prijelazna izvješća, a dio C za konačno izvješće. Pružatelji platnih usluga trebaju upotrijebiti isti obrazac prilikom podnošenja početnog, prijelaznog i konačnog izvješća povezanih s istim incidentom. Ako nije drugačije navedeno, sva su polja obvezna.

Zaglavlje

Početno izvješće: ovo je prva obavijest koju PPU podnosi nadležnom tijelu u matičnoj državi članici.

Prijelazno izvješće: sadrži detaljniji opis incidenta i njegovih posljedica. Predstavlja ažuriranje početnog (i, ako je to primjenjivo, prethodnog prijelaznog) izvješća o istom incidentu.

Konačno izvješće: ovo je posljednje izvješće koje će PPU poslati o incidentu jer i. je već provedena analiza temeljnog uzroka i procjene se mogu zamijeniti stvarnim podacima ili ii. incident se više ne smatra značajnim i potrebno ga je reklasificirati.

Incident reklasificiran kao incident koji nije značajan: incident više ne ispunjava kriterije za klasifikaciju kao značajni incident te se ne očekuje da će ih ispunjavati do rješenja. PPU-ovi trebaju objasniti razloge za tu reklasifikaciju.

Datum i vrijeme izvješća: točan datum i vrijeme podnošenja izvješća nadležnom tijelu.

Referentna oznaka incidenta (primjenjivo za prijelazno i konačno izvješće, kao i za ažuriranja početnog izvješća): referentna oznaka koju izdaje nadležno tijelo pri zaprimanju početnog izvješća radi nedvosmislene identifikacije incidenta. Svako nadležno tijela treba uključiti dvoznamenkastu ISO oznaku[2] svoje države članice kao prefiks.

A - Početno izvješće

A 1 - Opće informacije

Vrsta izvješća:

Pojedinačno: izvješće se odnosi na jednog PPU-a.

Konsolidirano: izvješće se odnosi na nekoliko PPU-ova u istoj državi članici koji su zahvaćeni istim značajnim operativnim ili sigurnosnim incidentom koji se koriste mogućnošću konsolidiranog izvješćivanja. Polja ispod naslova „Zahvaćeni PPU" treba ostaviti prazna (osim polja „Država/države zahvaćene incidentom"), a popis PPU-ova obuhvaćenih izvješćem treba navesti u odgovarajućoj tablici (Konsolidirano izvješće – popis PPU-ova).

Zahvaćeni PPU: odnosi se na PPU u kojem se odvija incident.

Naziv PPU-a: puni naziv PPU-a koji je obveznik izvješćivanja u obliku u kojem se pojavljuje u odgovarajućem službenom nacionalnom registru PPU-ova.

Nacionalni identifikacijski broj PPU-a: jedinstveni nacionalni identifikacijski broj koji nadležno tijelo matične države članice upotrebljava u svojem nacionalnom registru za nedvosmislenu identifikaciju PPU-a.

Vodeći subjekt grupe: u slučaju grupa subjekata kako su definirane u članku 4. stavku 40. Direktive PSD2, navedite naziv vodećeg subjekta.

Država/države zahvaćene incidentom: država ili države u kojima se pokazao utjecaj incidenta (npr. zahvaćeno je nekoliko podružnica PPU-a koje se nalaze u različitim državama), neovisno o ozbiljnosti incidenta u drugoj državi/drugim državama. Ta država može, no ne mora biti, matična država članica.

Primarna kontakt osoba: ime i prezime osobe odgovorne za izvješćivanje o incidentu ili, ako treća strana kao pružatelj usluga izvješćuje u ime zahvaćenog PPU-a, ime i prezime osobe na čelu odjela za upravljanje incidentima/rizicima ili sličnog odjela u zahvaćenom PPU-u.

[2] Alpha-2 oznake država u skladu s normom ISO-3166 dostupne su na poveznici https://www.iso.org/iso-3166-country-codes.html

E-pošta: adresa e-pošte na koju se po potrebi mogu slati zahtjevi za dodatna objašnjenja. To može biti privatna ili poslovna adresa e-pošte.

Telefon: broj telefona na koji se po potrebi mogu podnijeti zahtjevi za dodatna objašnjenja. To može biti privatni ili poslovni broj telefona.

Sekundarna kontakt osoba: ime i prezime alternativne osobe kojoj se nadležno tijelo može obratiti kako bi se raspitalo o incidentu kada primarna kontakt osoba nije dostupna. Ako u ime zahvaćenog PPU-a izvješće podnosi treća strana kao pružatelj usluga, ime i prezime alternativne osobe u odjelu za upravljanje incidentima/rizicima ili sličnom odjelu u zahvaćenom PPU-u.

E-pošta: adresa e-pošte alternativne kontakt osobe na koju se po potrebi mogu slati zahtjevi za dodatna objašnjenja. To može biti privatna ili poslovna adresa e-pošte.

Telefon: broj telefona alternativne kontakt osobe na koji se po potrebi mogu podnijeti zahtjevi za dodatna objašnjenja. To može biti privatni ili poslovni broj telefona.

