EBA/GL/2021/03

10. junij 2021

Revidirane smernice

o poročanju o večjih incidentih v skladu s PSD2

1. Obveznost glede skladnosti in poročanja

Vloga teh smernic

1. Ta dokument vsebuje smernice, izdane v skladu s členom 16 uredbe o organu ESMA[1]. V skladu s členom 16(3) uredbe o organu EBA si morajo pristojni organi in finančne institucije na vsak način prizadevati za spoštovanje smernic.

2. V smernicah je predstavljeno stališče organa EBA o ustreznih nadzorniških praksah v Evropskem sistemu finančnega nadzora oziroma o tem, kako bi bilo treba zakonodajo Unije uporabljati na posameznem področju. Pristojni organi iz člena 4(2) uredbe o organu EBA, na katere se smernice nanašajo, bi jih morali upoštevali tako, da jih ustrezno vključijo v svoje prakse (npr. s spremembo svojega pravnega okvira ali nadzornih postopkov), tudi če so smernice namenjene predvsem institucijam.

Obveznost poročanja

3. Pristojni organi morajo v skladu s členom 16(3) uredbe o EBA do (07.11.2021) organ EBA uradno obvestiti, ali upoštevajo oziroma ali nameravajo upoštevati te smernice, 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 spletišču organa EBA, z navedbo sklica „EBA/GL/2021/03“. Predložiti jih morajo osebe, ki so ustrezno 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 spletišču 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. Vsebina, področje uporabe in opredelitev pojmov

Vsebina

5. Organ EBA 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) PSD2 o takih incidentih obvestili pristojni organ v matični državi članici.

7. Poleg tega opredeljujejo, kako naj pristojni organi ocenijo pomembnost incidenta in podrobnosti v poročilih o incidentu, ki jih pristojni organi v skladu s členom 96(2) PSD2 posredujejo drugim domačim organom.

8. Te smernice obravnavajo tudi posredovanje ustreznih podrobnosti o incidentih organu EBA in ECB, 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 PSD2.

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 nenamerni.

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

12. Te smernice se uporabljajo tudi za večje incidente, ki vplivajo na funkcije, ki jih ponudniki plačilnih storitev prenesejo na tretje osebe.

Naslovniki

13. Prvi sklop smernic (oddelek 4) je naslovljen na ponudnike plačilnih storitev, kot so opredeljeni v členu 4(11) PSD2 in navedeni v členu 4(1) Uredbe (EU) št. 1093/2010.

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

Opredelitev pojmov

15. Če ni določeno drugače, imajo izrazi v teh smernicah enak pomen kot izrazi, ki se uporabljajo in so opredeljeni v PSD2. Poleg tega se v teh smernicah uporabljajo naslednje opredelitve:

operativni ali varnostni incident	Enkratni dogodek ali niz povezanih dogodkov, ki jih ponudnik plačilnih storitev ni načrtoval in ki imajo ali bodo verjetno imeli negativen učinek na celovitost, razpoložljivost, zaupnost in/ali avtentičnost s plačilom povezanih storitev.
celovitost	Lastnost, ki pomeni ohranjanje točnosti in popolnosti sredstev (vključno s podatki).
razpoložljivost	Lastnost s plačilom povezanih storitev, ki so v celoti dostopne in jih lahko uporabniki plačilnih storitev uporabljajo v skladu s sprejemljivimi ravnmi, ki jih predhodno opredeli ponudnik plačilnih storitev.
zaupnost	Lastnost, da se informacije ne dajo na voljo ali ne razkrivajo nepooblaščenim posameznikom, subjektom ali postopkom.
avtentičnost	Lastnost, da je vir točno ta, za katerega se predstavlja.
s plačilom povezane storitve	Vsaka poslovna dejavnost v smislu člena 4(3) PSD2 in vse tehnične podporne naloge, potrebne za pravilno izvajanje plačilnih storitev.

3. Izvajanje

Datum začetka uporabe

16. Te smernice se začnejo uporabljati 1. januarja 2022.

Razveljavitev

17. Naslednje smernice se razveljavijo z učinkom od 1. januarja 2022:

Smernice o poročanju o večjih incidentih v skladu z Direktivo (EU) 2015/2366 (PSD2) (EBA/GL/2017/10)

4. Smernice za ponudnike plačilnih storitev o obveščanju pristojnih organov v matični državi članici o večjih operativnih ali 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. eno ali več meril na „višji stopnji učinka“ ali

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

kakor je določeno v smernici 1.4 in na podlagi ocene, določene v teh smernicah.

