EBA/GL/2017/10

19/12/2017

Smjernice

o izvješćivanju o značajnim incidentima u skladu s Direktivom (EU) 2015/2366 (PSD2)

1. Obveze usklađivanja i izvješćivanja

Status ovih smjernica

1. Ovaj dokument sadrži smjernice izdane na temelju članka 16. Uredbe (EU) br. 1093/2010[1]. U skladu s člankom 16. stavkom 3. Uredbe (EU) br. 1093/2010 nadležna tijela i financijske institucije moraju ulagati napore da se usklade s ovim smjernicama.

2. Smjernice iznose 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 19/02/2018. U slučaju izostanka takve obavijesti unutar ovog roka EBA će smatrati da nadležna tijela nisu usklađena. Obavijesti se dostavljaju slanjem ispunjenog obrasca koji se nalazi na internetskoj stranici EBA-e na adresu compliance@eba.europa.eu s uputom „EBA/GL/2017/10”. Obavijesti bi trebale slati osobe s odgovarajućom nadležnošću za izvješćivanje o usklađenosti u ime svojih nadležnih tijela. Svaka se promjena statusa usklađenosti također mora prijaviti EBA-i.

4. Obavijesti će biti objavljene na EBA-inoj internetskoj stranici 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. Ove Smjernice pripremljene su 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 (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 će, u skladu s člankom 96. stavkom 2. prethodno navedene direktive, 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 (EU) 2015/2366.

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).

Adresati

12. Prva grupa Smjernica (4. poglavlje) odnosi se na pružatelje platnih usluga kako su definirani u članku 4. stavku 11. Direktive (EU) 2015/2366 i kako se na njih upućuje u članku 4. stavku 1. Uredbe (EU) 1093/2010.

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

Definicije

14. Ako nije drugačije naznačeno, pojmovi upotrijebljeni i utvrđeni u Direktivi (EU) 2015/2366 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, autentičnost i/ili kontinuitet usluga povezanih s plaćanjem.
Cjelovitost	Svojstvo čuvanja točnosti i potpunosti imovine (uključujući podataka).
Dostupnost	Svojstvo dostupnosti i mogućnosti korištenja uslugama povezanim s plaćanjem korisnicima 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.
Kontinuitet	Svojstvo potpune dostupnosti procesa, zadataka i imovine organizacije potrebnih za pružanje usluga povezanih s plaćanjem i njihovo funkcioniranje na prihvatljivim unaprijed određenim razinama.
Usluge povezane s plaćanjem	Bilo koja poslovna aktivnost u smislu članka 4. stavka 3. PSD2 i sva tehnička podrška potrebna za ispravno pružanje platnih usluga.

3. Provedba

Datum primjene

15. Ove smjernice primjenjuju se od 13. siječnja 2018.

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

iii. Razdoblje prekida rada usluge

Pružatelji platnih usluga trebaju utvrditi vremensko 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. točke 13. PSD2.

iv. 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).

v. Visoka razina unutarnje eskalacije

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

vi. 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 kartične platne sheme.

vii. 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 incident izravno ili neizravno utječe ili će vjerojatno utjecati te osobito one transakcije koje se neće moći 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).

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. radi sezonskog utjecaja), umjesto tog izračuna trebaju upotrijebiti drugi, reprezentativniji izračun i obavijestiti nadležno tijelo o osnovnim razlozima za taj pristup u odgovarajućem polju obrasca (vidi Prilog 1.).

ii. Zahvaćeni korisnici platnih usluga

Pružatelji platnih usluga 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. 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.

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. Razdoblje prekida rada usluge

Pružatelji platnih usluga trebaju razmotriti koliko će trajati prekid ili vjerojatni prekid bilo kojeg zadatka, procesa ili kanala povezanog s pružanjem platnih usluga, koji će, stoga, 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.

iv. 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.

v. *Visoka razina unutarnje eskalacije*

Pružatelji platnih usluga trebaju razmotriti je li, zbog utjecaja incidenta na usluge povezane s plaćanjem, član uprave odgovoran za informacijski sustav (ili osoba na sličnom položaju) obaviješten o incidentu, odnosno hoće li ga se vjerojatno obavijestiti o njemu, izvan bilo kojeg postupka periodičnog izvješćivanja i 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.