Izvještajni subjekt: ovaj se dio treba popuniti ako treća strana ispunjava obveze izvješćivanja u ime zahvaćenog PPU-a, ako je to primjenjivo.

Naziv izvještajnog subjekta: puni naziv subjekta koji izvješćuje o incidentu u obliku u kojem se naziv pojavljuje u odgovarajućem službenom nacionalnom registru poslovnih subjekata.

Nacionalni identifikacijski broj: jedinstveni nacionalni identifikacijski broj koji se upotrebljava u državi u kojoj se nalazi treća strana za nedvosmislenu identifikaciju subjekta koji izvješćuje o incidentu. Ako je treća strana koja provodi izvješćivanje PPU, nacionalni identifikacijski broj treba biti jedinstveni nacionalni identifikacijski broj PPU-a koji nadležno tijelo matične države članice upotrebljava u svojem nacionalnom registru.

Primarna kontakt osoba: ime i prezime osobe odgovorne za izvješćivanje o incidentu.

E-pošta: adresa e-pošte na koju se po potrebi mogu slati zahtjevi za dodatna objašnjenja. To može biti privatna ili poslovna adresa e-pošte.

Telefon: broj telefona na koji se po potrebi mogu podnijeti zahtjevi za dodatna objašnjenja. To može biti privatni ili poslovni broj telefona.

Sekundarna kontakt osoba: ime i prezime alternativne osobe u subjektu koji izvješćuje o incidentu kojoj se nadležno tijelo može obratiti kada primarna kontakt osoba nije dostupna.

E-pošta: adresa e-pošte alternativne kontakt osobe na koju se po potrebi mogu slati zahtjevi za dodatna objašnjenja. To može biti privatna ili poslovna adresa e-pošte.

Telefon: broj telefona alternativne kontakt osobe na koji se po potrebi mogu podnijeti zahtjevi za dodatna objašnjenja. To može biti privatni ili poslovni broj telefona.

A 2 - Otkrivanje i klasifikacija incidenta

Datum i vrijeme otkrivanja incidenta: datum i vrijeme kada je incident prvi put otkriven.

Datum i vrijeme klasifikacije incidenta: datum i vrijeme kada je sigurnosni ili operativni incident klasificiran kao značajan.

Incident otkrio: navedite je li incident otkrio korisnik platnih usluga, netko u PPU-u (npr. odjel za unutarnju reviziju) ili vanjska strana (npr. pružatelj usluga). Ako incident nije otkrio nitko od prethodno navedenih, navedite objašnjenje u odgovarajućem polju.

Vrsta incidenta: navedite je li, prema vašem saznanju te ako su informacije dostupne, riječ o operativnom ili sigurnosnom incidentu.

Operativni: incident koji je nastao zbog neprimjerenih ili neuspjelih procesa, osoba i sustava ili događaja više sile koji utječu na cjelovitost, dostupnost, povjerljivost i/ili autentičnost usluga povezanih s plaćanjem.

Sigurnosni: neovlašteni pristup imovini PPU-a, njezina neovlaštena upotreba, otkrivanje, prekid rada, promjena ili uništenje koji utječu na cjelovitost, dostupnost, povjerljivost i/ili autentičnost usluga povezanih s plaćanjem. To se može dogoditi, među ostalim, kada u PPU-u dođe do povrede sigurnosti mrežnih ili informacijskih sustava.

Kriteriji koji su povod za izvješće o značajnom incidentu: navedite koji su kriteriji povod za izvješće o značajnom incidentu. Među kriterijima moguće je odabrati nekoliko odgovora: zahvaćene transakcije, zahvaćeni korisnici platnih usluga, prekid rada usluge, povreda sigurnosti mrežnih ili informacijskih sustava, ekonomski učinak, visoka razina unutarnje eskalacije, potencijalno zahvaćeni drugi PPU-ovi ili relevantne infrastrukture i/ili učinak na reputaciju.
Kratak i općenit opis incidenta: ukratko navedite najvažnije pojedinosti o incidentu, uključujući moguće uzroke, trenutačne učinke itd.
Učinak u drugim državama članicama EU-a, ako je to primjenjivo: ukratko objasnite učinak incidenta u drugoj državi članici EU-a (npr. na korisnike platnih usluga i/ili infrastrukture platnog prometa). Ako je to izvedivo s obzirom na primjenjive rokove za izvješćivanje, dostavite prijevod na engleski jezik.
Izvješćivanje drugih nadležnih tijela: ako je to poznato u trenutku izvješćivanja, navedite je li incident prijavljen/hoće li biti prijavljen drugim nadležnim tijelima u okviru zasebnih okvira za izvješćivanje o incidentima. Ako je odgovor potvrdan, navedite nadležna tijela.
Razlozi za kašnjenje u podnošenju početnog izvješća: objasnite zašto vam je za klasifikaciju incidenta trebalo više od 24 sata.

