EBA/GL/2017/10

19/12/2017

Smernice

o poročanju o večjih incidentih v skladu z Direktivo (EU) 2015/2366 (PSD2)

1. Obveznosti glede skladnosti in poročanja

Vloga teh smernic

1. Dokument vsebuje smernice, izdane v skladu s členom 16 Uredbe (EU) št. 1093/2010[1]. V skladu s členom 16(3) Uredbe (EU) št. 1093/2010 si morajo pristojni organi in finančne institucije na vsak način prizadevati za upoštevanje smernic.

2. V smernicah je predstavljeno stališče organa EBA o ustreznih nadzorniških praksah v Evropskem sistemu finančnega nadzora in o tem, kako bi bilo treba zakonodajo Unije uporabljati na določenem področju. Pristojni organi iz člena 4(2) Uredbe (EU) št. 1093/2010, za katere smernice veljajo, bi jih morali upoštevali tako, da jih ustrezno vključijo v svoje prakse (npr. s spremembo svojega pravnega okvira ali nadzorniških postopkov), tudi če so smernice namenjene predvsem institucijam.

Dolžnost poročanja

3. Pristojni organi morajo v skladu s členom 16(3) Uredbe (EU) št. 1093/2010 do 19/02/2018 organ EBA uradno obvestiti, ali ravnajo oziroma ali nameravajo ravnati v skladu s temi smernicami, ali pa mu sporočiti razloge za njihovo neupoštevanje. Če pristojni organi do tega roka ne bodo poslali uradnega obvestila, bo organ EBA štel, da jih ne upoštevajo. Uradna obvestila je treba poslati na obrazcu, ki je na voljo na spletni strani organa EBA, na elektronski naslov compliance@eba.europa.eu z navedbo sklica „EBA/GL/2017/10“. Predložiti jih morajo osebe, ki so pooblaščene za poročanje o skladnosti v imenu svojih pristojnih organov. Organu EBA je treba sporočiti tudi vsako spremembo stanja glede upoštevanja smernic.

4. Uradna obvestila bodo v skladu s členom 16(3) objavljena na spletni strani organa EBA.

[1] Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12).

2. Predmet urejanja, področje uporabe in opredelitve pojmov

Predmet urejanja

5. Evropski bančni organ je te smernice pripravil na podlagi pooblastil iz člena 96(3) Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES (PSD2).

6. Te smernice določajo zlasti merila, ki jih ponudniki plačilnih storitev uporabljajo za razvrstitev večjih operativnih ali varnostnih incidentov, ter obliko in postopke, ki jih morajo upoštevati, da bi v skladu s členom 96(1) navedene direktive o takih incidentih obvestili pristojni organ v matični državi članici.

7. Poleg tega opredeljujejo tudi načine ocenjevanja pomembnosti incidentov s strani pristojnih organov in podrobnosti v poročilih o incidentih, ki jih pristojni organi v skladu s členom 96(2) posredujejo drugim domačim organom.

8. Obravnavajo tudi posredovanje ustreznih podatkov o incidentih Evropskemu bančnemu organu in Evropski centralni banki, da bi se zagotovil enoten in dosleden pristop.

Področje uporabe

9. Te smernice se uporabljajo v zvezi z razvrstitvijo večjih operativnih ali varnostnih incidentov in poročanjem o njih v skladu s členom 96 Direktive (EU) 2015/2366.

10. Uporabljajo se za vse incidente, ki spadajo v opredelitev pojma „večji operativni ali varnostni incident“, ki zajema zunanje in notranje dogodke, ki bi lahko bili zlonamerni ali slučajni.

11. Smernice se uporabljajo tudi takrat, kadar večji operativni ali varnostni incident izvira iz območij zunaj Unije (npr. kadar izvira iz nadrejene družbe ali podrejene družbe s sedežem zunaj Unije) in kadar na plačilne storitve, ki jih zagotavlja ponudnik plačilnih storitev iz Unije, vpliva bodisi neposredno (s plačilom povezano storitev izvaja družba zunaj Unije, na katero je vplival incident) ali posredno (zmogljivost ponudnika plačilnih storitev, da še naprej izvaja svoje plačilne dejavnosti, je zaradi incidenta ogrožena kako drugače).

Naslovniki

12. Prvi sklop smernic (razdelek 4) je naslovljen na ponudnike plačilnih storitev, kot so opredeljeni v členu 4(11) Direktive (EU) 2015/2366 in navedeni v členu 4(1) Uredbe (EU) št. 1093/2010.

13. Drugi in tretji sklop smernic (razdelka 5 in 6) sta naslovljena na pristojne organe, kot so opredeljeni v členu 4(2)(i) Uredbe (EU) št. 1093/2010.

Opredelitev pojmov

14. Če ni določeno drugače, imajo izrazi v teh smernicah enak pomen kot izrazi, ki se uporabljajo in so opredeljeni v Direktivi (EU) 2015/2366. Poleg tega se v teh smernicah uporabljajo naslednje opredelitve pojmov:

Operativni ali varnostni incident	Enkratni dogodek ali niz povezanih dogodkov, ki jih ponudnik plačilnih storitev ne načrtuje in ki ima ali bo verjetno imel negativen učinek na celovitost, razpoložljivost, zaupnost, avtentičnost in/ali neprekinjenost s plačilom povezanih storitev.
Celovitost	Lastnost, ki vključuje ohranjanje točnosti in popolnosti sredstev (vključno s podatki).
Razpoložljivost	Lastnost s plačilom povezanih storitev, ki vključuje dostopnost in možnost uporabe plačilnih storitev s strani uporabnikov.
Zaupnost	Lastnost, ki pomeni, da se informacije ne dajo na voljo ali ne razkrivajo nepooblaščenim posameznikom, subjektom ali postopkom.
Avtentičnost	Lastnost, ki pomeni, da je vir točno ta, za katerega se predstavlja.
Neprekinjenost	Lastnost postopkov, nalog in sredstev organizacije, ki je potrebna za izvajanje s plačilom povezanih storitev in ki zagotavlja da so te v celoti dostopne in se izvajajo na sprejemljivih, vnaprej opredeljenih ravneh.
S plačilom povezane storitve	Vsaka poslovna dejavnost v smislu člena 4(3) PSD2 in vse naloge tehnične podpore, potrebne za pravilno izvajanje plačilnih storitev.

3. Izvajanje

Datum začetka uporabe

15. Te smernice se začnejo uporabljati 13. januarja 2018.

4. Smernice za ponudnike plačilnih storitev o obveščanju pristojnih organov v matični državi članici o večjih operativnih in varnostnih incidentih

Smernica 1: razvrstitev incidenta v kategorijo večjih incidentov

1.1. Ponudniki plačilnih storitev bi morali v kategorijo večjih incidentov razvrstiti tiste operativne ali varnostne incidente, ki izpolnjujejo

a. enega ali več meril na „višji stopnji učinka“ ali

b. tri ali več meril na „nižji stopnji učinka“,

kot je določeno v odstavku 1.4 in na podlagi ocene, določene v teh smernicah.

1.2. Ponudniki plačilnih storitev bi morali oceniti operativni ali varnostni incident na podlagi naslednjih meril in njihovih osnovnih kazalnikov:

i. Transakcije, na katere je incident vplival

Ponudniki plačilnih storitev bi morali opredeliti skupno vrednost transakcij, na katere je incident vplival, ter število ogroženih plačil v obliki odstotka rednih plačilnih transakcij, opravljenih s plačilnimi storitvami, na katere je vplival incident.

ii. Uporabniki plačilnih storitev, na katere je incident vplival

Ponudniki plačilnih storitev bi morali opredeliti število uporabnikov plačilnih storitev, na katere je incident vplival, tako v absolutnem smislu kot v obliki odstotka skupnega števila uporabnikov plačilnih storitev.

iii. Čas nedelovanja storitve

Ponudniki plačilnih storitev bi morali opredeliti obdobje, v katerem storitev verjetno ne bo na voljo za uporabnike plačilnih storitev ali v katerem ponudnik plačilnih storitev ne bo mogel izpolniti plačilnega naloga, opredeljenega v členu 4(13) PSD2.

iv. Gospodarski učinek

Ponudniki plačilnih storitev bi morali celostno opredeliti denarne stroške, povezane z incidentom, in pri tem upoštevati absolutno vrednost ter, kadar je ustrezno, relativno pomembnost teh stroškov glede na velikost ponudnika plačilnih storitev (tj. glede na njegov temeljni kapital).

v. Visoka raven notranjega stopnjevanja

Ponudniki plačilnih storitev bi morali opredeliti, ali je njihovo vodstvo bilo o tem incidentu obveščeno oziroma ali bo o njem verjetno obveščeno.

vi. Drugi ponudniki plačilnih storitev ali ustrezne infrastrukture, na katere bi incident lahko vplival

Ponudniki plačilnih storitev bi morali opredeliti sistemske posledice, ki jih bo incident verjetno imel, tj. njegov verjetni učinek širjenja, ki poleg prvega ponudnika plačilnih storitev, na katerega je incident vplival, zajame tudi druge ponudnike plačilnih storitev, infrastrukture finančnega trga in/ali kartične sheme.

vii. Učinek na ugled

Ponudniki plačilnih storitev bi morali opredeliti, kako lahko incident oslabi zaupanje uporabnikov v samega ponudnika plačilnih storitev in, splošneje, v storitev kot tako ali celoten trg.