vi. *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 kartične 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.

vii. *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

smatrati vjerojatnost da će incident prouzročiti štetu društvu dobrim indikatorom potencijalnog utjecaja na njegovu reputaciju. Pružatelji platnih usluga trebaju razmotriti (i) je li incident utjecao na vidljivi proces i je li 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.), (ii) je li došlo do propusta u ispunjavanju regulatornih obveza ili je vjerojatno da će do njega doći, (iii) jesu li prekršene ili je vjerojatno da će se prekršiti sankcije te (iv) je li se i prije dogodila ista vrsta incidenta.

1.4. Pružatelji platnih usluga trebaju procijeniti incident tako da odrede za svaki kriterij jesu li se već dostigli relevantni pragovi iz Tablice 1., odnosno je li vjerojatno da će se dostići prije nego što se incident riješi.

Tablica 1.: Pragovi

Kriterij	Niža razina utjecaja	Viša razina utjecaja
Zahvaćene transakcije	> 10 % redovnog volumena transakcija pružatelja platnih usluga (u smislu broja transakcija) **i** > 100 000 EUR	> 25 % redovnog volumena transakcija pružatelja platnih usluga (u smislu broja transakcija) **ili** > 5 milijuna EUR
Zahvaćeni korisnici platnih usluga	> 5 000 **i** > 10 % korisnika platnih usluga pružatelja platnih usluga	> 50 000 **ili** > 25 % korisnika platnih usluga pružatelja platnih usluga
Razdoblje prekida rada usluge	> 2 sata	Nije primjenjivo
Ekonomski učinak	Nije primjenjivo	> maks. (0,1 % osnovnog kapitala,* 200 000 EUR) **ili** > 5 milijuna 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

* 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).

Smjernica 2.: postupak obavješćivanja

2.1. Pružatelji platnih usluga trebaju prikupiti sve relevantne informacije, pripremiti izvješće o incidentu s pomoću obrasca iz Priloga 1. i podnijeti ga nadležnom tijelu u matičnoj državi članici. Pružatelji platnih usluga trebaju ispuniti obrazac pridržavajući se uputa navedenih u Prilogu 1.

2.2. Pružatelji platnih usluga trebaju upotrijebiti isti obrazac za obavješćivanje nadležnog tijela tijekom trajanja incidenta (tj. za početno, prijelazno i konačno izvješće kako je opisano u odlomcima od 2.7 do 2.21). Pružatelji platnih usluga trebaju obrazac ispunjavati postupno i na najbolji mogući način kako sve više informacija postaje dostupno tijekom provođenja unutarnjih istraga.

2.3. Pružatelji platnih usluga osim toga trebaju nadležnom tijelu u svojoj matičnoj državi članici podnijeti primjerak obavijesti koja je dostavljena (ili će se dostaviti) korisnicima, ako je primjenjivo, u skladu s odredbama drugog podstavka stavka 1. članka 96. PSD2 čim ona postane dostupna.

2.4. Pružatelji platnih usluga trebaju nadležnom tijelu u matičnoj državi članici dostaviti sve dodatne informacije, ako su dostupne i ako ih nadležno tijelo smatra relevantnima, tako da dopunsku dokumentaciju prilože standardiziranom obrascu u obliku jednog priloga ili više njih.

2.5. 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.

2.6. 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 otkrije značajan operativni ili sigurnosni incident.

2.8. Pružatelji platnih usluga trebaju podnijeti početno izvješće nadležnom tijelu unutar četiri sata od trenutka otkrivanja značajnog operativnog ili sigurnosnog incidenta ili, ako se zna da kanali za izvješćivanje nadležnog tijela nisu dostupni ili funkcionalni u danom trenutku, čim oni ponovno postanu dostupni ili funkcionalni.

2.9. Pružatelji platnih usluga osim toga trebaju podnijeti početno izvješće nadležnom tijelu u matičnoj državi članici kada incident koji prethodno nije bio značajan postane značajan incident. U tom slučaju pružatelji platnih usluga trebaju podnijeti početno izvješće nadležnom tijelu odmah 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 ili funkcionalni.