B Prijelazno izvješće

B 1 – Opće informacije

Detaljniji opis incidenta: opišite glavne značajke incidenta na način da navedete barem informacije o konkretnom problemu i povezani kontekst, opis načina na koji je došlo do incidenta i kako se razvijao te posljedice, osobito za korisnike platnih usluga itd. Također navedite informacije o komunikaciji s korisnicima platnih usluga, ako je to primjenjivo.
Je li bio povezan s prethodnim incidentom/incidentima?: ako su te informacije dostupne, navedite je li incident povezan s prethodnim incidentima. Ako je incident bio povezan s prethodnim incidentima, navedite koji su to incidenti.
Jesu li bili zahvaćeni ili uključeni pružatelji usluga/treće strane?: ako su te informacije dostupne, navedite je li incident zahvatio ili uključivao druge pružatelje usluga/treće strane. Ako je incident zahvatio ili uključivao pružatelje usluga/treće strane, navedite ih i navedite više informacija.
Je li pokrenuto upravljanje kriznim situacijama (unutarnje i/ili vanjsko)?: navedite je li pokrenut postupak upravljanja kriznim situacijama (unutarnjeg i/ili vanjskog). Ako je upravljanje kriznim situacijama pokrenuto, navedite više informacija.
Datum i vrijeme početka incidenta: datum i vrijeme kada je incident počeo, ako su poznati.
Datum i vrijeme kada je incident riješen ili se očekuje da će biti riješen: navedite datum i vrijeme kada je incident stavljen pod kontrolu ili se očekuje da će biti stavljen pod kontrolu i kada je redovno poslovanje ponovno uspostavljeno ili se očekuje da će biti ponovno uspostavljeno.
Zahvaćena funkcionalna područja: navedite korak ili korake u postupku plaćanja na koje je incident utjecao, kao što su autentifikacija/autorizacija, komunikacija, obračun, izravna namira, posredna namira i drugo.

Autentifikacija/autorizacija: postupci koji PPU-u omogućuju provjeru identiteta korisnika platnih usluga ili valjanosti upotrebe određenog platnog instrumenta, uključujući upotrebu personaliziranih sigurnosnih podataka korisnika i davanje suglasnosti korisnika platnih usluga (ili treće strane koja djeluje u ime tog korisnika) za prijenos novčanih sredstava.

Komunikacija: protok informacija u svrhu identifikacije, autentifikacije, obavješćivanja i informiranja koji se odvijaju između PPU-a koji vodi račun i pružatelja usluge iniciranja plaćanja, pružatelja usluge informiranja o računu, platitelja, primatelja plaćanja i drugih PPU-ova.

Obračun: proces prijenosa, poravnanja i u nekim slučajevima potvrđivanja naloga za prijenos prije namire, što može uključivati netiranje naloga i utvrđivanje konačnih položaja za namiru.

Izravna namira: dovršetak transakcije ili obrade s ciljem ispunjavanja obveza sudionika prijenosom novčanih sredstava kada zahvaćeni PPU sâm izvršava prijenos.

Neizravna namira: dovršetak transakcije ili obrade s ciljem ispunjavanja obveza sudionika prijenosom novčanih sredstava kada drugi PPU izvršava prijenos u ime zahvaćenog PPU-a.

Drugo: zahvaćeno funkcionalno područje nije nijedno od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Izmjene prethodnih izvješća: navedite promjene u informacijama dostavljenima u prethodnim izvješćima u vezi s istim incidentom (odnosno, u početnom ili, ako je to primjenjivo, prijelaznom izvješću).

B 2 – Klasifikacija incidenta / informacije o incidentu

Zahvaćene transakcije: PPU-ovi trebaju navesti pragove koji su dosegnuti ili je vjerojatno da će biti dosegnuti zbog incidenta, ako oni postoje, i povezane statističke podatke: broj zahvaćenih transakcija, postotak zahvaćenih transakcija u ukupnom broju platnih transakcija izvršenih istom platnom uslugom koja je zahvaćena incidentom te ukupnu vrijednost tih transakcija. PPU-ovi trebaju navesti konkretne vrijednosti tih varijabli, koje mogu biti stvarne ili procijenjene. Opće je pravilo da PPU-ovi trebaju smatrati da su „zahvaćene transakcije" sve domaće i prekogranične transakcije na koje incident izravno ili neizravno utječe ili će vjerojatno utjecati te, osobito, transakcije koje se neće moći inicirati ili obraditi, transakcije s promijenjenim sadržajem poruke o plaćanju i transakcije inicirane s namjerom prijevare (neovisno o tome jesu li novčana sredstva vraćena ili ne). Nadalje, PPU-ovi trebaju smatrati da je „redovan volumen platnih transakcija" godišnji dnevni prosjek domaćih i prekograničnih platnih transakcija izvršenih istim platnim uslugama koje su zahvaćene incidentom, pri čemu prethodna godina služi kao referentno razdoblje za izračune. Ako PPU-ovi smatraju da dobiveni broj nije reprezentativan (npr. zbog sezonskog utjecaja), umjesto tog izračuna trebaju upotrijebiti drugi, reprezentativniji izračun i obavijestiti nadležno tijelo o osnovnim razlozima za taj pristup u polju „Napomene". U slučajevima kada incident utječe na platne transakcije u valutama koje nisu euro, pri izračunu pragova i izvješćivanju o vrijednosti zahvaćenih transakcija PPU-ovi trebaju iznos transakcija u valuti koja nije euro pretvoriti u euro primjenom dnevnog referentnog deviznog tečaja ESB-a za dan koji prethodi danu podnošenja izvješća o incidentu.