1.3. Ponudniki plačilnih storitev bi morali izračunati vrednost kazalnikov v skladu z naslednjo metodologijo:

i. Transakcije, na katere je incident vplival

Ponudniki plačilnih transakcij bi praviloma morali „transakcije, na katere je incident vplival“, razumeti kot vse domače in čezmejne transakcije, na katere je ali verjetno bo neposredno ali posredno vplival incident, ter zlasti kot tiste transakcije, ki jih ni bilo mogoče odrediti ali obdelati, tiste, pri katerih se je spremenila vsebina plačilnega sporočila, in tiste, ki so bile odrejene na goljufiv način (ne glede na to, ali so bila sredstva povrnjena ali ne).

Poleg tega bi morali redne plačilne transakcije razumeti kot letno povprečje dnevnih domačih in čezmejnih plačilnih transakcij, ki se izvajajo z istimi plačilnimi storitvami, na katere je vplival incident, pri čemer predhodno leto velja za referenčno obdobje za izračun. Če ponudniki plačilnih storitev menijo, da ta podatek ni reprezentativen (npr. zaradi sezonske narave), bi morali uporabiti drugo, bolj reprezentativno metriko in utemeljiti ta pristop pristojnemu organu v ustreznem polju v predlogi (glejte Prilogo 1).

ii. Uporabniki plačilnih storitev, na katere je incident vplival

Ponudniki plačilnih storitev bi morali „uporabnike plačilnih storitev, na katere je incident vplival“, razumeti kot vse stranke (domače ali tuje, potrošnike ali podjetja), ki imajo s ponudnikom plačilnih storitev, na katere je incident vplival, sklenjeno pogodbeno razmerje, na podlagi katerega imajo dostop do plačilne storitve, na katero je vplival incident, in ki so ali verjetno bodo utrpeli posledice tega incidenta. Da bi opredelili število uporabnikov plačilnih storitev, ki so morda uporabljali plačilno storitev v času trajanja incidenta, bi morali uporabiti ocene, ki temeljijo na preteklih dejavnostih.

Če gre za skupine ponudnikov plačilnih storitev, bi moral vsak ponudnik plačilnih storitev upoštevati samo svoje uporabnike plačilnih storitev. Kadar ponudnik plačilnih storitev nudi operativne storitve drugim, bi moral upoštevati samo svoje uporabnike plačilnih storitev (če

obstajajo), ponudniki plačilnih storitev, ki koristijo te operativne storitve, pa bi morali oceniti incident v povezavi s svojimi uporabniki plačilnih storitev.

Poleg tega bi ponudniki plačilnih storitev morali kot skupno število uporabnikov plačilnih storitev upoštevati seštevek domačih in čezmejnih uporabnikov plačilnih storitev, s katerimi so v času incidenta v pogodbenem razmerju (ali najnovejši razpoložljivi podatek) in ki imajo dostop do plačilne storitve, na katero je incident vplival, ne glede na njihovo velikost oziroma ne glede na to, ali veljajo za aktivne ali pasivne uporabnike plačilnih storitev.

iii. Čas nedelovanja storitve

Ponudniki plačilnih storitev bi morali upoštevati obdobje, v katerem katera koli naloga, postopek ali kanal, povezan z izvajanjem plačilnih storitev, ne deluje oziroma verjetno ne bo deloval in tako onemogoča (i) odreditev in/ali izvršitev plačilne storitve in/ali (ii) dostop do plačilnega računa. Ponudniki plačilnih storitev bi morali čas nedelovanja storitve računati od trenutka, ko nastopi nedelovanje, pri tem pa upoštevati tako časovne intervale, ki zajemajo poslovni čas, v katerem običajno poteka izvrševanje plačilnih storitev, kot tudi ure, v katerih se ne posluje, in obdobja izvajanja vzdrževalnih del, kadar je to ustrezno in primerno. Če ponudniki plačilnih storitev ne morejo opredeliti, kdaj je nastopilo nedelovanje, bi morali čas nedelovanja storitve izjemoma računati od trenutka, ko je bilo nedelovanje zaznano.

iv. Gospodarski učinek

Ponudniki plačilnih storitev bi morali upoštevati stroške, ki se lahko neposredno povežejo z incidentom, ter stroške, ki so z incidentom posredno povezani. Med drugim bi morali upoštevati razlaščena sredstva, stroške nadomestitve strojne ali programske opreme, druge forenzične ali sanacijske stroške, pristojbine zaradi neupoštevanja pogodbenih obveznosti, sankcije, zunanje obveznosti in izgubljene prihodke. V zvezi s posrednimi stroški bi morali upoštevati samo tiste, ki so že znani ali se bodo zelo verjetno materializirali.

v. *Visoka raven notranjega stopnjevanja*

Ponudniki plačilnih storitev bi morali upoštevati, ali je zaradi učinka na s plačilom povezane storitve glavni uradnik za informiranje (ali oseba na podobnem položaju) bil oziroma verjetno bo obveščen o incidentu brez uporabe kakršnega koli rednega postopka obveščanja in ali je bil oziroma verjetno bo obveščen ves čas trajanja incidenta. Upoštevati bi morali tudi, ali je zaradi učinka incidenta na s plačilom povezane storitve bil sprožen oziroma ali se bo verjetno sprožil krizni način delovanja.

vi. *Drugi ponudniki plačilnih storitev ali ustrezne infrastrukture, na katere bi lahko incident vplival*

Ponudniki plačilnih storitev bi morali oceniti učinek incidenta na finančni trg, ki zajema infrastrukture finančnega trga in/ali kartične sheme, ki nudijo podporo njim samim kakor tudi drugim ponudnikom plačilnih storitev. Zlasti bi morali oceniti, ali se je incident ponovil pri drugih ponudnikih plačilnih storitev oziroma ali se bo verjetno ponovil, ali je vplival oziroma ali bo verjetno vplival na nemoteno delovanje infrastruktur finančnega trga in ali je ogrozil oziroma ali bo verjetno ogrozil dobro delovanje celotnega finančnega sistema. Upoštevati bi morali različne razsežnosti, na primer ali je komponenta/programska oprema, na katero je

incident vplival, lastniška ali na splošno dostopna, ali je ogrožena mreža notranja ali zunanja in ali je ponudnik plačilnih storitev prenehal oziroma ali bo verjetno prenehal izpolnjevati svoje obveznosti znotraj infrastruktur finančnega trga, katerih član je.

vii. *Učinek na ugled*

Ponudniki plačilnih storitev bi morali upoštevati stopnjo prepoznavnosti, za katero lahko z največjo možno gotovostjo potrdijo, da jo je incident dosegel ali jo bo verjetno dosegel na trgu. Kot dober kazalnik možnosti vpliva incidenta na njihov ugled bi zlasti morali upoštevati verjetnost, da bo incident povzročil družbeno škodo. Upoštevati bi morali, (i) ali je incident vplival na prepoznavni postopek, zaradi česar bodo o njem verjetno poročali oziroma so že poročali mediji (ne samo tradicionalni mediji, kot so časopisi, temveč tudi spletni dnevniki, družabna omrežja itd.), (ii) ali regulativne obveznosti niso bile oziroma ali verjetno ne bodo izpolnjene, (iii) ali je prišlo oziroma ali bo verjetno prišlo do kršenja sankcij in (iv) ali se je ista vrsta incidenta zgodila že v preteklosti.

1.4. Ponudniki plačilnih storitev bi morali oceniti incident tako, da za vsako posamezno merilo določijo, ali so ustrezne mejne vrednosti iz preglednice 1 dosežene oziroma ali bodo verjetno dosežene, še preden se incident razreši.

Preglednica 1 Mejne vrednosti

Merila	Nižja stopnja učinka	Višja stopnja učinka
Transakcije, na katere je incident vplival	> 10 % rednih transakcij ponudnika plačilnih storitev (v smislu števila transakcij) **in** > 100 000 EUR	> 25 % rednih transakcij ponudnika plačilnih storitev (v smislu števila transakcij) **ali** > 5 milijonov EUR
Uporabniki plačilnih storitev, na katere je incident vplival	> 5 000 **in** > 10 % uporabnikov plačilnih storitev ponudnika plačilnih storitev	> 50 000 **ali** > 25 % uporabnikov plačilnih storitev ponudnika plačilnih storitev
Čas nedelovanja storitve	> 2 uri	Se ne uporablja
Gospodarski učinek	Se ne uporablja	> Maks. (0,1 % temeljnega kapitala,* 200 000 EUR) **ali** > 5 milijonov EUR
Visoka raven notranjega stopnjevanja	Da	Da in verjetno bo sprožen krizni način delovanja (ali enakovreden način)
Drugi ponudniki plačilnih storitev ali ustrezne infrastrukture, na katere bi lahko incident vplival	Da	Se ne uporablja
Učinek na ugled	Da	Se ne uporablja

*Temeljni kapital, kot je opredeljen v členu 25 Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe (EU) št. 648/2012.

1.5. Ponudniki plačilnih storitev bi se morali zateči k uporabi ocenjenih vrednosti, če svojih presoj o tem, ali je določena mejna vrednost dosežena oziroma ali bo verjetno dosežena, še preden se incident razreši, ne morejo podpreti z dejanskimi podatki (npr. to bi se lahko zgodilo v začetni fazi preiskave).

1.6. Ponudniki plačilnih storitev bi morali to ocenjevanje izvajati neprekinjeno ves čas trajanja incidenta, da bi ugotovili možno spremembo statusa incidenta bodisi navzgor (prerazvrstitev incidenta, ki ne velja za večjega, v kategorijo večjih incidentov) ali navzdol (prerazvrstitev večjega incidenta v kategorijo incidentov, ki ne veljajo za večje).