2.10. Pružatelji platnih usluga trebaju svojim početnim izvješćima obuhvatiti i informacije u zaglavlju (tj. dio A obrasca) te u njima opisati neke osnovne značajke incidenta i njegove očekivane posljedice na temelju informacija dostupnih odmah po otkrivanju ili reklasifikaciji incidenta. Pružatelji platnih usluga trebaju pribjeći procjenama kada im nisu dostupni stvarni podaci. Pružatelji platnih usluga trebaju u svojim početnim izvješćima navesti i datum sljedećeg ažuriranja koje bi se trebalo obaviti što je prije moguće, a nikako kasnije od tri radna dana.

Prijelazno izvješće

2.11. Pružatelji platnih usluga trebaju podnijeti prijelazno izvješće svaki put kada smatraju da postoje relevantne novosti o statusu, a najkasnije do datuma za koji je zakazano sljedeće ažuriranje navedeno u prethodnom izvješću (bilo početnom izvješću ili prethodnom prijelaznom izvješću).

2.12. Pružatelji platnih usluga trebaju podnijeti nadležnom tijelu prvo prijelazno izvješće s detaljnijim opisom incidenta i njegovih posljedica (dio B obrasca). Nadalje, pružatelji platnih usluga trebaju pripremiti dodatna prijelazna izvješća ažuriranjem informacija koje su već pružene u dijelu A i B obrasca u najmanju ruku kada saznaju za nove relevantne informacije ili značajne promjene do kojih je došlo od prethodne obavijesti (npr. je li incident eskalirao ili se smanjio, jesu li otkriveni novi uzroci ili su poduzete radnje za rješavanje problema). Pružatelji platnih usluga trebaju u svakom slučaju pripremiti prijelazno izvješće na zahtjev nadležnog tijela u matičnoj državi članici.

2.13. Baš kao i u slučaju početnih izvješća, kada nisu dostupni stvarni podaci, pružatelji platnih usluga trebaju pribjeći procjenama.

2.14. Nadalje, pružatelji platnih usluga trebaju u svakom izvješću navesti i datum sljedećeg ažuriranja koje bi se trebalo obaviti što je prije moguće, a nikako kasnije od tri radna dana. Ako nije u mogućnosti obaviti ažuriranje do procijenjenog datuma, pružatelj platnih usluga treba obavijestiti nadležno tijelo o razlozima odgode, predložiti novi vjerojatan datum podnošenja (ne kasnije od tri radna dana) i poslati novo prijelazno izvješće kojim se ažuriraju isključivo informacije o procijenjenom datumu sljedećeg ažuriranja.

2.15. Pružatelji platnih usluga trebaju poslati posljednje prijelazno izvješće kada se ponovno uspostavi redovito poslovanje, a njime obavješćuju nadležno tijelo 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 sporazumom o razini usluga (SLA) u pogledu vremena obrade, kapaciteta, sigurnosnih zahtjeva itd. i kada se više ne provode izvanredne mjere.

2.16. Ako se redovito poslovanje ponovno uspostavi unutar četiri sata od otkrivanja incidenta, pružatelji platnih usluga trebaju nastojati istodobno podnijeti i početno i posljednje prijelazno izvješće (tj. ispuniti dio A i B obrasca) unutar tog roka od četiri sata.

Konačno izvješće

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

2.18. Pružatelji platnih usluga trebaju podnijeti konačno izvješće nadležnom tijelu najkasnije dva tjedna 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) trebaju se obratiti nadležnom tijelu prije njegova isteka i navesti prikladno opravdanje za odgodu, kao i novi procijenjeni datum konačnog izvješća.

2.19. Ako mogu pružiti sve potrebne informacije u konačnom izvješću (tj. dijelu C obrasca) u roku od četiri sata od otkrivanja incidenta, pružatelji platnih usluga trebaju nastojati navesti u svom početnom izvješću informacije povezane s početnim, posljednjim prijelaznim i konačnim izvješćem.

2.20. Pružatelji platnih usluga trebaju nastojati navesti u svojim konačnim izvješćima cjelovite informacije, tj. (i) stvarne podatke o utjecaju umjesto procijenjenih (kao i sva druga ažuriranja potrebna u dijelu A i B obrasca) te (ii) informacije iz dijela C obrasca, koje obuhvaćaju i temeljni uzrok ako je već poznat i sažetak mjera koje su usvojene ili se planiraju usvojiti radi uklanjanja problema i sprečavanja njegove ponovne pojave u budućnosti.