Zahvaćeni korisnici platnih usluga: PPU-ovi trebaju navesti pragove koji su dosegnuti ili je vjerojatno da će biti dosegnuti zbog incidenta, ako oni postoje, i povezane statističke podatke: ukupan broj korisnika platnih usluga koji su zahvaćeni i postotak zahvaćenih korisnika platnih usluga u ukupnom broju korisnika platnih usluga. PPU-ovi trebaju navesti konkretne vrijednosti tih varijabli, koje mogu biti stvarne ili procijenjene. PPU-ovi trebaju smatrati da su „zahvaćeni korisnici platnih usluga" svi klijenti (domaći ili međunarodni, potrošači ili poduzeća) koji imaju ugovor s zahvaćenim pružateljem platnih usluga kojim im se odobrava pristup zahvaćenoj platnoj usluzi i koji su pretrpjeli ili će vjerojatno pretrpjeti posljedice incidenta. PPU-ovi trebaju procijeniti broj korisnika platnih usluga koji su se možda koristili platnom uslugom tijekom trajanja incidenta na temelju prošle aktivnosti. U slučaju grupa, svaki PPU treba uzeti u obzir samo svoje korisnike platnih usluga. Ako PPU nudi operativne usluge drugim subjektima, taj PPU treba uzeti u obzir samo svoje korisnike platnih usluga (ako oni postoje), a PPU-ovi koji primaju te operativne usluge također trebaju ocijeniti incident u odnosu na vlastite korisnike platnih usluga. Nadalje, PPU-ovi trebaju smatrati da je ukupan broj korisnika platnih usluga zbroj domaćih i prekograničnih korisnika platnih usluga koji su ugovorno vezani za njih u trenutku incidenta (ili, kao alternativa, njihov najnoviji dostupan broj) i koji su imali pristup zahvaćenoj platnoj usluzi neovisno o njihovoj veličini i neovisno o tome smatraju li se aktivnim ili pasivnim korisnicima platnih usluga.

Povreda sigurnosti mrežnih ili informacijskih sustava: PPU-ovi trebaju utvrditi je li neka zlonamjerna radnja ugrozila dostupnost, autentičnost, cjelovitost ili povjerljivost mrežnih ili informacijskih sustava (uključujući podatke) povezanih s pružanjem platnih usluga.

Razdoblje prekida rada usluge: PPU-ovi trebaju navesti je li prag dosegnut ili je vjerojatno da će biti dosegnut zbog incidenta te povezani statistički podatak: ukupno razdoblje prekida rada usluge. PPU-ovi trebaju navesti konkretnu vrijednost te varijable, koja može biti stvarna ili procijenjena. PPU-ovi trebaju razmotriti koliko će trajati prekid ili vjerojatni prekid bilo kojeg zadatka, procesa ili kanala povezanog s

pružanjem platnih usluga zbog kojeg će biti spriječeni i. iniciranje i/ili izvršavanje platne usluge i/ili ii. pristup računu za plaćanje. PPU-ovi trebaju računati razdoblje prekida rada usluge od trenutka u kojem prekid počinje te trebaju uzeti u obzir vremenska razdoblja kada su otvoreni za poslovanje, a koja su potrebna za izvršavanje platnih usluga, kao i vrijeme zatvaranja i razdoblja održavanja, ako je to relevantno i primjenjivo. Ako pružatelji platnih usluga ne mogu utvrditi kada je počelo razdoblje prekida rada usluge, iznimno trebaju računati razdoblje prekida rada usluge od trenutka u kojem je prekid rada otkriven.

Ekonomski učinak: PPU-ovi trebaju navesti je li prag dosegnut ili je vjerojatno da će biti dosegnut zbog incidenta i povezane statističke podatke: izravne troškove i neizravne troškove. PPU-ovi trebaju navesti konkretne vrijednosti tih varijabli, koje mogu biti stvarne ili procijenjene. PPU-ovi trebaju razmotriti troškove koji se mogu izravno povezati s incidentom i one koji su neizravno povezani s incidentom. PPU-ovi trebaju, među ostalim, uzeti u obzir oduzeta novčana sredstva ili imovinu, troškove zamjene hardvera ili softvera, druge troškove forenzičnih ili korektivnih radnji, naknade zbog neispunjenja ugovornih obveza, kazne, vanjske odgovornosti i izgubljene prihode. PPU-ovi trebaju uzeti u obzir samo one neizravne troškove koji su već poznati ili za koje je vrlo vjerojatno da će nastati. U slučajevima kada su troškovi izraženi u valutama koje nisu euro, pri izračunu praga i izvješćivanju o vrijednosti ekonomskog učinka PPU-ovi trebaju iznos troškova u valuti koja nije euro pretvoriti u euro primjenom dnevnog referentnog deviznog tečaja ESB-a za dan koji prethodi danu podnošenja izvješća o incidentu.