Smernica 2: postopek obveščanja

2.1. Ponudniki plačilnih storitev bi morali zbrati vse ustrezne informacije, pripraviti poročilo o incidentu s pomočjo predloge iz Priloge 1 in poročilo predložiti pristojnemu organu v matični državi članici. Predlogo bi morali izpolniti v skladu z navodili iz Priloge 1.

2.2. S pomočjo iste predloge bi morali pristojni organ obveščati ves čas trajanja incidenta (tj. predloga se uporabi za prvo, vmesno in končno poročilo, kot je opisano v odstavkih 2.7 do 2.21). Predlogo bi morali v času trajanja notranjih preiskav po najboljših prizadevanjih dopolnjevati vsakič, ko je na voljo več informacij.

2.3. Če je ustrezno, bi morali pristojnemu organu v svoji matični državi članici čim prej predložiti tudi izvod informacij, ki so ga posredovali (ali ki ga bodo posredovali) svojim uporabnikom, kot je določeno v drugem odstavku člena 96(1) PSD2.

2.4. Ponudniki plačilnih storitev bi morali pristojnemu organu v matični državi članici predložiti vse dodatne informacije, ki so na voljo in ki so po njihovem mnenju pomembne za pristojni organ, tako da k standardizirani predlogi priložijo dopolnilno dokumentacijo v obliki ene ali več prilog.

2.5. Odzvati bi se morali na vse zahteve pristojnega organa v matični državi članici po predložitvi dodatnih informacij ali pojasnil v zvezi s predloženo dokumentacijo.

2.6. Ves čas bi morali ohranjati zaupnost in celovitost informacij, ki jih izmenjujejo s pristojnim organom v matični državi članici in pred slednjim dokazati tudi svojo istovetnost.

Prvo poročilo

2.7. Ponudniki plačilnih storitev bi morali pristojnemu organu v matični državi članici predložiti prvo poročilo ob prvem odkritju večjega operativnega ali varnostnega incidenta.

2.8. To poročilo bi pristojnemu organu morali poslati v štirih urah od trenutka, ko je bil večji operativni varnostni incident prvič odkrit, ali takoj, ko so kanali poročanja pristojnega organa, za katere je znano, da niso na voljo ali v tem času ne delujejo, ponovno na voljo/delujoči.

2.9. Ponudniki plačilnih storitev bi morali pristojnemu organu v matični državi članici predložiti prvo poročilo tudi, kadar incident, ki prej še ni veljal za večjega, postane večji incident. V tem posebnem primeru bi morali ponudniki plačilnih storitev poslati pristojnemu organu prvo poročilo takoj, ko se ugotovi sprememba statusa, ali takoj, ko so kanali poročanja pristojnega organa, za katere je znano, da niso na voljo ali v tem času ne delujejo, ponovno na voljo/delujoči.

2.10. Ponudniki plačilnih storitev bi morali v svoja prva poročila vključiti glavne informacije (tj. razdelek A priloge), s katerimi predstavijo nekatere osnovne značilnosti incidenta in njegove pričakovane posledice na podlagi razpoložljivih informacij, ki so na voljo takoj po odkritju ali prerazvrstitvi incidenta. Kadar dejanski podatki niso na voljo, bi se morali ponudniki plačilnih storitev zateči k uporabi ocenjenih vrednosti. V svojem prvem poročilu bi morali navesti tudi datum naslednje dopolnitve, ki bi se morala opraviti čim prej in v vsakem primeru najpozneje v treh delovnih dneh.

Vmesno poročilo

2.11. Ponudniki plačilnih storitev bi morali predložiti vmesno poročilo vsakič, ko menijo, da gre za pomembnejšo dopolnitev informacij glede statusa, in sicer vsaj do datuma naslednje dopolnitve, določenega v predhodnem poročilu (bodisi v prvem ali predhodnem vmesnem poročilu).

2.12. Pristojnemu organu bi morali predložiti prvo vmesno poročilo s podrobnejšim opisom incidenta in njegovih posledic (razdelek B predloge). Poleg tega bi morali pripraviti dodatna vmesna poročila z dopolnjenimi informacijami, ki so že bile navedene v razdelkih A in B predloge, in sicer vsaj kadar se seznanijo z novimi informacijami ali večjimi spremembami, ki so se pojavile po predhodnem obvestilu (npr. ali se je incident stopnjeval ali ublažil, novi ugotovljeni vzroki ali ukrepi za odpravo težave). Ponudniki plačilnih storitev bi morali v vsakem primeru pripraviti vmesno poročilo na zahtevo pristojnega organa matične države članice.

2.13. Kot v primeru prvih poročil bi morali ponudniki plačilnih storitev tudi v tem primeru uporabiti ocenjene vrednosti, kadar dejanski podatki niso na voljo.

2.14. Poleg tega bi morali v vsakem poročilu navesti tudi datum naslednje dopolnitve, ki bi se morala opraviti čim prej in v vsakem primeru najpozneje v treh delovnih dneh. Če ponudnik plačilne storitve ne bi mogel upoštevati predvidenega datuma naslednje dopolnitve, bi se moral obrniti na pristojni organ, da bi mu pojasnil razloge za zamudo, predlagal nov predviden rok za predložitev (največ tri delovne dni) in poslal novo vmesno poročilo, v katerem bi bile dopolnjene izključno informacije o predvidenem datumu naslednje dopolnitve.

2.15. Ponudniki plačilnih storitev bi morali poslati zadnje vmesno poročilo po ponovni vzpostavitvi rednih dejavnosti in običajnega poslovanja, o čemer obvestijo pristojni organ. Ponovno vzpostavljeno običajno poslovanje bi bilo treba razumeti kot ponovno izvajanje

dejavnosti/operacij na isti ravni storitve/pod istimi pogoji, kot je opredelil ponudnik plačilnih storitev ali kot je določeno na zunanji ravni v sporazumu o ravni storitve v smislu časa obdelave, zmogljivosti, varnostnih zahtev itd., in kadar se ukrepi za obvladovanje nepredvidljivih okoliščin ne izvajajo več.

2.16. Če se običajno poslovanje vzpostavi še pred iztekom štirih ur po odkritju incidenta, bi si ponudniki plačilnih storitev morali prizadevati za sočasno posredovanje prvega in zadnjega vmesnega poročila (tj. izpolniti razdelka A in B predloge) do izteka štiriurnega roka.

Končno poročilo

2.17. Ponudniki plačilnih storitev bi morali poslati končno poročilo, ko je opravljena analiza temeljnih vzrokov (ne glede na to, ali se blažilni ukrepi že izvajajo oziroma ali je bil končni temeljni vzrok že opredeljen) in ko so na voljo dejanski podatki, ki lahko nadomestijo ocenjene vrednosti.

2.18. Ponudniki plačilnih storitev bi morali predložiti končno poročilo pristojnemu organu največ dva tedna po trenutku, ki šteje za vzpostavitev običajnega poslovanja. Ponudniki plačilnih storitev, ki želijo ta rok podaljšati (npr. če še vedno ni na voljo nobenih dejanskih podatkov o učinku), bi se morali obrniti na pristojni organ še pred iztekom roka in predložiti ustrezno utemeljitev za to zamudo ter navesti nov predviden datum končnega poročila.

2.19. Če imajo ponudniki plačilnih storitev možnost, da vse informacije, ki se zahtevajo v končnem poročilu (tj. v razdelku C predloge), zagotovijo v štirih urah po odkritju incidenta, bi si morali prizadevati, da v svojem prvem poročilu predložijo informacije, povezane s prvim, zadnjim vmesnim in končnim poročilom.

2.20. Prizadevati bi si morali, da v končno poročilo vključijo celovite informacije, tj. (i) dejanske podatke o učinku namesto ocenjenih vrednosti (ter vse druge dopolnitve, ki se zahtevajo v razdelku A in B predloge) in (ii) izpolnjen razdelek C predloge, v katerem se navedeta temeljni vzrok, če je že znan, ter povzetek sprejetih ali načrtovanih ukrepov za odpravo težave in preprečevanje njene ponovitve v prihodnosti.

2.21. Ponudniki plačilnih storitev bi morali končno poročilo poslati tudi, kadar na podlagi neprekinjenega ocenjevanja incidenta ugotovijo, da incident, o katerem so že poročali, ne izpolnjuje več meril, na podlagi katerih velja za večjega, in da ni pričakovati, da jih bo izpolnil, še preden se razreši. V tem primeru bi ponudniki plačilnih storitev morali poslati končno poročilo takoj, ko ugotovijo te okoliščine in v vsakem primeru do predvidenega datuma naslednjega poročila. V teh posebnih okoliščinah bi ponudniki plačilnih storitev namesto izpolnjevanja razdelka C predloge morali odkljukati okvirček „prerazvrstitev incidenta v kategorijo incidentov, ki ne veljajo za večje“ ter pojasniti razloge, ki utemeljujejo ta prehod na nižjo raven.