2.21. Pružatelji platnih usluga osim toga trebaju poslati konačno izvješće *kao rezultat kontinuirane procjene incidenta*, kada 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 i u svakom slučaju do procijenjenog datuma 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 opravda klasifikacija u nižu kategoriju incidenta.

Smjernica 3.: delegirano i konsolidirano izvješćivanje

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

a. Službenim ugovorom ili, ako je primjenjivo, postojećim unutarnjim 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. 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. 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 (EMD) ili

    ii. Smjernicama Odbora europskih nadzornih tijela za bankarstvo (CEBS) o eksternalizaciji u kreditnim institucijama.

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

d. Pravilno je osigurana 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 zahvaćenim istim značajnim operativnim ili sigurnosnim incident) trebaju o tome obavijestiti nadležno tijelo u matičnoj državi članici, navesti podatke za kontakt, navedene 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. Treba osigurati da treća strana procijeni značajnost 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 tako dugo dok ne postoje dokazi da ne treba biti obuhvaćen*

e. Treba zajamčiti da, u slučaju polja obrasca u kojima nije moguće dati zajednički odgovor (npr. dio B 2, B 4 ili C 3), 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 raspone, u poljima u kojima je to moguće, kako bi naznačila najnižu i najvišu vrijednost koje su zabilježene ili procijenjene za različite pružatelje platnih usluga.

f. Pružatelji platnih usluga trebaju osigurati da ih treća strana u svakom trenutku obavješćuje o svim relevantnim informacijama o incidentu te svim interakcijama s nadležnim tijelom i sadržaju tih interakcija, no 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 postupcima koje je uspostavilo to tijelo. Pružatelji platnih usluga osim toga 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. PSD2 i ovim Smjernicama. Nadalje, pružatelji platnih usluga trebaju osigurati da se incident ne prijavi dva puta, tj. da ga jednom prijavi pružatelj platnih usluga i još jednom treća strana.

Smjernica 4.: operativna i sigurnosna politika

4.1. Pružatelji platnih usluga trebaju osigurati da se njihovom općom operativnom i sigurnosnom politikom jasno određuju sve odgovornosti za izvješćivanje o incidentima u skladu s 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 će se 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 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 će se podijeliti

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

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

- 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 planiraju poduzeti za oporavak od incidenta
- opis načina na koji bi incident mogao utjecati na druge PPU-ove i/ili infrastrukture
- opis medijske pokrivenosti (ako postoji)
- uzrok incidenta.

6.3. Nadležna tijela trebaju provesti ispravnu anonimizaciju po potrebi i izostaviti sve informacije koje bi mogle biti podložne ograničenjima u pogledu povjerljivosti ili intelektualnog vlasništva prije nego što podijele bilo koje informacije povezane s incidentom s drugim relevantnim domaćim tijelima. Unatoč tome, nadležna tijela trebaju dostaviti drugim relevantnim domaćim tijelima naziv i adresu izvještajnog pružatelja platnih usluga kada predmetna 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 su pohranjene i razmijenjene s drugim relevantnim domaćim tijelima te ispravno sebe 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 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 će se podijeliti s EBA-om i ESB-om te o formatu i postupcima za obavješćivanje o njima

Smjernica 7.: informacije koje će se podijeliti

7.1. Nadležna tijela trebaju uvijek dostaviti EBA-i i ESB-u sva izvješća primljena od (ili u ime) pružatelja platnih usluga koje je pogodio značajni operativni ili sigurnosni incident (tj. početno, prijelazno i konačno izvješće).

Smjernica 8.: komunikacija

8.1. Nadležna tijela trebaju u svakom trenutku čuvati povjerljivost i cjelovitost informacija koje su pohranjene i razmijenjene s EBA-om i ESB-om te ispravno sebe 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 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 pomoglo u smanjenju rizika od prekida poslovanja, nadležna tijela trebaju podržavati odgovarajuće načine komunikacije.