> **Izravni troškovi:** troškovi (u eurima) izravno uzrokovani incidentom, uključujući troškove ispravljanja incidenta (npr. oduzeta sredstva ili imovina, troškovi zamjene hardvera i softvera, naknade zbog neispunjenja ugovornih obveza).
>
> **Neizravni troškovi:** troškovi (u eurima) neizravno uzrokovani incidentom (npr. troškovi odštete/naknade klijentima, mogući pravni troškovi).

Visoka razina unutarnje eskalacije: PPU-ovi trebaju razmotriti je li, zbog utjecaja incidenta na usluge povezane s plaćanjem, upravljačko tijelo, kako je definirano Smjernicama EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima, u skladu sa smjernicom 60. točkom (d) Smjernica EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima, obaviješteno ili će vjerojatno biti obaviješteno o incidentu izvan bilo kojeg postupka periodičnog izvješćivanja te redovito tijekom trajanja incidenta. Nadalje, pružatelji platnih usluga trebaju razmotriti je li, zbog utjecaja incidenta na usluge povezane s plaćanjem, već aktivirano krizno stanje, odnosno je li vjerojatno da će se ono aktivirati.

Potencijalno zahvaćeni drugi PPU-ovi ili relevantne infrastrukture: PPU-ovi trebaju procijeniti utjecaj incidenta na financijsko tržište, koje obuhvaća infrastrukture financijskog tržišta i/ili platne sheme koje im pružaju potpora te druge PPU-ove. PPU-ovi osobito trebaju ocijeniti je li se incident već proširio na druge PPU-ove, odnosno hoće li do toga vjerojatno doći, je li utjecao ili će vjerojatno utjecati na neometano funkcioniranje infrastruktura financijskog tržišta te je li ugrozio ili će vjerojatno ugroziti pravilno funkcioniranje financijskog sustava kao cjeline. PPU-ovi trebaju imati na umu različita pitanja, primjerice: jesu li zahvaćena komponenta/softver zaštićeni autorskim pravom ili javno dostupni, je li kompromitirana mreža unutarnja ili vanjska i je li PPU prestao ili će vjerojatno prestati ispunjavati svoje obveze u infrastrukturama financijskog tržišta u kojima je član.

Učinak na reputaciju: PPU-ovi trebaju razmotriti mjeru u kojoj je incident, prema njihovom saznanju, postao ili je vjerojatno da će postati vidljiv na tržištu. PPU-ovi osobito trebaju razmotriti vjerojatnost da će incident prouzročiti štetu društvu, što je dobar indikator potencijalnog utjecaja na njihovu reputaciju. PPU-ovi trebaju razmotriti i. jesu li se korisnici platnih usluga i/ili drugi PPU-ovi žalili na negativan učinak incidenta; ii. je li incident utjecao na vidljiv postupak povezan s platnim uslugama te će stoga vjerojatno biti pokriven u medijima ili je već pokriven u medijima (uzimajući u obzir ne samo tradicionalne medije, kao što su novine, nego i blogove, društvene mreže itd.; međutim, pokrivenost u medijima u ovom kontekstu ne podrazumijeva tek nekoliko negativnih komentara pratitelja, treba postojati valjano izvješće ili značajan broj negativnih komentara/upozorenja); iii. je li došlo do propusta u ispunjavanju ugovornih obveza ili će vjerojatno doći do propusta u njihovu ispunjavanju, što je dovelo do pokretanja

pravnih radnji protiv pružatelja platnih usluga; iv. je li došlo do propusta u ispunjavanju regulatornih obveza, što je dovelo do toga da su nadzorne mjere ili sankcije javno objavljene ili će vjerojatno biti javno objavljene; te v. je li i prije došlo do incidenta slične vrste.

B 3 – Opis incidenta

Vrsta incidenta: operativni ili sigurnosni. Dodatno objašnjenje navodi se u odgovarajućem polju u početnom izvješću.

Uzrok incidenta: navedite uzrok incidenta ili, ako on još nije poznat, najvjerojatniji uzrok. Može se odabrati više odgovora.

Pod istragom: označite okvir ako uzrok još nije utvrđen.

Zlonamjerna radnja: radnje ciljano usmjerene na PPU. To obuhvaća zlonamjerne kodove, prikupljanje informacija, upade, distribuirane napade / uskraćivanje usluga (D/DoS), namjerne unutarnje radnje, namjerno vanjsko fizičko oštećenje, sigurnost informacijskog sadržaja, prijevarne radnje i drugo. Za dodatne pojedinosti vidjeti dio C2 ovog obrasca.