1.2. Ponudniki plačilnih storitev bi morali operativni ali varnostni incident oceniti 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, v absolutnem smislu in kot odstotek skupnega števila uporabnikov plačilnih storitev.

iii. Kršitev varnosti omrežnih ali informacijskih sistemov

Ponudniki plačilnih storitev bi morali ugotoviti, ali je kakšno zlonamerno dejanje ogrozilo varnost omrežnih ali informacijskih sistemov v zvezi z izvajanjem plačilnih storitev.

iv. Čas nedelovanja storitve

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

v. Gospodarski učinek

Ponudniki plačilnih storitev bi morali celostno opredeliti denarne stroške, povezane z incidentom, ter pri tem upoštevati absolutno vrednost in po potrebi relativno pomembnost

teh stroškov glede na velikost ponudnika plačilnih storitev (tj. glede na njegov temeljni kapital).

vi. 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.

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

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

viii. Učinek na ugled

Ponudniki plačilnih storitev bi morali opredeliti, kako lahko incident oslabi zaupanje uporabnikov v samega ponudnika plačilnih storitev, in splošneje, v osnovno storitev 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 incident neposredno ali posredno vplival, 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 goljufivo naročene (ne glede na to, ali so bila sredstva povrnjena) ali katerih pravilna izvedba je bila zaradi incidenta kakor koli drugače onemogočena ali otežena.

Ponudniki plačilnih transakcij bi morali pri operativnih incidentih, ki vplivajo na zmožnost odrejanja in/ali obdelave transakcij, poročati samo o tistih, ki trajajo dlje kot eno uro. Trajanje incidenta je treba začeti meriti od trenutka, ko incident nastopi, do trenutka, ko se redne dejavnosti/operacije vzpostavijo do takšne ravni storitve, kakršna je bila zagotavljana pred incidentom.

Poleg tega bi morali ponudniki plačilnih storitev 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 za referenčno obdobje za izračun velja predhodno leto. Če ponudniki plačilnih storitev menijo, da ta podatek ni reprezentativen (npr. zaradi sezonske narave), bi morali uporabiti drugo, bolj reprezentativno metriko in ta pristop utemeljiti pristojnemu organu v ustreznem polju v predlogi (glej Prilogo).

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 katerega 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 ponudniki plačilnih storitev uporabiti ocene, ki temeljijo na preteklih dejavnostih.

Pri skupinah bi moral vsak ponudnik plačilnih storitev upoštevati samo svoje uporabnike plačilnih storitev. Če ponudnik plačilnih storitev ponuja operativne storitve drugim, bi moral upoštevati samo svoje uporabnike plačilnih storitev (če obstajajo), ponudniki plačilnih storitev, ki prejemajo te operativne storitve, pa bi morali oceniti incident v povezavi s svojimi uporabniki plačilnih storitev.

Ponudniki plačilnih transakcij bi morali pri operativnih incidentih, ki vplivajo na zmožnost odrejanja in/ali obdelave transakcij, poročati samo o tistih incidentih, ki vplivajo na uporabnike plačilnih storitve in trajajo dlje kot eno uro. Trajanje incidenta je treba začeti meriti od trenutka, ko incident nastopi, do trenutka, ko se redne dejavnosti/operacije vzpostavijo do takšne ravni storitve, kakršna je bila zagotavljana pred incidentom.

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 ali to, ali veljajo za aktivne ali pasivne uporabnike plačilnih storitev.

iii. Kršitev varnosti omrežnih ali informacijskih sistemov

Ponudniki plačilnih storitev bi morali ugotoviti, ali je kakšno zlonamerno dejanje ogrozilo dostopnost, avtentičnost, celovitost ali zaupnost omrežnih ali informacijskih sistemov (vključno s podatki) v zvezi z izvajanjem plačilnih storitev.

iv. 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 izvedbo plačilne storitve in/ali (ii) dostop do plačilnega računa. Ponudniki plačilnih storitev bi morali čas nedelovanja storitve meriti od trenutka, ko nedelovanje nastopi, pri tem pa upoštevati tako časovne intervale, ki zajemajo poslovni čas, v katerem se izvajajo plačilne storitve, kakor 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.

v. Gospodarski učinek

Ponudniki plačilnih storitev bi morali upoštevati stroške, ki se lahko neposredno povežejo z incidentom, in 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 neizpolnjevanja pogodbenih obvez, sankcije, zunanje obveznosti in izpad prihodkov. V zvezi s posrednimi stroški bi morali upoštevati samo tiste, ki so že znani ali se bodo zelo verjetno materializirali.