Smernica 3: delegirana in konsolidirana poročila

3.1. Kadar pristojni organ to dovoli, bi morali ponudniki plačilnih storitev, ki želijo na podlagi PSD2 prenesti obveznosti poročanja na tretjo stran, obvestiti o tem pristojni organ v matični državi članici in zagotoviti, da so izpolnjeni naslednji pogoji:

a. formalna pogodba, ali kjer je ustrezno, obstoječi notranji sporazumi v skupini, ki so podlaga za delegirano poročanje med ponudnikom plačilnih storitev in tretjo stranjo, nedvomno opredeljuje porazdelitev odgovornosti vseh strani. Zlasti jasno določa, da je ponudnik plačilnih storitev, na katerega je vplival incident, ne glede na možnost prenosa obveznosti poročanja, v celoti odgovoren za izpolnjevanje zahtev iz člena 96 PSD2 in za vsebino informacij, posredovanih pristojnemu organu v matični državi članici;

b. prenos obveznosti je skladen z zahtevami za uporabo zunanjih izvajalcev za izvajanje operativnih nalog, določenimi v

i. členu 19(6) PSD2 v zvezi s plačilnimi institucijami in institucijami za izdajo elektronskega denarja, ki se smiselno uporablja v skladu s členom 3 Direktive 2009/110/ES (direktive o elektronskem denarju) ali

ii. smernicah Odbora evropskih bančnih nadzornikov (CEBS) o uporabi zunanjih izvajalcev v zvezi s kreditnimi institucijami;

c. informacije se predložijo pristojnemu organu v matični državi članici vnaprej in v vsakem primeru v skladu z vsemi roki in postopki, ki jih določi pristojni organ, kadar je to primerno;

d. ustrezno se zagotovijo zaupnost občutljivih podatkov ter kakovost, skladnost, celovitost in zanesljivost informacij, ki jih je treba posredovati pristojnemu organu.

3.2. Ponudniki plačilnih storitev, ki želijo pooblaščeni tretji strani omogočiti, da izpolni obveznosti poročanja na konsolidirani podlagi (tj. s predložitvijo enega samega poročila za več ponudnikov plačilnih storitev, na katere je vplival isti večji operativni ali varnostni incident), bi morali o tem obvestiti pristojni organ v matični državi članici, navesti kontaktne podatke v rubriki „Ponudniki plačilnih storitev, na katere je incident vplival“ v predlogi in zagotoviti, da so izpolnjeni naslednji pogoji:

a. ta določba se vključi v pogodbo, ki je podlaga za delegiranje poročil;

b. konsolidirano poročanje je odvisno od tega, ali je incident posledica prekinitve storitev, ki jih izvaja tretja stran;

c. konsolidirano poročanje se omeji na ponudnike plačilnih storitev s sedežem v isti državi članici;

d. zagotovi se, da tretja stran oceni pomembnost incidenta za vsakega ponudnika plačilnih storitev, na katerega je incident vplival, in da v konsolidirano poročilo vključi samo tiste ponudnike plačilnih storitev, v zvezi s katerimi je incident razvrščen v kategorijo večjih incidentov. Zagotovi se tudi, da je ponudnik plačilnih storitev v primeru dvoma vključen v konsolidirano poročilo toliko časa, dokler se ne pojavijo dokazi, ki potrjujejo, da to ni več potrebno;

e. v primeru polj v predlogi, kjer skupen odgovor ni možen (npr. razdelek B2, B4 ali C3), se zagotovi, da jih tretja stran (i) izpolni posebej za vsakega ponudnika plačilnih storitev, na katerega je vplival incident, in pri tem opredeli še istovetnost vsakega ponudnika plačilnih storitev, na katerega se informacije nanašajo, ali (ii) da v tistih poljih, kjer je to možno, uporabi razpone, ki predstavljajo najnižje in najvišje vrednosti, ki so bile opažene ali ocenjene pri različnih ponudnikih plačilnih storitev;

f. ponudniki plačilnih storitev bi morali zagotoviti, da jih tretja stran ves čas obvešča o vseh ustreznih informacijah v zvezi z incidentom in vseh morebitnih interakcijah med tretjo stranjo in pristojnim organom ter o vsebini teh informacij, vendar samo dokler je to skladno s ciljem preprečevanja kakršnih koli kršitev zaupnosti v zvezi z informacijami, ki se nanašajo na druge ponudnike plačilnih storitev.

3.3. Ponudniki plačilnih storitev ne bi smeli prenesti svojih obveznosti poročanja, dokler o tem ne obvestijo pristojnega organa v matični državi članici, ali potem, ko so bili obveščeni, da pogodba o zunanjem izvajanju ne izpolnjuje zahtev iz smernice 3.1(b).

3.4. Ponudniki plačilnih storitev, ki želijo odstopiti od prenosa svoji obveznosti poročanja, bi morali to odločitev sporočiti pristojnemu organu v matični državi članici v skladu z roki in postopki, ki jih ta pristojni organ določi. Pristojni organ v matični državi članici bi morali tudi obvestiti o vseh pomembnih dogodkih, ki vplivajo na pooblaščeno tretjo stran in njeno zmožnost, da izpolni obveznosti poročanja.

3.5. Ponudniki plačilnih storitev bi morali dejansko izvršiti svoje obveznosti poročanja brez kakršne koli uporabe zunanje pomoči, kadar pooblaščena tretja stran ne obvesti pristojnega organa v matični državi članici o večjem operativnem ali varnostnem incidentu v skladu s členom 96 PSD2 in temi smernicami. Poleg tega bi morali tudi zagotoviti, da se o incidentu ne poroča dvakrat, tj. navedeni ponudnik plačilnih storitev in nato še tretja stran.

Smernica 4: operativna in varnostna strategija

4.1. Ponudniki plačilnih storitev bi morali zagotoviti, da njihova splošna operativna in varnostna strategija jasno opredeljuje vse odgovornosti za poročanje o incidentih v skladu s PSD2 ter vse postopke, ki se izvajajo, da bi se izpolnile zahteve iz teh smernic.

5. Smernice za pristojne organe o merilih za ocenjevanje pomembnosti incidentov in podrobnostih poročil o incidentih, ki se posredujejo drugim domačim organom

Smernica 5: ocenjevanje pomembnosti incidenta

5.1. Pristojni organi v matični državi članici bi morali oceniti pomembnost večjega operativnega ali varnostnega incidenta za druge domače organe, in sicer na podlagi svojega strokovnega mnenja ter z uporabo naslednjih meril kot glavnih kazalnikov pomembnosti navedenega incidenta:

a. vzroki incidenta sodijo v regulativno okolje drugega domačega organa (tj. njegovo področje pristojnosti);
b. posledice incidenta učinkujejo na cilje drugega domačega organa (npr. ohranjanje finančne stabilnosti);
c. incident v širšem obsegu vpliva ali bi lahko vplival na uporabnike plačilnih storitev;
d. o incidentu bodo verjetno ali so obsežno poročali mediji.

5.2. Pristojni organi v domači državi članici bi morali to ocenjevanje izvajati neprekinjeno ves čas trajanja incidenta, da bi prepoznali morebitne spremembe, zaradi katerih bi incident, ki do tedaj ni veljal za pomembnega, postal pomemben.

Smernica 6: informacije, ki jih je treba posredovati

6.1. Ne glede na druge pravne zahteve glede posredovanja z incidentom povezanih informacij drugim domačim organom, bi pristojni organi morali zagotoviti informacije o večjih operativnih ali varnostnih incidentih domačim organom, določenim na podlagi uporabe smernice 5.1 (tj. „drugi ustrezni domači organi“), in sicer najmanj ob prejetju prvega poročila (ali poročila, na podlagi katerega so se informacije začele posredovati) ter ko so obveščeni o ponovni vzpostavitvi običajnega poslovanja (tj. zadnje vmesno poročilo).

6.2. Pristojni organi bi morali drugim ustreznim domačim organom posredovati informacije, ki jih potrebujejo, da bi se ustvarila jasna slika o tem, kaj se je zgodilo in kakšne so posledice. Zato bi morali v naslednja polja predloge (v prvem ali vmesnem poročilu) navesti najmanj informacije, ki jih posreduje ponudnik plačilnih storitev:

- datum in čas odkritja incidenta;
- datum in čas začetka incidenta;

- datum in čas razrešitve ali predvidene razrešitve incidenta;
- kratek opis incidenta (vključno z neobčutljivimi deli podrobnega opisa);
- kratek opis sprejetih ali načrtovanih ukrepov za okrevanje po incidentu;
- opis, kako bi incident lahko vplival na druge ponudnike plačilnih storitev in/ali infrastrukture;
- opis (če obstaja) poročanj v medijih;
- vzrok incidenta.

6.3. Pristojni organi bi morali po potrebi opraviti ustrezno anonimizacijo in izključiti vse informacije, za katere bi lahko veljale omejitve v zvezi z zaupnostjo ali intelektualno lastnino, preden posredujejo z incidentom povezane informacije drugim ustreznim domačim organom. Kljub temu bi pristojni organi morali posredovati drugim ustreznim domačim organom ime in naslov ponudnika plačilnih storitev, ki pripravi poročilo, kadar navedeni domači organi lahko zagotovijo, da bodo z informacijami ravnali zaupno.

6.4. Pristojni organi bi morali ves čas ohranjati zaupnost in celovitost informacij, ki jih hranijo in izmenjujejo z drugimi ustreznimi domačimi organi, ter tudi sami ustrezno potrditi svojo istovetnost pred drugimi ustreznimi domačimi organi. Zlasti bi morali z vsemi informacijami, ki jih prejmejo na podlagi teh smernic, ravnati v skladu z dolžnostjo varovanja poklicne skrivnosti, določeno v PSD2, brez poseganja v veljavno pravo Unije ter nacionalne zahteve.

6. Smernice za pristojne organe o merilih za ocenjevanje pomembnih podrobnosti poročil o incidentih, ki se posredujejo Evropskemu bančnemu organu in Evropski centralni banki, ter o obliki in postopkih njihovega sporočanja

Smernica 7: informacije, ki jih je treba posredovati

7.1. Pristojni organi bi morali Evropskemu bančnemu organu in Evropski centralni banki vedno posredovati vsa poročila, ki jih prejmejo od (ali v imenu) ponudnikov plačilnih storitev, na katere je vplival večji operativni ali varnostni incident (tj. prvo, vmesno in končno poročilo).