Pogreška u procesu: incident je uzrokovan lošim dizajnom ili izvršenjem procesa plaćanja, kontrole procesa i/ili potpornih procesa (npr. proces promjene/migracije, testiranje, konfiguracija, kapacitet, praćenje).

Kvar sustava: uzrok incidenta povezan je s neprikladnim dizajnom, izvršenjem, komponentama, specifikacijama, integracijom ili složenošću sustava, mreža, infrastruktura i baza podataka koje podupiru aktivnosti plaćanja.

Ljudske pogreške: incident je uzrokovan nenamjernom pogreškom osobe tijekom plaćanja (npr. prijenos pogrešne skupne datoteke plaćanja u sustav plaćanja) ili u vezi s njime (npr. došlo je do slučajnog prekida napajanja, pa je plaćanje stavljeno na čekanje).

Vanjski događaji: uzrok je povezan s događajima na koje organizacija općenito nema utjecaj (npr. prirodne katastrofe, neispravnost u radu tehničkog pružatelja usluga).

Drugo: uzrok incidenta nije nijedan od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Je li incident na vas utjecao izravno ili neizravno putem pružatelja usluga?: ako su te informacije dostupne, navedite je li incident usmjeren izravno na PPU ili neizravno utječe na njega putem treće strane. U slučaju neizravnog utjecaja, navedite naziv jednog ili više pružatelja usluga.

B 4 – Učinak incidenta

Opći učinak: navedite koja su svojstva zahvaćena operativnim ili sigurnosnim incidentom. Može se odabrati više odgovora.

Cjelovitost: svojstvo čuvanja točnosti i potpunosti imovine (uključujući podatke).

Dostupnost: svojstvo dostupnosti i mogućnosti korištenja uslugama povezanim s plaćanjem korisnicima platnih usluga u skladu s unaprijed određenim prihvatljivim razinama

Povjerljivost: svojstvo uskraćivanja dostupnosti ili otkrivanja informacija neovlaštenim fizičkim osobama, subjektima ili procesima.

Autentičnost: svojstvo izvora da je upravo ono što tvrdi da jest.

Zahvaćeni komercijalni kanali: navedite kanal ili kanale za interakciju s korisnicima platnih usluga na koje je incident utjecao. Može se označiti više stavki.

Podružnice: mjesto poslovanja (koje nije mjesto uprave) koje je dio PPU-a, nema pravnu osobnost i izravno provodi određene ili sve transakcije svojstvene poslovanju PPU-a. Sva mjesta poslovanja koja je u istoj državi članici osnovao PPU s mjestom uprave u drugoj državi članici trebaju se smatrati jednom podružnicom.

E-bankarstvo: upotreba računala za izvršenje financijskih transakcija putem interneta.

Telefonsko bankarstvo: upotreba telefona za izvršenje financijskih transakcija.

Mobilno bankarstvo: upotreba određenih aplikacija za bankarstvo na pametnom telefonu ili sličnom uređaju za izvršenje financijskih transakcija.

Bankomati: elektromehanički uređaji koji omogućuju korisnicima platnih usluga podizanje gotovog novca s njihovih računa i/ili pristup drugim uslugama.

Prodajno mjesto: fizički prostor trgovca u kojem je platna transakcija inicirana.

E-trgovina: platna transakcija inicirana je na virtualnom prodajnom mjestu (npr. za plaćanja inicirana putem interneta upotrebom kreditnih transfera, platnih kartica, prijenosa elektroničkog novca između računa elektroničkog novca).

Drugo: zahvaćeni komercijalni kanal nije nijedan od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Zahvaćene platne usluge: navedite platne usluge koje zbog incidenta ne rade ispravno. Može se označiti više stavki.

Polaganje gotovog novca na račun za plaćanje: predavanje gotovog novca PPU-u kako bi se uplatio na račun za plaćanje.

Podizanje gotovog novca s računa za plaćanje: zahtjev koji je PPU zaprimio od korisnika platnih usluga za isplatu gotovog novca i terećenje njegova/njezina računa za plaćanje odgovarajućim iznosom.

Postupci koji su potrebni za vođenje računa za plaćanje: radnje koje se moraju izvršiti kako bi se aktivirao, deaktivirao i/ili održavao račun za plaćanje (npr. otvaranje, blokiranje).

Prihvaćanje platnih instrumenata: platna usluga u okviru koje PPU s primateljem plaćanja ugovara prihvaćanje i obradu platnih transakcija što dovodi do prijenosa novčanih sredstava primatelju plaćanja.

Kreditni transferi: platna usluga kojom se račun za plaćanje primatelja plaćanja odobrava za platnu transakciju ili niz platnih transakcija na teret platiteljeva računa za plaćanje, od strane PPU-a kod kojeg se vodi platiteljev račun za plaćanje, na osnovi upute koju daje platitelj.