Prilog 1. – Obrasci za izvješćivanje za pružatelje platnih usluga

CLASSIFICATION: RESTRICTED

Major Incident Report

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

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

A - Initial report

A 1 - GENERAL DETAILS

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

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

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

B - Intermediate report

B 1 - GENERAL DETAILS

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

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

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

B 3 - INCIDENT DESCRIPTION

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

B 4 - INCIDENT IMPACT

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

B 5 - INCIDENT MITIGATION

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

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

Notes:

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

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

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

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

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

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

UPUTE ZA POPUNJAVANJE OBRAZACA

Pružatelji platnih usluga trebaju ispuniti odgovarajući dio obrasca ovisno o fazi izvješćivanja u kojoj se nalaze: dio A služi za početno izvješće, dio B za prijelazno izvješće, a dio C za konačno izvješće. Sva su polja obvezna osim ako je drugačije navedeno.

Zaglavlje

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

Prijelazno izvješće: ovo je ažuriranje prethodnog (početnog ili prijelaznog) izvješća o istom incidentu.

Posljednje prijelazno izvješće: ovime se nadležno tijelo u matičnoj državi članici obavješćuje da je redovno poslovanje ponovno uspostavljeno, pa se neće podnositi daljnja prijelazna izvješća.

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

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 njegova rješenja. PPU-ovi bi trebali objasniti razloge za tu klasifikaciju u nižu kategoriju.

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

Identifikacijski broj incidenta ako je primjenjivo (za prijelazno i konačno izvješće): referentni broj koji izdaje nadležno tijelo pri zaprimanju početnog izvješća radi jedinstvene identifikacije incidenta ako je primjenjivo (tj. ako nadležno tijelo dodjeljuje takav referentni broj).

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 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 naziv pojavljuje u odgovarajućem službenom nacionalnom registru PPU-ova.

Jedinstveni identifikacijski broj PPU-a ako je relevantan: relevantan jedinstveni identifikacijski broj koji se koristi u državama članicama za identifikaciju PPU-a, a koji PPU mora unijeti ako ne popuni polje „Autorizacijski broj PPU-a".

Autorizacijski broj PPU-a: autorizacijski broj matične države članice.

Vodeći subjekt grupe: u slučaju grupe subjekata kako je definirana u članku 4. stavku 40. 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 navedite naziv vodećeg subjekta.

Matična država: država članica u kojoj se nalazi registrirano sjedište PPU-a ili, ako PPU nema registrirano sjedište u skladu s nacionalnim pravom, država članica u kojoj se nalazi njegovo mjesto uprave.

Država/države zahvaćene incidentom: država ili države u kojima se utjecaj incidenta materijalizirao (npr. zahvaćeno je nekoliko podružnica PPU-a koje se nalaze u različitim 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 izvješćuje u ime zahvaćenog PPU-a, ime i prezime osobe na čelu odjela za upravljanje incidentima/rizicima ili sličnog odjela u zahvaćenom PPU-u.

Elektronička pošta: adresa e-pošte na koju se mogu po potrebi slati zahtjevi za dodatna objašnjenja. To može biti adresa privatne ili poslovne e-pošte.

Telefon: telefonski broj na koji se po potrebi mogu podnijeti zahtjevi za dodatna objašnjenja. To može biti broj privatnog ili poslovnog 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 treća strana izvješćuje u ime zahvaćenog PPU-a, ime i prezime alternativne osobe u odjelu za upravljanje incidentima/rizicima ili sličnom odjelu u zahvaćenom PPU-u.

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

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

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

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

Jedinstveni identifikacijski broj ako je relevantan: relevantan jedinstveni identifikacijski broj koji se u državi u kojoj se nalazi treća strana koristi za identifikaciju subjekta koji izvješćuje o incidentu, a koji izvještajni subjekt treba navesti ako ne popuni polje „Autorizacijski broj".

Autorizacijski broj ako je primjenjiv: autorizacijski broj treće strane u državi u kojoj se nalazi, kada je primjenjivo.

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

Elektronička pošta: adresa e-pošte na koju se mogu po potrebi slati zahtjevi za dodatna objašnjenja. To može biti adresa privatne ili poslovne e-pošte.

Telefon: telefonski broj na koji se po potrebi mogu podnijeti zahtjevi za dodatna objašnjenja. To može biti broj privatnog ili poslovnog 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.