Smernica 8: komunikacija

8.1. Pristojni organi bi morali ves čas ohranjati zaupnost in celovitost informacij, ki jih hranijo in izmenjujejo z Evropskim bančnim organom in Evropsko centralno banko, ter tudi sami ustrezno potrditi svojo istovetnost pred Evropskim bančnim organom in Evropsko centralno banko. Zlasti bi morali z vsemi informacijami, ki jih prejmejo na podlagi teh smernic, ravnati v skladu z dolžnostjo varovanja poklicne skrivnosti, določeno v PSD2, brez poseganja v veljavno pravo Unije ter nacionalne zahteve.

8.2. Da bi se preprečile zamude pri posredovanju z incidentom povezanih informacij Evropskemu bančnemu organu/Evropski centralni banki in da bi se pripomoglo k zmanjšanju tveganja prekinitve delovanja, bi pristojni organi morali podpreti ustrezna komunikacijska sredstva.

Priloga 1 – Predloge poročil za ponudnike plačilnih storitev

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**

NAVODILA ZA IZPOLNJEVANJE PREDLOG

Ponudniki plačilnih storitev bi morali izpolniti ustrezne razdelke predloge, odvisno od trenutne faze poročanja: razdelek A za prvo poročilo, razdelek B za vmesna poročila in razdelek C za končno poročilo. Če ni jasno določeno drugače, so vsa polja obvezna.

Naslov

Prvo poročilo: pomeni prvo obvestilo, ki jo ponudnik plačilnih storitev predloži pristojnemu organu v matični državi članici.

Vmesno poročilo: pomeni dopolnitev predhodnega (prvega ali vmesnega) poročila o istem incidentu.

Zadnje vmesno poročilo: poročilo, s katerim se pristojni organ v matični državi članici obvesti, da so ponovno vzpostavljene redne dejavnosti in običajno poslovanje in da se ne bodo predložila več nobena vmesna poročila.

Končno poročilo: pomeni zadnje poročilo, ki ga ponudnik plačilnih storitev pošlje v zvezi z incidentom, (i) ker je analiza temeljnih vzrokov že opravljena in ker se ocene lahko nadomestijo z dejanskimi podatki, ali (ii) ker incident več ne velja za večjega.

Prerazvrstitev incidenta v kategorijo incidentov, ki ne veljajo za večje: incident ne izpolnjuje več meril, na podlagi katerih lahko velja za večjega, in ni pričakovati, da jih bo izpolnil pred razrešitvijo. Ponudnik plačilnih storitev bi moral pojasniti razloge za prerazvrstitev na nižjo raven.

Datum in čas poročila: točen datum in čas predložitve poročila pristojnemu organu.

Identifikacijska številka incidenta, če je ustrezno (za vmesno in končno poročilo): referenčna številka, ki jo izda pristojni organ v času prvega poročila za edinstveno identifikacijo incidenta, če je ustrezno (tj. če takšno referenčno številko zagotovi pristojni organ).

A – Prvo poročilo

A 1 – Splošni podatki

Vrsta poročila:

Posamično: poročilo se nanaša na enega samega ponudnika plačilnih storitev.

Konsolidirano: poročilo se nanaša na več ponudnikov plačilnih storitev, ki izberejo možnost konsolidiranega poročanja. Polja v rubriki „Ponudnik plačilnih storitev, na katere je incident vplival“ naj ostanejo prazna (z izjemo polja „Država(-e), na katero(e) je incident vplival“), seznam ponudnikov plačilnih storitev, vključen v poročilo, pa naj se zagotovi tako, da se izpolni ustrezna preglednica (Konsolidirano poročilo – Seznam ponudnikov plačilnih storitev).

Ponudnik plačilnih storitev, na katerega je incident vplival: se nanaša na ponudnika plačilnih storitev, ki se spopada z incidentom.

Ime ponudnika plačilnih storitev: polno ime ponudnika plačilnih storitev, ki je vključen v postopek poročanja, kot je navedeno v veljavnem uradnem nacionalnem registru ponudnikov plačilnih storitev.

Edinstvena identifikacijska številka ponudnika plačilnih storitev, če je ustrezno: ustrezna edinstvena identifikacijska številka, ki se uporablja v vsaki državi članici za identifikacijo ponudnika plačilnih storitev in ki jo ponudnik plačilnih storitev navede, če polje „Številka dovoljenja za opravljanje plačilnih storitev“, ni izpolnjeno.

Številka dovoljenja za opravljanje plačilnih storitev: številka dovoljenja v matični državi članici.

Vodja skupine: v primeru skupin subjektov na podlagi opredelitve v členu 4(40) Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter

2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES navedite ime vodje skupine.

Matična država: država članica, v kateri je registrirani sedež ponudnika plačilnih storitev, ali, če ponudnik plačilnih storitev v skladu z nacionalnim pravom nima registriranega sedeža, država članica, kjer je njegov glavni sedež.

Država(-e), na katero(-e) je incident vplival: država ali države, v kateri se je pokazal učinek incidenta (npr. incident je vplival na več podružnic ponudnika plačilnih storitev v različnih državah). To je lahko matična država članica ali pa tudi ne.

Glavna kontaktna oseba: ime in priimek osebe, odgovorne za poročanje o incidentu, ali, če tretja stran poroča v imenu ponudnika plačilnih storitev, na katerega je incident vplival, ime in priimek osebe na čelu oddelka za obvladovanje incidentov/tveganj ali podobnega področja pri ponudniku plačilnih storitev, na katerega je incident vplival.

E-naslov: naslov elektronske pošte, na katerega se lahko po potrebi naslovijo vse zahteve za dodatna pojasnila. To je lahko zasebni naslov ali naslov v podjetju.

Telefon: telefonska številka, na katero se lahko po potrebi pokliče v primeru zahtev za dodatna pojasnila. To je lahko zasebna telefonska številka ali telefonska številka v podjetju.

Druga kontaktna oseba: ime in priimek druge osebe, na katero se pristojni organ lahko obrne z vprašanji o incidentu, kadar glavna kontaktna oseba ni na voljo. Če tretja stran poroča v imenu ponudnika plačilnih storitev, na katerega je incident vplival, se navedeta ime in priimek dodatne osebe iz oddelka za obvladovanje incidentov/tveganj ali podobnega področja pri ponudniku plačilnih storitev, na katerega je incident vplival.

E-naslov: naslov elektronske pošte druge kontaktne osebe, na katerega se lahko po potrebi naslovijo vse zahteve za dodatna pojasnila. To je lahko zasebni naslov ali naslov v podjetju.

Telefon: telefonska številka druge kontaktne osebe, na katero se lahko po potrebi pokliče v primeru zahtev za dodatna pojasnila. To je lahko zasebna telefonska številka ali telefonska številka v podjetju.

Subjekt, ki poroča: ta razdelek bi bilo treba izpolniti, če obveznosti poročanja izpolnjuje tretja stran v imenu ponudnika plačilnih storitev, na katerega je incident vplival.

Ime subjekta, ki poroča: polno ime subjekta, ki poroča o incidentu, kot je navedeno v veljavnem uradnem nacionalnem poslovnem registru.

Edinstvena identifikacijska številka, če je ustrezno: ustrezna edinstvena identifikacijska številka, ki se uporablja v državi tretje strani za identifikacijo tretje strani, ki poroča o incidentu, in ki jo subjekt, ki poroča, navede, če polje „Številka dovoljenja“ ni izpolnjeno.

Številka dovoljenja, če je ustrezno: številka dovoljenja tretje strani v državi tretje strani, kadar je to ustrezno.

Glavna kontaktna oseba: ime in priimek osebe, odgovorne za poročanje o incidentu.

E-naslov: naslov elektronske pošte, na katerega se lahko po potrebi naslovijo vse zahteve za dodatna pojasnila. To je lahko zasebni naslov ali naslov v podjetju.

Telefon: telefonska številka, na katero se lahko po potrebi pokliče v primeru zahtev za dodatna pojasnila. To je lahko zasebna telefonska številka ali telefonska številka v podjetju.

Druga kontaktna oseba: ime in priimek druge osebe pri subjektu, ki poroča o incidentu, na katero se pristojni organ lahko obrne, kadar glavna kontaktna oseba ni na voljo.

E-naslov: naslov elektronske pošte druge kontaktne osebe, na katerega se lahko po potrebi naslovijo vse zahteve za dodatna pojasnila. To je lahko zasebni naslov ali naslov v podjetju.

Telefon: telefonska številka druge kontaktne osebe, na katero se lahko po potrebi pokliče v primeru zahtev za dodatna pojasnila. To je lahko zasebna telefonska številka ali telefonska številka v podjetju.

A 2 – Odkrivanje incidenta in začetna razvrstitev

Datum in čas odkritja incidenta: datum in čas, ko je bil incident prvič odkrit.

Incident odkril: navedite, ali je incident odkril uporabnik plačilnih storitev, druga oseba pri ponudniku plačilnih storitev (npr. ki opravlja naloge notranje revizije) ali zunanja stran (npr. zunanji ponudnik storitev). Če ne gre za nikogar od navedenih, to pojasnite v ustreznem polju.

Kratek in splošen opis incidenta: na kratko pojasnite najpomembnejše elemente incidenta, vključno z najverjetnejšimi vzroki, takojšnjimi učinki itd.