vi. *Visoka raven notranjega stopnjevanja*

Ponudniki plačilnih storitev bi morali upoštevati, ali je zaradi vpliva na s plačilom povezane storitve upravljalni organ, kot je opredeljen v Smernicah EBA o upravljanju tveganj, povezanih z IKT in varnostjo, bil obveščen oziroma ali bo verjetno obveščen o incidentu v skladu s smernico 60(d) iz Smernic EBA o upravljanju tveganj, povezanih z IKT in varnostjo, izven postopka periodičnega obveščanja in neprekinjeno ves čas trajanja incidenta. Ponudniki plačilnih storitev bi morali upoštevati tudi, ali je zaradi učinka incidenta na s plačilom povezane storitve bil sprožen oziroma ali bo verjetno sprožen krizni način delovanja.

vii. *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 plačilne sheme, ki zagotavljajo podporo njim in preostalim 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. Ponudniki plačilnih storitev bi morali upoštevati 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.

viii. *Učinek na ugled*

Ponudniki plačilnih storitev bi morali upoštevati stopnjo opaznosti, za katero lahko s kar največjo gotovostjo potrdijo, da jo je incident dosegel ali jo bo verjetno dosegel na trgu. Kot dober kazalnik verjetnost vpliva incidenta na njihov ugled bi zlasti morali upoštevati verjetnost, da incident povzroči družbeno škodo. Ponudniki plačilnih storitev bi morali upoštevati, ali (i) so se uporabniki plačilnih storitev in/ali drugi ponudniki plačilnih storitev pritožili zaradi škodljivega učinka incidenta, (ii) je incident vplival na prepoznaven proces, povezan s plačilno storitvijo, in bodo zato verjetno o njem poročali mediji ali pa so že (ob upoštevanju ne samo tradicionalnih medijev, kot so časopisi, ampak tudi blogov, socialnih omrežij itd.), (iii) pogodbene obveze niso bile izpolnjene ali verjetno ne bodo izpolnjene, kar vodi v objavo pravnih ukrepov proti ponudniku plačilnih storitev, (iv) niso bile izpolnjene regulativne zahteve, kar vodi v naložitev nadzornih ukrepov ali sankcij, ki so bili ali bodo verjetno javno dostopni, in (v) se je podobna vrsta incidenta že zgodila.

1.4. Ponudniki plačilnih storitev bi morali incident oceniti 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: Pragovi

Merila	Nižja stopnja učinka	Višja stopnja učinka
Transakcije, na katere je incident vplival	> 10 % rednih transakcij ponudnika plačilnih storitev (v smislu števila transakcij) **in** trajanje incidenta > 1 uro* **ali** > 500.000 EUR **in** trajanje incidenta > 1 uro*	> 25 % rednih transakcij ponudnika plačilnih storitev (v smislu števila transakcij) **ali** > 15.000.000 EUR
Uporabniki plačilnih storitev, na katere je incident vplival	> 5.000 **in** trajanje incidenta > 1 uro* **ali** > 10 % uporabnikov plačilnih storitev ponudnika plačilnih storitev **in** trajanje incidenta > 1 uro*	> 50.000 **ali** > 25 % uporabnikov plačilnih storitev ponudnika plačilnih storitev
Čas nedelovanja storitve	> 2 uri	Ni relevantno
Kršitev varnosti omrežnih ali informacijskih sistemov	Da	Ni relevantno
Gospodarski učinek	Ni relevantno	> Maks. (0,1 % temeljnega kapitala**, 200.000 EUR) **ali** > 5.000.000 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	Ni relevantno
Učinek na ugled	Da	Ni relevantno

* Prag za incident, ki traja dlje kot eno uro, velja samo za operativne incidente, ki vplivajo na zmožnost ponudnika plačilnih storitev, da odredi in/ali obdela transakcije.

**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 morali uporabiti ocene, 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 morebitno spremembo statusa incidenta bodisi navzgor (prerazvrstitev incidenta, ki ne velja za večjega, v kategorijo večjih incidentov) bodisi navzdol (prerazvrstitev večjega incidenta v kategorijo incidentov, ki ne veljajo za večje). O vsakršni prerazvrstitvi večjega incidenta v kategorijo incidentov, ki ne veljajo za večje, je treba v skladu z zahtevo iz smernice 2.21 brez nepotrebnega odlašanja obvestiti pristojni organ.