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

Telefon: može se navesti telefonski broj alternativne kontakt osobe na koji se po potrebi mogu podnijeti zahtjevi za dodatna objašnjenja. To može biti broj privatnog ili poslovnog telefona.

A 2 – Otkrivanje incidenta i početna klasifikacija

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

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

Kratak i opći opis incidenta: ukratko navedite najvažnije pojedinosti o incidentu, uključujući moguće uzroke, trenutačne učinke itd.
Kada se procjenjuje da će biti sljedeće ažuriranje izvješća?: navedite procijenjeni datum i vrijeme podnošenja sljedećeg ažuriranja (prijelazno ili konačno izvješće).

B – Prijelazno izvješće

B 1 – Opće informacije

Detaljniji opis incidenta: opišite glavne značajke incidenta i obuhvatite barem točke navedene u upitniku (s kojim se točno problemom PPU suočava, kako je nastao i razvio se, moguće veze s prethodnim incidentima, posljedice, osobito za korisnike platnih usluga itd.).

Datum i vrijeme početka incidenta: datum i vrijeme kada je incident počeo ako su poznati.

Status incidenta:

Dijagnostika: utvrđene su značajke incidenta.
Popravak: ponovno se konfiguriraju napadnuti dijelovi.
Oporavak: neispravne stavke vraćaju se u posljednje stanje koje se može oporaviti.
Ponovna uspostava: ponovno se pruža usluga povezana s plaćanjem.

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.

B 2 – Klasifikacija incidenta / informacije o incidentu

Opći učinak: navedite koje je značajke sustava incident pogodio. Može se označiti više stavki.

Cjelovitost: čuvanje točnosti i cjelovitosti imovine (uključujući podataka).
Dostupnost: jamčenje dostupnosti i mogućnosti korištenja uslugama povezanim s plaćanjem korisnicima platnih usluga.
Povjerljivost: uskraćivanje dostupnosti ili otkrivanja informacija neovlaštenim fizičkim osobama, subjektima ili procesima.
Autentičnost: izvor je upravo ono što tvrdi da jest.
Kontinuitet: potpuna dostupnost procesa, zadataka i imovine organizacije potrebnih za pružanje usluga povezanih s plaćanjem i njihovo funkcioniranje na prihvatljivim unaprijed određenim razinama.

Zahvaćene transakcije: PPU-ovi trebaju navesti pragove koji su dosegnuti ili je vjerojatno da će biti dosegnuti zbog incidenta, ako oni postoje, i povezanu statistiku: 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. Subjekti koji izvješćuju u ime nekoliko PPU-ova (tj. konsolidirano izvješćivanje) mogu umjesto toga navesti raspone vrijednosti, pri čemu se crticom odvaja najniža od najviše vrijednosti zabilježene ili procijenjene za grupu PPU-ova uključenih u izvješće. 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, one transakcije koje se neće moći 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). 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. radi sezonskoj utjecaja), umjesto tog izračuna

trebaju upotrijebiti drugi, reprezentativniji izračun i obavijestiti nadležno tijelo o osnovnim razlozima za taj pristup u polju „Napomene”.

Zahvaćeni korisnici platnih usluga: PPU-ovi trebaju navesti pragove koji su 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. Subjekti koji izvješćuju u ime nekoliko PPU-ova (tj. konsolidirano izvješćivanje) mogu umjesto toga navesti raspone vrijednosti, pri čemu se crticom odvaja najniža od najviše vrijednosti zabilježene ili procijenjene za grupu PPU-ova uključenih u izvješće. 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 na temelju prošle aktivnosti procijeniti broj korisnika platnih usluga koji su se možda koristili platnom uslugom tijekom trajanja incidenta. 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 postoje), a PPU-ovi koji primaju te operativne usluge osim toga 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.