Predviden čas naslednje dopolnitve: navedite predviden čas predložitve naslednje dopolnitve (vmesno ali končno poročilo).

B – Vmesno poročilo

B 1 – Splošni podatki

Podrobnejši opis incidenta: opišite glavne lastnosti incidenta in pri tem izpolnite vsaj točke, ki so vključene v vprašalnik (s katerimi specifičnimi elementi se spopada ponudnik plačilnih storitev, kako se je incident začel in stopnjeval, možne povezave s prejšnjim incidentom, posledice, zlasti za uporabnike plačilnih storitev, itd.).

Datum in čas začetka incidenta: datum in čas, ko se je incident začel, če sta poznana.

Status incidenta:

diagnostika: značilnosti incidenta so bile pravkar ugotovljene;
popravilo škode: ponovna konfiguracija napadenih elementov je v teku;
okrevanje: elementi, ki so utrpeli škodo, ponovno vzpostavljajo svoje prejšnje stanje;
razrešitev: s plačili povezana storitev se ponovno izvaja.

Datum in čas razrešitve ali pričakovane razrešitve incidenta: navedite datum in čas opravljene ali pričakovane ponovne vzpostavitve nadzora nad incidentom in običajnega poslovanja.

B 2 – Razvrstitev incidenta/Informacije o incidentu

Celoten učinek: navedite, na katere razsežnosti je incident vplival. Odkljukate lahko več okvirčkov.

Celovitost: lastnost , ki vključuje ohranjanje točnosti in popolnosti sredstev (vključno s podatki).

Razpoložljivost: lastnost s plačilom povezanih storitev, ki vključuje dostopnost in možnost uporabe s strani uporabnikov plačilnih storitev.

Zaupnost: lastnost, ki pomeni, da se informacije ne dajo na voljo ali ne razkrivajo nepooblaščenim posameznikom, subjektom ali postopkom.

Avtentičnost: lastnost, ki pomeni, da je vir točno ta, za katerega se predstavlja.

Neprekinjenost: lastnost postopkov, opravil in sredstev organizacije, potrebna za izvajanje s plačilom povezanih storitev, tako da so te v celoti dostopne in se izvajajo na sprejemljivih, vnaprej opredeljenih ravneh.

Transakcije, na katere je incident vplival: Ponudniki plačilnih storitev bi morali navesti morebitne mejne vrednosti, ki jih je incident dosegel oziroma ki jih bo verjetno dosegel, ter vse povezane podatke: število transakcij, na katere je incident vplival, odstotek takih transakcij glede na število plačilnih transakcij, izvedenih iz isto plačilno storitvijo, na katero je vplival incident, ter skupno vrednost transakcij. Ponudniki plačilnih storitev bi morali navesti posebne vrednosti teh spremenljivk bodisi z dejanskimi podatki ali ocenami. Subjekti, ki poročajo v imenu več

ponudnikov plačilnih storitev (tj. konsolidirano poročanje), lahko namesto tega navedejo razpon vrednosti, s katerim prikažejo najnižjo in najvišjo vrednost, ločeni z vezajem, ki sta bili ugotovljeni ali ocenjeni znotraj skupine ponudnikov plačilnih storitev, zajetih v poročilu. Ponudniki plačilnih storitev bi praviloma morali „transakcije, na katere je incident vplival“, razumeti kot vse domače in čezmejne transakcije, na katere je ali verjetno bo incident neposredno ali posredno vplival, ter zlasti kot tiste transakcije, pri katerih ni bilo mogoče sprožiti zahtevo po transakciji ali jih obdelati, tiste, pri katerih se je spremenila vsebina plačilnega sporočila, in tiste, ki so bile odrejene na goljufiv način (ne glede na to ali so bila sredstva povrnjena ali ne). Poleg tega bi redne plačilne transakcije morali razumeti kot letno povprečje dnevnih domačih in čezmejnih plačilnih transakcij, ki se izvajajo z istimi plačilnimi storitvami, na katere je vplival incident, pri čemer je predhodno leto referenčno obdobje za izračun. Če ponudniki plačilnih storitev menijo, da ta podatek ni reprezentativen (npr. zaradi sezonske narave), bi morali uporabiti drugo, bolj reprezentativno metriko in pristojnemu organu v polju „Pripombe“ sporočiti utemeljitev.

Uporabniki plačilnih storitev, na katere je incident vplival: Ponudniki plačilnih storitev bi morali navesti morebitne mejne vrednosti, ki jih je incident dosegel oziroma ki jih bo verjetno dosegel, ter vse s tem povezane podatke: skupno število uporabnikov plačilnih storitev, na katere je incident vplival, in odstotek takih uporabnikov glede na skupno število uporabnikov plačilnih storitev. Ponudniki plačilnih storitev bi morali navesti konkretne vrednosti teh spremenljivk, bodisi z navedbo dejanskih podatkov ali ocen. Subjekti, ki poročajo v imenu več ponudnikov plačilnih storitev (tj. konsolidirano poročanje), lahko namesto tega navedejo razpon vrednosti, s katerim prikažejo najnižjo in najvišjo vrednost, ločeni z vezajem, ki sta bili ugotovljeni ali ocenjeni znotraj skupine ponudnikov plačilnih storitev, zajetih v poročilu. Ponudniki plačilnih storitev bi morali „uporabnike plačilnih storitev, na katere je incident vplival“, razumeti kot vse stranke (domače ali tuje, potrošnike ali podjetja), ki imajo s ponudnikom plačilnih storitev, na katerega je incident vplival, sklenjeno pogodbo, na podlagi katere imajo dostop do plačilne storitve, na katero je vplival incident, in ki so ali verjetno bodo utrpeli posledice incidenta. Da bi lahko opredelili število uporabnikov plačilnih storitev, ki so morda uporabljali plačilno storitev v času trajanja incidenta, bi morali ponudniki plačilnih storitev uporabiti ocene, ki temeljijo na preteklih dejavnostih. V primeru skupin bi vsak ponudnik plačilnih storitev moral upoštevati samo svoje uporabnike plačilnih storitev. Kadar ponudnik plačilnih storitev nudi operativne storitve drugim, bi moral upoštevati samo svoje uporabnike plačilnih storitev (če obstajajo), ponudniki plačilnih storitev, ki sprejemajo te operativne storitve, pa bi morali prav tako oceniti incident v povezavi s svojimi uporabniki plačilnih storitev. Poleg tega bi ponudniki plačilnih storitev morali kot skupno število uporabnikov plačilnih storitev upoštevati seštevek domačih in tujih uporabnikov plačilnih storitev, ki so z njimi pogodbeno povezani v času incidenta (ali najnovejši razpoložljivi podatek) in ki imajo dostop do plačilne storitve, na katero je incident vplival, ne glede na njihovo velikost oziroma ne glede na to, ali veljajo za aktivne ali pasivne uporabnike plačilnih storitev.

Čas nedelovanja storitve: Ponudniki plačilnih storitev bi morali navesti, ali je incident dosegel mejno vrednost oziroma ali jo bo verjetno dosegel, ter s tem povezan podatek o trajanju: celoten čas nedelovanja storitve. Ponudniki plačilnih storitev bi morali navesti konkretne vrednosti te spremenljivke, bodisi z navedbo dejanskih podatkov ali ocen. Subjekti, ki poročajo v imenu več ponudnikov plačilnih storitev (tj. konsolidirano poročanje), lahko namesto tega navedejo razpon vrednosti, s katerim prikažejo najnižjo in najvišjo vrednost, ločeni z vezajem, ki sta bili ugotovljeni ali ocenjeni znotraj skupine ponudnikov plačilnih storitev, zajetih v poročilu. Ponudniki plačilnih storitev bi morali upoštevati obdobje, v katerem katera koli naloga, postopek ali kanal, povezan z izvajanjem plačilnih storitev, ne deluje oziroma verjetno ne bo deloval in tako onemogoča (i) odreditev in/ali izvršitev plačilne storitve in/ali (ii) dostop do plačilnega računa. Ponudniki plačilnih storitev bi morali čas nedelovanja storitve šteti od trenutka, ko nastopi nedelovanje, pri tem pa upoštevati tako časovne intervale, ki zajemajo poslovni čas, potreben za izvrševanje plačilnih

storitev, ure, v katerih se ne posluje, in obdobja izvajanja vzdrževalnih del, kadar je to ustrezno in primerno. Če ponudniki plačilnih storitev ne morejo določiti, kdaj je nastopilo nedelovanje, bi morali čas nedelovanja storitve izjemoma šteti od trenutka, ko je bilo nedelovanje zaznano.

Gospodarski učinek: Ponudniki plačilnih storitev bi morali navesti, ali je incident dosegel mejno vrednost oziroma ali jo bo verjetno dosegel, ter s tem povezane podatke: neposredne in posredne stroške. Ponudniki plačilnih storitev bi morali navesti konkretne vrednosti teh spremenljivk, bodisi z navedbo dejanskih podatkov ali ocen. Subjekti, ki poročajo v imenu več ponudnikov plačilnih storitev (tj. konsolidirano poročanje), lahko namesto tega navedejo razpon vrednosti, s katerim prikažejo najnižjo in najvišjo vrednost, ločeni z vezajem, ki sta bili ugotovljeni ali ocenjeni znotraj skupine ponudnikov plačilnih storitev, zajetih v poročilu. Ponudniki plačilnih storitev bi morali upoštevati tako stroške, ki so neposredno povezani z incidentom, kot tudi stroške, ki so z incidentom posredno povezani. Med drugim bi morali upoštevati razlaščena sredstva, stroške nadomestitve strojne ali programske opreme, druge forenzične ali sanacijske stroške, pristojbine zaradi neupoštevanja pogodbenih obveznosti, sankcije, zunanje obveznosti in izgubljene prihodke. V zvezi s posrednimi stroški bi morali upoštevati samo tiste, ki so že znani ali se bodo zelo verjetno materializirali.