Smernica 2: postopek obveščanja

2.1. Ponudniki plačilnih storitev bi morali zbrati vse ustrezne informacije, pripraviti poročilo o incidentu z izpolnitvijo predloge v Prilogi in ga predložiti pristojnemu organu v matični državi članici z uporabo standardizirane mape, razpoložljive na spletišču organa EBA. Vsa polja v predlogi bi morali izpolniti po navodilih iz Priloge.

2.2. Ponudniki plačilnih storitev bi morali za predložitev prvega, vmesnega in končnega poročila v zvezi z istim incidentom uporabiti isto predlogo. Zato bi morali postopno izpolniti enotno predlogo in po potrebi posodobiti informacije, podane v predhodnih poročilih.

2.3. Če je ustrezno, bi morali ponudniki plačilnih storitev pristojnemu organu v matični državi članici čim prej predložiti še kopijo informacij, ki so jih sporočili (ali jih bodo sporočili) svojim uporabnikom, kot je določeno v drugem odstavku člena 96(1) PSD2.

2.4. Ponudniki plačilnih storitev bi morali na podlagi zahteve pristojnega organa v matični državi članici predložiti vse dodatne dokumente za dopolnitev informacij, predloženih na podlagi standardizirane predloge. Ponudniki plačilnih storitev bi se morali odzvati na vse zahteve pristojnega organa v matični državi članici po predložitvi dodatnih informacij ali pojasnil v zvezi s predloženo dokumentacijo.

2.5. Vse dodatne informacije iz dokumentov, ki jih predložijo pristojnemu organu bodisi na pobudo ponudnika plačilnih storitev bodisi na zahtevo pristojnega organa v skladu s smernico 2.4, morajo navesti v predlogi iz smernice 2.1

2.6. Ponudniki plačilnih storitev bi morali ves čas ohranjati zaupnost in celovitost informacij, ki jih izmenjujejo s pristojnim organom v matični državi članici, in temu vsakič ustrezno dokazati svojo istovetnost.

Prvo poročilo

2.7. Ponudniki plačilnih storitev bi morali pristojnemu organu v matični državi članici predložiti prvo poročilo, potem ko operativni ali varnostni incident razvrstijo v kategorijo večjih incidentov. Pristojni organi bi morali brez nepotrebnega odlašanja potrditi prejem prvega

poročila in dodeliti edinstveno referenčno oznako, ki incident nedvoumno označuje. Ponudniki plačilnih storitev bi morali to referenčno oznako navesti ob predložitvi posodobitve bodisi prvega poročila bodisi vmesnega ali končnega poročila v zvezi z istim incidentom, razen če se vmesno in končno poročilo predložita skupaj s prvim.

2.8. Ponudniki plačilnih storitev bi morali pristojnemu organu v matični državi članici poslati prvo poročilo v štirih urah od trenutka, ko je operativni ali varnostni incident razvrščen v kategorijo večjih incidentov. Če je znano, da kanali poročanja pristojnega organa v tem času niso na voljo ali ne delujejo, bi morali ponudniki plačilnih storitev poslati prvo poročilo takoj, ko so kanali spet na voljo/delujoči.

2.9. Ponudniki plačilnih storitev bi morali incident v skladu s smernicama 1.1 in 1.4 razvrstiti kmalu po odkritju, vendar ne pozneje kot v 24 urah, in brez nepotrebnega odlašanja po tem, ko so informacije, potrebne za razvrstitev incidenta, na razpolago ponudniku plačilnih storitev. Če je za razvrstitev incidenta potrebno več časa, bi morali ponudniki plačilnih storitev razloge za to predstaviti v prvem poročilu, predloženem pristojnemu organu.

2.10. Ponudniki plačilnih storitev bi prav tako morali pristojnemu organu v matični državi članici predložiti prvo poročilo, kadar je incident, ki prej ni veljal za večjega, na novo razvrščen v kategorijo večjih incidentov. 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 v tem času niso na voljo ali ne delujejo, spet na voljo/delujoči.

2.11. Ponudniki plačilnih storitev bi morali v prvih poročilih predložiti glavne informacije (tj. oddelek A predloge), s katerimi predstavijo nekatere osnovne značilnosti incidenta in njegove pričakovane posledice na podlagi informacij, ki so na voljo takoj po razvrstitvi incidenta v kategorijo večjih incidentov. Kadar dejanski podatki niso na voljo, bi morali ponudniki plačilnih storitev uporabiti ocene.