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. Subjekti koji izvješćuju u ime nekoliko PPU-ova (tj. konsolidirano izvješćivanje) mogu umjesto toga navesti raspon vrijednosti, pri čemu se crticom odvaja najniža od najviše vrijednosti zabilježene ili procijenjene za grupu PPU-ova uključenih u izvješće. PPU-ovi trebaju razmotriti koliko će trajati prekid ili vjerojatni prekid bilo kojeg zadatka, procesa ili kanala povezanog s pružanjem platnih usluga i, stoga, spriječiti (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. Subjekti koji izvješćuju u ime nekoliko PPU-ova (tj. konsolidirano izvješćivanje) mogu umjesto toga navesti raspon vrijednosti, pri čemu se crticom odvaja najniža od najviše vrijednosti zabilježene ili procijenjene za grupu PPU-ova uključenih u izvješće. 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.

Izravni troškovi: novčani iznos (u eurima) izravno utrošen na incident, uključujući novčana sredstva potrebna za njegovo ispravljanje (npr. oduzeta sredstva ili imovina, troškovi zamjene hardvera i softvera, naknade zbog neispunjenja ugovornih obveza).
Neizravni troškovi: novčani iznos (u eurima) neizravno utrošen na incident (npr. troškovi odštete/naknade klijentima, prihodi izgubljeni zbog propuštenih poslovnih prilika, mogući pravni troškovi).

Visoka razina unutarnje eskalacije: PPU-ovi trebaju razmotriti je li, zbog utjecaja incidenta na usluge povezane s plaćanjem, član uprave odgovoran za informacijski sustav (ili osoba na sličnom položaju) obaviješten o incidentu, odnosno hoće li ga se vjerojatno obavijestiti o njemu izvan bilo kojeg postupka periodičnog izvješćivanja i redovito tijekom trajanja incidenta. U slučaju delegiranog izvješćivanja do eskalacije bi došlo kod treće strane. Nadalje, PPU-ovi 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 programe kartičnog plaćanja kojima mu se pruža potpora te druge pružatelje platnih usluga. 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 pouzdanost 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 te 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 smatrati vjerojatnost da će incident prouzročiti štetu društvu dobrim pokazateljem njegova potencijala da utječe na njihovu reputaciju. PPU-ovi trebaju razmotriti (i) je li incident utjecao na vidljivi proces i je li stoga vjerojatno da će biti medijski pokriven odnosno je li on već medijski pokriven (uzimajući u obzir ne samo tradicionalne medije kao što su novine, nego i blogove, društvene mreže itd.), (ii) je li došlo do propusta u ispunjavanju regulatornih obveza ili je vjerojatno da će do njega doći, (iii) jesu li prekršene ili je vjerojatno da će se prekršiti sankcije te (iv) je li se i prije dogodila ista vrsta incidenta.

B 3 – Opis incidenta

Vrsta incidenta: navedite je li, prema vašem saznanju, riječ o operativnom ili sigurnosnom incidentu.

Operativni: incident koji je nastao zbog neprikladnih ili neuspjelih procesa, osoba i sustava ili događaja više sile koji utječu na cjelovitost, dostupnost, povjerljivost, autentičnost i/ili kontinuitet 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, autentičnost i/ili kontinuitet usluga povezanih s plaćanjem. Do toga može doći kada je, među ostalim, PPU zahvaćen kibernetičkim napadom, kada su sigurnosne politike neprikladno isplanirane ili provedene ili kada ne postoji prikladna fizička zaštita.

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

Pod istragom: uzrok još nije utvrđen.

Vanjski napad: izvor uzroka potječe izvana i ciljano je usmjeren na PPU (npr. napadi zlonamjernog softvera).

Unutarnji napad: izvor uzroka potječe iznutra i ciljano je usmjeren na PPU (npr. unutarnja prijevara).

Vrsta napada:

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

Zaraženi unutarnji sustavi: štetna aktivnost kojom se napadaju računalni sustavi u pokušaju krađe prostora na tvrdom disku ili procesorskog vremena, pristupanja osobnim podacima, oštećenja podataka, slanja neželjene pošte kontaktima itd.

Ciljani upad: neovlašteni pokušaj špijuniranja, uhođenja i krađe informacija u kibernetičkom prostoru.

Drugo: sve druge vrste napada koje je PPU pretrpio bilo izravno ili putem pružatelja usluge. Točnije, ako je došlo do napada usmjerenog na procese autorizacije i autentifikacije, treba označiti ovaj okvir. Pojedinosti treba unijeti u polje za slobodan unos teksta.