> **Neposredni stroški:** znesek (v evrih) neposrednega stroška incidenta, vključno s sredstvi, potrebnimi za njegovo odpravo (npr. razlaščena sredstva, stroški nadomestitve strojne ali programske opreme, pristojbine zaradi neupoštevanja pogodbenih obveznosti).
>
> **Posredni stroški:** znesek (v evrih) neposrednega stroška incidenta (npr. odškodnina/nadomestilo za stranko, izgubljeni prihodki zaradi zamujenih poslovnih priložnosti, možni pravni stroški).

Visoka raven notranjega stopnjevanja: Ponudniki plačilnih storitev bi morali odgovoriti na vprašanje, ali je zaradi učinka na s plačilom povezane storitve glavni uradnik za obveščanje (ali oseba na podobnem položaju) bil oziroma verjetno bo obveščen o incidentu brez uporabe kakršnega koli rednega postopka obveščanja in ali je bil oziroma verjetno bo obveščen ves čas trajanja incidenta. V primeru delegiranega poročanja do stopnjevanja pride pri tretji strani. Upoštevati bi morali tudi vprašanje, ali je zaradi učinka incidenta na s plačilom povezane storitve bil sprožen oziroma ali se bo verjetno sprožil krizni način delovanja.

Drugi ponudniki plačilnih storitev ali ustrezne infrastrukture, na katere bi incident lahko vplival: ponudniki plačilnih storitev bi morali oceniti učinek incidenta na finančni trg, kar zajema infrastrukture finančnega trga in/ali kartične sheme, ki podpirajo ta trg in druge ponudnike plačilnih storitev. Zlasti bi morali oceniti, ali se je incident ponovil pri drugih ponudnikih plačilnih storitev oziroma ali se bo verjetno ponovil, ali je vplival oziroma ali bo verjetno vplival na nemoteno delovanje infrastruktur finančnega trga in ali je ogrozil oziroma ali bo verjetno ogrozil stabilnost celotnega finančnega sistema. Upoštevati bi morali različne razsežnosti, na primer ali je komponenta/programska oprema, na katero je incident vplival, lastniška ali splošno dostopna, ali je ogrožena mreža notranja ali zunanja in ali je ponudnik plačilnih storitev prenehal oziroma ali bo verjetno prenehal izpolnjevati svoje obveznosti znotraj infrastruktur finančnega trga, katerih član je.

Učinek na ugled: Ponudniki plačilnih storitev bi morali upoštevati stopnjo prepoznavnosti, ki jo je po njihovem najboljšem vedenju incident dosegel ali jo bo verjetno dosegel na trgu. Kot dober kazalnik možnosti vpliva incidenta na njihov ugled bi zlasti morali upoštevati verjetnost, da bo incident povzročil družbeno škodo. Upoštevati bi morali vprašanje, (i) ali je incident vplival na prepoznavni postopek, zaradi česar bodo o njem verjetno poročali oziroma so že poročali mediji (ne samo tradicionalni mediji, kot so časopisi, temveč tudi spletni dnevniki, družabna omrežja itd.), (ii) ali regulativne obveznosti niso bile oziroma ali verjetno ne bodo izpolnjene, (iii) ali je prišlo

oziroma ali bo verjetno prišlo do kršenja sankcij in (iv) ali se je ista vrsta incidenta zgodila že prej.

B 3 – Opis incidenta

Vrsta incidenta: navedite, z največjo možno gotovostjo, ali gre za operativni ali varnostni incident.

Operativni: incident, ki ga povzročijo neustrezni ali neuspeli postopki, ljudje in sistemi ali višja sila, ki vpliva na celovitost, razpoložljivost, zaupnost, avtentičnost in/ali neprekinjenost s plačilom povezanih storitev.

Varnostni: nepooblaščen dostop, uporaba, razkritje, motnje, sprememba ali uničenje sredstev ponudnika plačilnih storitev, ki vpliva na celovitost, razpoložljivost, zaupnost, avtentičnost in/ali neprekinjenost s plačilom povezanih storitev. To se lahko zgodi, kadar se ponudnik plačilnih storitev med drugim sooči s kibernetskimi napadi, neustrezno zasnovo ali izvajanjem varnostne strategije ali neustrezno fizično varnostjo.

Vzrok incidenta: navedite vzrok incidenta ali, če ta še ni znan, najverjetnejši vzrok. Odkljukate lahko več okvirčkov.

V fazi preiskave: vzrok še ni določen.

Zunanji napad: vzrok izvira od zunaj in je namerno usmerjen zoper ponudnika plačilnih storitev (npr. napadi z zlonamernim programom).

Notranji napad: vzrok izvira od znotraj in je namerno usmerjen zoper ponudnika plačilnih storitev (npr. notranja goljufija)

Vrsta napada:

Porazdeljen napad/Napad za zavrnitev storitve (D/DoS): poskus onesposabljanja spletne storitve, tako da se jo preobremeni s prometom iz več virov.

Okužba notranjih sistemov: škodljiva dejavnost, s katero se napadejo računalniški sistemi, ki poskuša ukrasti prostor na trdem disku ali čas CPU, pridobiti dostop do zasebnih podatkov, poškodovati podatke, zasuti stike z neželenimi sporočili itd.

Ciljni vdor: nepooblaščeno vohunjenje, vohljanje in kraja informacij prek kibernetskega prostora.

Drugo: vsaka druga vrsta napada, ki jo lahko doživi ponudnik plačilnih storitev neposredno ali prek ponudnika storitve. Ta okvirček bi bilo treba odkljukati zlasti v primeru napada na postopek odobritve in avtentikacije. Podrobnosti bi bilo treba navesti v praznem besedilnem polju.

Zunanji dogodki: vzrok je povezan z dogodki, na katere organizacija na splošno nima vpliva (npr. naravne nesreče, pravna vprašanja, poslovna vprašanja in odvisnost od storitev).

Človeška napaka: incident je posledica nenamerne napake osebe, ki se zgodi bodisi v okviru plačilnega postopka (npr. naložitev napačne paketne datoteke s plačili v sistem plačil) ali nekako povezano z njim (npr. nenamerna prekinitev električnega napajanja, zaradi česar se plačilna dejavnost začasno ustavi).

Neuspešen postopek: vzrok incidenta je slaba zasnova ali izvrševanje plačilnega postopka, postopkovnih kontrol in/ali podpornih postopkov (npr. postopkov za spremembo/prehod, testiranje, konfiguriranje, zmogljivosti, spremljanje).

Nedelovanje sistema: vzrok incidenta je povezan z neustrezno zasnovo, izvrševanjem, komponentami, specifikacijami, integracijo ali kompleksnostjo sistemov, ki podpirajo plačilno dejavnost.

Drugo: vzrok incidenta ni nobeden od navedenih. Dodatne podrobnosti bi bilo treba navesti v praznem besedilnem polju.

Ali je incident na vas vplival neposredno ali posredno prek ponudnika storitve?: incident je lahko usmerjen neposredno zoper ponudnika plačilnih storitev ali nanj vpliva posredno prek tretje strani. V primeru posrednega učinka navedite ime ponudnika(-ov) storitev.

B 4 – Učinek incidenta

Zgradbe (navedite naslov), na katere je incident vplival, če je ustrezno: če je incident vplival na fizično zgradbo, navedite njen naslov.

Poslovni kanali, na katere je incident vplival: navedite kanal ali kanale interakcije z uporabniki plačilnih storitev, na katere je incident vplival. Odkljukate lahko več okvirčkov.

Podružnice: kraj poslovanja (ki ni sedež), ki je del ponudnika plačilnih storitev, ni pravna oseba in neposredno izvaja nekatere ali vse transakcije, povezane s poslovanjem ponudnika plačilnih storitev. Vse poslovne enote, ki jih v isti državi članici ustanovi ponudnik plačilnih storitev z glavnim sedežem v drugi državi članici, bi se morali šteti za eno samo podružnico.

E-bančništvo: uporaba računalnikov za izvajanje finančnih transakcij prek interneta.

Telefonsko bančništvo: uporaba telefonov za izvajanje finančnih transakcij.

Mobilno bančništvo: uporaba posebnih bančnih aplikacij na pametnih telefonih ali podobnih napravah za izvajanje finančnih transakcij.

Bankomati: elektromehanske naprave, ki omogočajo uporabnikom plačilnih storitev dvigovanje gotovine s svojih računov in/ali dostop do drugih storitev.

Prodajno mesto: fizičen prostor trgovca, v katerem se izvede plačilna transakcija.

Drugo: poslovni kanal, na katerega je incident vplival, ni nobeden od navedenih. Dodatne podrobnosti bi bilo treba navesti v praznem besedilnem polju.

Plačilne storitve, na katere je incident vplival: navedite tiste plačilne storitve, ki zaradi incidenta ne delujejo pravilno. Odkljukate lahko več okvirčkov.

Polog gotovine na plačilni račun: izročitev gotovine ponudniku plačilnih storitev, ki ga knjiži v dobro plačilnega računa.

Dvig gotovine s plačilnega računa: zahteva, ki jo prejme ponudnik plačilnih storitev od uporabnika plačilne storitve, da se slednjemu izroči gotovina in da se ustrezen znesek knjiži v breme njegovega plačilnega računa.