Vmesno poročilo

2.12. Ponudniki plačilnih storitev bi morali predložiti vmesno poročilo po vzpostavitvi rednih dejavnosti in običajnega poslovanja, o čemer obvestijo pristojni organ. Običajno poslovanje bi morali šteti za vzpostavljeno, ko dejavnosti/operacije spet izvajajo na isti ravni storitve/pod istimi pogoji, kakor so to opredelili sami ali kakor je določeno na zunanji ravni v sporazumu o ravni storitve (čas obdelave, zmogljivost, varnostne zahteve itd.), in ko se ukrepi ob nepredvidljivih dogodkih ne izvajajo več. Vmesno poročilo bi moralo vsebovati podrobnejši opis incidenta in njegove posledice (oddelek B predloge).

2.13. Če redne dejavnosti še niso vzpostavljene, morajo ponudniki plačilnih storitev pristojnemu organu predložiti vmesno poročilo v treh delovnih dneh od predložitve prvega poročila.

2.14. Ponudniki plačilnih storitev bi morali posodobiti informacije, ki so jih že navedli v oddelkih A in B predloge, kadar opazijo večje spremembe po predložitvi predhodnega poročila (npr. ali

se je incident stopnjeval ali ublažil, novi ugotovljeni vzroki ali ukrepi za odpravo težave). To velja tudi, kadar incident ni razrešen v treh delovnih dneh, kar pomeni, da bi morali ponudniki plačilnih storitev predložiti dodatno vmesno poročilo. Vsekakor bi morali dodatno vmesno poročilo predložiti na zahtevo pristojnega organa matične države članice.

2.15. Kot pri prvih poročilih bi morali ponudniki plačilnih storitev uporabiti ocene, kadar dejanski podatki niso na voljo.

2.16. Če se običajno poslovanje vzpostavi še pred iztekom štirih ur po razvrstitvi incidenta v kategorijo večjih incidentov, bi si ponudniki plačilnih storitev morali prizadevati za sočasno predložitev prvega in vmesnega poročila (tj. izpolniti oddelka A in B predloge) do izteka štiriurnega roka.

Končno poročilo

2.17. Ponudniki plačilnih storitev bi morali končno poročilo predložiti, 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 morebitne ocene.

2.18. Ponudniki plačilnih storitev bi morali končno poročilo predložiti pristojnemu organu največ 20 delovnih dni po tem, ko se šteje, da je vzpostavljeno običajno poslovanje. Če potrebujejo več časa (npr. kadar niso na voljo nobeni dejanski podatki o učinku ali temeljni vzroki še niso bili prepoznani), bi to morali sporočiti pristojnemu organu še pred iztekom roka in zamudo ustrezno utemeljiti ter navesti nov predvideni datum končnega poročila.

2.19. Če lahko ponudniki plačilnih storitev vse informacije, ki se zahtevajo v končnem poročilu (tj. v oddelku C predloge), zagotovijo v štirih urah po razvrstitvi incidenta v kategorijo večjih incidentov, bi si morali prizadevati, da informacije, povezane s prvim, vmesnim in končnim poročilom, predložijo hkrati.

2.20. Ponudniki plačilnih storitev bi morali v končno poročilo vključiti celovite informacije, tj. (i) dejanske podatke o učinku namesto ocen (ter vse druge potrebne posodobitve oddelkov A in B predloge) in (ii) izpolnjen oddelek 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 za razvrstitev med večje in da ni pričakovati, da jih bo izpolnil, še preden se razreši. V tem primeru bi morali končno poročilo poslati takoj, ko ugotovijo te okoliščine, vsekakor pa do roka za predložitev naslednjega poročila. V teh posebnih okoliščinah bi ponudniki plačilnih storitev namesto izpolnjevanja oddelka C predloge morali obkljukati okvirček „incidenta v kategorijo incidentov, ki ne veljajo za večje“ ter pojasniti razloge, ki utemeljujejo to prerazvrstitev.

Smernica 3: delegirana in konsolidirana poročila

3.1. Če pristojni organ to dovoljuje, bi morali ponudniki plačilnih storitev, ki želijo obveznost poročanja iz PSD2 prenesti na tretjo osebo, o tem obvestiti 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 med ponudnikom plačilnih storitev in tretjo osebo, ki so podlaga za delegirano poročanje, nedvomno opredeljujejo porazdelitev odgovornosti vseh strank. 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; ali

ii. Smernicah EBA o zunanjem izvajanju (EBA/GL/2019/02) v zvezi z vsemi ponudniki plačilnih storitev.

c. Informacije se predložijo pristojnemu organu v matični državi članici vnaprej, vsekakor pa v rokih in po postopkih, ki jih je določil pristojni organ, kjer je to ustrezno.