Vanjski događaji: uzrok je povezan s događajima na koje organizacija općenito nema utjecaj (npr. prirodne katastrofe, pravni problemi, poslovni problemi i ovisnost o uslugama).

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).

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 složenosti sustava koji podupiru aktivnosti plaćanja.

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?: incident može biti usmjeren izravno na PPU ili može neizravno utjecati na njega putem treće strane. U slučaju neizravnog utjecaja navedite naziv jednog ili više pružatelja usluga.

B 4 – Učinak incidenta

Zahvaćena zgrada (ili više njih) (adresa) ako je primjenjivo: ako je zahvaćena određena zgrada, navedite njezinu adresu.

Zahvaćeni komercijalni kanali: navedite kanal ili kanale za interakciju s korisnicima platnih usluga koji su zahvaćeni incidentom. 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.
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 on 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, pružatelju platnih usluga primatelja plaćanja ili platiteljevu vlastitom pružatelju platnih usluga.
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 platitelja.
Novčana pošiljka: platna usluga u okviru koje se novčana sredstva primaju od platitelja 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: usluge iniciranja naloga za plaćanje na zahtjev korisnika platnih usluga u odnosu na račun za plaćanje koji vodi drugi PPU.
Usluge informiranja o računu: internetske 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-a.
Drugo: zahvaćena platna usluga nije nijedna od prethodno navedenih. Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Zahvaćena funkcionalna područja: navedite korak ili korake procesa plaćanja koje je pogodio incident. Može se označiti više stavki.

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 ili vrijednosnih papira.

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.

Zahvaćeni sustavi i komponente: navedite dio ili dijelove tehnološke infrastrukture PPU-a koje je pogodio incident. Može se označiti više stavki.

Aplikacija/softver: programi, operativni sustavi itd. koji podupiru pružanje platnih usluga PPU-a.

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

Hardver: fizička tehnološka oprema na kojoj se odvijaju procesi i/ili na koju se pohranjuju podaci potrebni PPU-u za izvršenje aktivnosti povezanih s plaćanjem.

Mreža/infrastruktura: javne ili privatne telekomunikacijske mreže na kojima je omogućena razmjena podataka i informacija tijekom procesa plaćanja (npr. internet).

Drugo: zahvaćeni sustav i komponenta nisu nijedno od prethodno navedenog.
Dodatne pojedinosti treba unijeti u polje za slobodan unos teksta.

Zahvaćeno osoblje: navedite je li incident imao utjecaja na osoblje PPU-a i, ako jest, navedite pojedinosti u polju za slobodan unos teksta.

B 5 – Ublažavanje incidenta

Koje su radnje/mjere do sada poduzete ili planirane za oporavak od incidenta?: navedite pojedinosti o radnjama koje su poduzete ili se planiraju poduzeti za privremeno rješavanje incidenta.

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

Je li PPU ukinuo ili oslabio određene kontrole zbog incidenta?: navedite je li PPU morao ručno ukinuti određene kontrole (npr. prestati s primjenom načela četiri oka) kako bi riješio incident, a ako jest, navedite pojedinosti o osnovnim razlozima kojima se opravdava slabljenje ili ukidanje kontrola.

C – Konačno izvješće

C 1 – Opće informacije

Ažuriranje informacija iz prijelaznog izvješća (sažetak): navedite nove informacije o radnjama poduzetima za oporavak od incidenta i sprečavanje njegova ponavljanja, analizi temeljnog uzroka, stečenim spoznajama itd.

Datum i vrijeme zatvaranja incidenta: navedite datum i vrijeme kada se smatra da je incident zatvoren.

Jesu li ponovno uspostavljene izvorne kontrole?: ako je PPU morao ukinuti ili oslabiti određene kontrole zbog incidenta, navedite jesu li te kontrole ponovno uspostavljene i unesite dodatne informacije u polje za slobodan unos teksta.

C 2 – Analiza temeljnog uzorka i daljnje mjere

Što je temeljni uzrok ako je već poznat?: objasnite što je temeljni uzrok incidenta ili, ako on još nije poznat, privremene zaključke donesene na osnovi analize temeljnog uzroka. PPU-ovi mogu priložiti datoteku s detaljnim informacijama ako to smatraju potrebnim.

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