Dejavnosti, ki so potrebne za upravljanje plačilnega računa: tiste dejavnosti, ki jih je treba izvajati na plačilnem računu, da bi aktivirali, deaktivirali in/ali vzdrževali (npr. odpiranje, blokiranje).

Pridobivanje plačilnih instrumentov: plačilna storitev, ki zajema sklenitev pogodbenega razmerja med ponudnikom plačilnih storitev in prejemnikom plačila, na podlagi katerega se ponudnik plačilnih storitev zaveže, da bo sprejel in obdelal plačilne transakcije, s katerimi se sredstva prenesejo na prejemnika plačila.

Kreditni prenosi: plačilna storitev v dobro plačilnega računa prejemnika plačila na podlagi plačilne transakcije ali niza plačilnih transakcij s plačilnega računa plačnika, ki jo na podlagi navodila plačnika opravi ponudnik plačilnih storitev, ki vodi njegov plačilni račun.

Direktne obremenitve: plačilna storitev za obremenitev plačilnega računa plačnika, pri kateri plačilno transakcijo odredi prejemnik plačila na podlagi soglasja, ki ga plačnik da bodisi prejemniku plačila bodisi ponudniku plačilnih storitev prejemnika plačila ali svojemu ponudniku plačilnih storitev.

Kartična plačila: plačilna storitev na podlagi infrastrukture in pravil poslovanja kartične sheme za izvedbo plačilne transakcije s katero koli kartico oziroma telekomunikacijsko, digitalno ali IT napravo ali programsko opremo, če s tem pride do transakcije z debetno ali kreditno kartico. Kartične plačilne transakcije ne zajemajo transakcij, ki temeljijo na drugih vrstah plačilnih storitev.

Izdaja plačilnih instrumentov: plačilna storitev, pri kateri ponudnik plačilnih storitev s plačnikom sklene pogodbeno razmerje, na podlagi katerega plačniku zagotavlja plačilni instrument za odreditev in obdelavo njegovih plačilnih transakcij.

Denarna nakazila: plačilna storitev, pri kateri se sredstva prejmejo od plačnika brez odprtja plačilnega računa v imenu plačnika ali prejemnika plačila, izključno zato, da se prenese ustrezen znesek prejemniku plačila ali drugemu ponudniku plačilnih storitev, ki deluje v imenu prejemnika plačila, in/ali kadar se taka sredstva prejmejo v imenu prejemnika plačila in se mu dajo na voljo.

Storitve odreditve plačil: plačilne storitve za odreditev plačilnega naloga na zahtevo uporabnika plačilnih storitev v zvezi s plačilnim računom, odprtem pri drugem ponudniku plačilnih storitev.

Storitve zagotavljanja informacij o računih: spletne storitve za zagotavljanje konsolidiranih informacij o enem ali več plačilnih računih, ki jih ima uporabnik plačilnih storitev pri drugem ponudniku plačilnih storitev ali pri več kot enem ponudniku plačilnih storitev.

Drugo: plačilna storitev, na katero je incident vplival, ni nobena od navedenih. Dodatne podrobnosti bi bilo treba navesti v praznem besedilnem polju.

Funkcionalna področja, na katera je incident vplival: navedite korak ali korake plačilnega postopka, na katere je vplival incident. Odkljukate lahko več okvirčkov.

Avtentikacija/odobritev: postopki, ki ponudniku plačilnih storitev omogočajo, da preveri istovetnost uporabnika plačilnih storitev ali upravičenost uporabe določenega plačilnega instrumenta, vključno z uporabo uporabnikovih osebnih varnostnih elementov, in soglasje uporabnika plačilnih storitev (ali tretje strani, ki deluje v imenu tega uporabnika) glede prenosa sredstev ali vrednostnih papirjev.

Komunikacija: pretok informacij za namene identifikacije, avtentikacije, priglasitve in posredovanja informacij med ponudnikom plačilnih storitev, ki vodi račun, ter ponudniki storitev odreditve plačil, ponudniki storitev zagotavljanja informacij o računih, plačniki, prejemniki plačil in drugimi ponudniki plačilnih storitev.

Kliring: postopek prenosa, uskladitve in v nekaterih primerih potrditve nalogov za prenos pred poravnavo, ki po možnosti vključuje neto izravnavo nalogov in vzpostavitev končnih pozicij za poravnave.

Neposredna poravnava: zaključek transakcije ali obdelave, da bi se s prenosom sredstev poravnale obveznosti udeležencev, kadar to dejanje izvede sam ponudnik plačilnih storitev, na katerega je vplival incident.

Posredna poravnava: Neposredna poravnava: zaključek transakcije ali obdelave, da bi se s prenosom sredstev poravnale obveznosti udeležencev, kadar to dejanje v imenu ponudnika plačilnih storitev, na katerega je vplival incident, izvede drugi ponudnik plačilnih storitev.

Drugo: funkcionalno področje, na katero je incident vplival, ni nobeno od navedenih. Dodatne podrobnosti bi bilo treba navesti v praznem besedilnem polju.

Sistemi in komponente, na katere je incident vplival: navedite, na kateri del ali dele tehnološke infrastrukture ponudnika plačilnih storitev je incident vplival. Odkljukate lahko več okvirčkov.

Aplikacija/programska oprema: programi, operacijski sistemi itd., ki podpirajo izvajanje plačilnih storitev s strani ponudnika plačilnih storitev.

Podatkovna zbirka: podatkovna struktura, v kateri so shranjene osebne informacije in informacije o plačilih, potrebne za izvrševanje plačilnih transakcij.
Strojna oprema: fizična tehnološka oprema, ki izvaja procese in/ali shranjuje podatke, ki jih ponudniki plačilnih storitev potrebujejo za izvajanje s plačilom povezanih dejavnosti.
Omrežje/infrastruktura: javna ali zasebna telekomunikacijska omrežja, ki omogočajo izmenjavo podatkov in informacij med plačilnim postopkom (npr. internet).
Drugo: sistem in komponenta, na katera je incident vplival, nista nobena od navedenih. Dodatne podrobnosti bi bilo treba navesti v praznem besedilnem polju.

Osebje, na katero je incident vplival: navedite, ali je incident imel kakršen koli učinek na osebje ponudnika plačilnih storitev in, če je imel, navedite podrobnosti v praznem besedilnem polju.

B 5 – Blažitev incidenta

Katera dejanja/ukrepi se izvajajo ali načrtujejo za okrevanje po incidentu?: opišite dejanja, ki se izvajajo ali so v načrtu za začasno obvladovanje incidenta.
Ali so aktivirani načrti za zagotavljanje neprekinjenega poslovanja/okrevanje po incidentu?: navedite, ali je temu tako, in v primeru, da je, opišite vse podrobnosti o tem, kaj se je zgodilo (tj. kdaj so bili aktivirani in kaj so ti načrti vsebovali).
Ali je ponudnik plačilnih storitev zaradi incidenta prenehal izvajati ali začel manj strogo izvajati nekatere kontrole?: navedite, ali je ponudnik plačilnih storitev moral zaradi razreševanja incidenta opustiti nekatere kontrole (npr. ali je prenehal uporabljati načelo štirih oči), in če je, navedite podrobnosti o temeljnih razlogih, ki upravičujejo manj strogo izvajanje ali prenehanje izvajanja kontrol.

C – Končno poročilo

C 1 – Splošni podatki

Dopolnitev informacij iz vmesnega poročila (povzetek): navedite dodatne informacije o ukrepih za okrevanje po incidentu in preprečevanje njegove ponovitve, analizi temeljnih vzrokov, pridobljenih izkušnjah itd.

Datum in čas zaključka incidenta: navedite datum in čas, ko naj bi se incident zaključil.

Ali so prvotne kontrole ponovno vzpostavljene?: če je ponudnik plačilnih storitev moral zaradi incidenta prenehati izvajati ali začeti manj strogo izvajati nekatere kontrole, navedite, ali so te kontrole sedaj spet vzpostavljene, in vpišite vse dodatne informacije v prazno besedilno polje.

C 2 – Analiza temeljnega vzroka in nadaljnje spremljanje

Kaj je bil temeljni vzrok, če je že poznan?: pojasnite, kaj je temeljni vzrok incidenta ali, če ta še ni znan, navedite predhodne ugotovitve, do katerih ste prišli na podlagi analize temeljnega vzroka. Ponudniki plačilnih storitev lahko priložijo datoteko s podrobnimi informacijami, če menijo, da je to potrebno.

Glavna korektivna dejanja/ukrepi, ki se izvajajo ali načrtujejo, da bi se preprečila ponovitev incidenta v prihodnosti, če so že poznani: opišite glavne sprejete ali načrtovane ukrepe za preprečevanje ponovitve incidenta v prihodnosti.

C 3 – Dodatne informacije

Ali so za namene obveščanja z incidentom seznanjeni drugi ponudniki plačilnih storitev?: navedite, s katerimi ponudniki plačilnih storitev je bil formalno ali neformalno vzpostavljen stik, da bi se jih obvestilo o incidentu, in navedite podatke o ponudnikih plačilnih storitev, ki so bili

obveščeni, informacije, ki so jim bile posredovane, ter temeljne razloge za posredovanje teh informacij.

Ali je zoper ponudnika plačilnih storitev sprožen kakršen koli pravni postopek?: navedite, ali je bil ponudnik plačilnih storitev v času priprave končnega poročila zaradi incidenta udeležen v kakršnem koli pravnem postopku (npr. je bil priveden pred sodišče ali mu je bilo odvzeto dovoljenje).