Izravna terećenja: platna usluga za terećenje platiteljeva računa za plaćanje, pri čemu je platnu transakciju inicirao primatelj plaćanja na temelju suglasnosti koju je platitelj dao primatelju plaćanja, PPU-u primatelja plaćanja ili PPU-u samog platitelja.

Kartična plaćanja: platna usluga koja se temelji na infrastrukturi i pravilima poslovanja kartične platne sheme za izvršavanje platne transakcije bilo kojom karticom, telekomunikacijskim, digitalnim ili IT uređajem ili softverom ako je time izvršena transakcija debitnom ili kreditnom karticom. Platne transakcije na temelju kartica isključuju transakcije na temelju drugih vrsta platnih usluga.

Izdavanje platnih instrumenata: platna usluga koju pruža PPU ugovarajući s platiteljem da će mu pružiti platni instrument za iniciranje i obradu platnih transakcija.

Novčana pošiljka: platna usluga u okviru koje se od platitelja primaju novčana sredstva bez otvaranja računa za plaćanje na ime platitelja ili primatelja plaćanja, s isključivom svrhom prijenosa odgovarajućeg iznosa primatelju plaćanja ili drugom PPU-u koji djeluje u ime primatelja plaćanja, i/ili u okviru koje se takva novčana sredstva primaju u ime primatelja plaćanja te mu se stavljaju na raspolaganje.

Usluge iniciranja plaćanja: usluga iniciranja naloga za plaćanje na zahtjev korisnika platnih usluga u odnosu na račun za plaćanje koji vodi drugi PPU.

Usluge informiranja o računu: online platne usluge kojima se pružaju konsolidirane informacije o jednom ili više računa za plaćanje koje korisnik platnih usluga ima ili kod drugog PPU-a ili kod više PPU-ova.

B 5 – Ublažavanje incidenta

Koje su radnje/mjere dosad poduzete ili se namjeravaju poduzeti za oporavak od incidenta?: navedite pojedinosti o radnjama koje su poduzete ili se namjeravaju poduzeti za privremeno rješavanje incidenta.

Je li aktiviran plan kontinuiteta poslovanja i/ili plan oporavka informacijskog sustava?: navedite jesu li aktivirani ili ne; ako jesu, navedite najvažnije pojedinosti o tome (tj. kada su aktivirani i od čega se ti planovi sastoje).

C – Konačno izvješće

C 1 – Opće informacije

Ažuriranje informacija iz početnog izvješća i prijelaznog/prijelaznih izvješća (sažetak): navedite dodatne informacije o incidentu, uključujući konkretne izmjene informacija navedenih u prijelaznom izvješću. Navedite i sve ostale relevantne informacije.

Jesu li ponovno uspostavljene izvorne kontrole?: navedite je li PPU u bilo kojem trenutku tijekom incidenta morao ukinuti ili oslabiti određene kontrole. Ako jest, navedite jesu li te kontrole ponovno uspostavljene; u protivnom u polju za slobodan unos teksta objasnite koje kontrole nisu ponovno uspostavljene te dodatni rok potreban za njihovu ponovnu uspostavu.

C 2 – Analiza temeljnog uzroka i daljnje mjere

Što je temeljni uzrok, ako je već poznat?: navedite temeljni uzrok incidenta ili, ako još nije poznat, najvjerojatniji temeljni uzrok. Može se odabrati više odgovora. (Imajte na umu da je glavni uzrok potrebno razlikovati od učinka incidenta.)

Zlonamjerna radnja: vanjske ili unutarnje radnje ciljano usmjerene protiv PPU-a. Podijeljene su u sljedeće kategorije:

Zlonamjerni kod: npr. virus, crv, trojanski softver, špijunski softver.

Prikupljanje informacija: npr. skeniranje, otkrivanje sadržaja, društveni inženjering.

Upadi: npr. narušena pouzdanost povlaštenog računa, narušena pouzdanost nepovlaštenog računa, narušena pouzdanost aplikacije, bot.

Distribuirani napad / uskraćivanje usluga (D/DoS): pokušaj da se mrežna usluga učini nedostupnom tako da je se preplavi prometom iz velikog broja izvora.

Namjerne unutarnje radnje: npr. sabotaža, krađa.

Namjerno vanjsko fizičko oštećenje: npr. sabotaža, fizički napad prostora/podatkovnih centara.

Sigurnost informacijskog sadržaja: neovlašteni pristup informacijama, neovlaštene izmjene informacija).

Prijevarne radnje: neovlaštena uporaba resursa, autorskih prava, napad lažnim predstavljanjem, krađa identiteta.

Drugo (navesti): uzrok incidenta nije nijedan od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Pogreška u procesu: incident je uzrokovan lošim dizajnom ili izvršenjem procesa plaćanja, kontrole procesa i/ili potpornih procesa (npr. proces promjene/migracije, testiranje, konfiguracija, kapacitet, praćenje). Podijeljene su u sljedeće kategorije:

Manjkavo praćenje i nadzor: npr. u odnosu na tekuće operacije, datume isteka certifikata, datume isteka licencija, datume isteka zakrpa, utvrđene maksimalne vrijednosti brojača, razine popunjenosti baze podataka, upravljanje korisničkim pravima, načelo dvostruke kontrole.

Problemi u komunikaciji: npr. između sudionika na tržištu ili unutar organizacije.

Neispravan rad: npr. ne provodi se razmjena certifikata, predmemorija je puna.

Neodgovarajuće upravljanje promjenama: npr. neidentificirane pogreške konfiguracije, uvođenje promjena koje uključuju ažuriranja, problemi s održavanjem, neočekivane pogreške.

Neprimjerenost internih postupaka i dokumentacije: npr. nedostatak transparentnosti u pogledu funkcionalnosti, procesa i pojave kvarova, nedostatak dokumentacije.

Problemi s oporavkom: npr. upravljanje izvanrednim situacijama, neprimjereno udvajanje.

Drugo (navesti): uzrok incidenta nije nijedan od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Kvar sustava: uzrok incidenta povezan je s neprikladnim dizajnom, izvršenjem, komponentama, specifikacijama, integracijom ili složenosti sustava, mreža, infrastruktura i baza podataka koje podupiru aktivnosti plaćanja. Podijeljene su u sljedeće kategorije:

Kvar hardvera: kvar fizičke tehnološke opreme na kojoj se odvijaju procesi i/ili na koju se pohranjuju podaci potrebni PPU-ima za izvršenje aktivnosti povezanih s plaćanjem (npr. kvar tvrdih diskova, podatkovnih centara, druge infrastrukture).

Mrežni kvar: kvar javnih ili privatnih telekomunikacijskih mreža koje omogućavaju razmjenu podataka i informacija (npr. internet) tijekom procesa plaćanja.

Problemi s bazom podataka: podatkovna struktura u kojoj se pohranjuju osobni podaci i podaci o plaćanju koji su potrebni za izvršenje platnih transakcija.

Kvar softvera/aplikacije: kvarovi programa, operacijskih sustava itd. koji podupiru pružanje platnih usluga PPU-a (npr. neispravan rad, nepoznate funkcije).

Fizičko oštećenje: npr. nenamjerno oštećenje uzrokovano neprikladnim uvjetima, građevinskim radovima.

Drugo (navesti): uzrok incidenta nije nijedan od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Ljudska pogreška: incident je uzrokovan nenamjernom pogreškom osobe bilo tijekom plaćanja (npr. prijenos pogrešne skupne datoteke plaćanja u sustav plaćanja) ili u vezi s njime (npr. došlo je do slučajnog prekida napajanja, pa je plaćanje stavljeno na čekanje). Podijeljene su u sljedeće kategorije:

Nenamjerne: npr. greške, pogreške, propusti, manjak iskustva i znanja.

Propust u djelovanju: npr. zbog manjka vještina, znanja, iskustva i osviještenosti.

Nedostatni resursi: npr. nedostatak ljudskih resursa, dostupnost osoblja.

Drugo (navesti): uzrok incidenta nije nijedan od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Vanjski događaj: uzrok je povezan s događajima koji su općenito izvan kontrole organizacije. Podijeljeni su u sljedeće kategorije:

Pogreška dobavljača/pružatelja tehničkih usluga: npr. prekid napajanja, prekid internetske veze, pravna pitanja, poslovna pitanja, ovisnosti o uslugama.

Viša sila: npr. pogreške u napajanju, požari, prirodni uzroci kao što su potresi, poplave, obilne oborine, jaki vjetar.

Drugo (navesti): uzrok incidenta nije nijedan od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Drugo: uzrok incidenta nije nijedan od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Ostale relevantne informacije o temeljnom uzroku: navedite sve dodatne pojedinosti o temeljnom uzroku, uključujući preliminarne zaključke izvedene iz analize temeljnih uzroka.

Glavne korektivne radnje/mjere koje su poduzete ili se namjeravaju poduzeti za sprečavanje ponavljanja incidenta u budućnosti, ako su već poznate: opišite glavne radnje koje su poduzete ili se namjeravaju poduzeti za sprečavanje ponavljanja incidenta u budućnosti.

C 3 – Dodatne informacije

Jesu li drugi PPU-ovi obaviješteni o incidentu?: navedite pregled PPU-ova s kojima se formalno ili neformalno kontaktiralo radi informiranja o incidentu i u njemu navedite pojedinosti o informiranim PPU-ovima, informacije koje su se podijelile s njima i osnovne razloge za dijeljenje tih informacija.
Jesu li poduzete pravne radnje protiv PPU-a?: navedite je li u trenutku podnošenja konačnog izvješća bila poduzeta neka pravna radnja protiv PPU-a (npr. sudski postupak ili gubitak licence) zbog incidenta.
Procjena djelotvornosti poduzetih mjera: ako je to moguće, navedite samoprocjenu djelotvornosti mjera poduzetih tijekom trajanja incidenta, uključujući sva iskustva stečena tijekom incidenta.