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

3.2. Ponudniki plačilnih storitev, ki želijo pooblaščeni tretji osebi omogočiti, da obveznost poročanja izpolni konsolidirano (tj. s predložitvijo enega 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 poročanja;

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

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

d. predloži se seznam vseh ponudnikov plačilnih storitev, na katere je vplival incident;

e. zagotovi se, da tretja oseba oceni pomembnost incidenta za vsakega ponudnika plačilnih storitev, na katerega je incident vplival, in da v konsolidirano poročilo zajame samo tiste ponudnike plačilnih storitev, pri katerih je bil 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 dokazujejo nasprotno;

f. zagotovi se, da polja predloge, pri katerih skupen odgovor ni mogoč (npr. oddelek B2, B4 ali C3 predloge), tretja oseba (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) uporabi zbirne vrednosti, kot so bile ugotovljene ali ocenjene pri ponudnikih plačilnih storitev;

g. tretja oseba ves čas obvešča ponudnika plačilnih storitev o vseh ustreznih informacijah glede incidenta in vseh morebitnih stikih s pristojnim organom ter o vsebini teh stikov, vendar samo do te mere, da ni kršena zaupnost informacij, ki se nanašajo na druge ponudnike plačilnih storitev.

3.3. Ponudniki plačilnih storitev obveznosti poročanja ne bi smeli prenesti, 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 obveznosti poročanja, bi morali to odločitev sporočiti pristojnemu organu v matični državi članici v rokih in po postopkih, ki jih je ta določil. Pristojni organ v matični državi članici bi morali obvestiti tudi o vseh pomembnih dogodkih, ki vplivajo na pooblaščeno tretjo osebo in njeno zmožnost, da izpolni obveznost poročanja.

3.5. Ponudniki plačilnih storitev bi morali obveznost poročanja dejansko izpolniti brez kakršne koli zunanje pomoči, kadar pooblaščena tretja oseba 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 zagotoviti, da se o incidentu ne poroča dvakrat, namreč naprej ponudnik plačilnih storitev in nato še tretja oseba.

3.6. Ponudniki plačilnih storitev bi morali zagotoviti, da se, kadar incident povzroči motnja v storitvah, ki jih zagotavlja ponudnik tehničnih storitev (ali infrastruktura), ki vpliva na več ponudnikov plačilnih storitev, delegirano poročanje nanaša na individualne podatke ponudnika plačilnih storitev (razen pri konsolidiranem poročanju).

Smernica 4: operativna in varnostna strategija

4.1. Ponudniki plačilnih storitev bi morali zagotoviti, da njihova splošna operativna in varnostna politika 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 spadajo v regulativno domeno 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 že obsežno poročali mediji.

5.2. Pristojni organi v matični 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 ustreznim domačim organom, določenim na podlagi uporabe smernice 5.1, in sicer vsaj ob prejetju prvega poročila (ali poročila, zaradi katerega so se informacije začele posredovati) ter ko so obveščeni o vzpostavitvi običajnega poslovanja (tj. vmesno poročilo).

6.2. Pristojni organi bi morali ustreznim domačim organom posredovati potrebne informacije, da bi se ustvarila jasna slika o tem, kaj se je zgodilo in kakšne so lahko posledice. Zato bi morali posredovati vsaj informacije, ki jih je ponudnik plačilnih storitev navedel v naslednjih poljih predloge (v prvem ali vmesnem poročilu):

- datum in ura, ko je bil incident razvrščen v kategorijo večjih incidentov;
- datum in ura odkritja incidenta;

- datum in ura začetka incidenta;
- datum in ura 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;
- morebitni opis poročanj v medijih;
- vzrok incidenta.

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

6.4. Pristojni organi bi morali ves čas ohranjati zaupnost in celovitost informacij, ki jih hranijo in izmenjujejo z ustreznimi domačimi organi, ter ustreznim domačim organom ustrezno potrditi svojo istovetnost. Pristojni organi bi zlasti 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 organu EBA in ECB, ter o obliki in postopkih njihovega sporočanja.

Smernica 7: informacije, ki jih je treba posredovati

7.1. Pristojni organi bi morali organu EBA in ECB vedno posredovati vsa poročila, ki jih prejmejo od (ali v imenu) ponudnikov plačilnih storitev, na katere je vplival večji operativni ali varnostni incident, in za to uporabiti standardizirano mapo, ki je na voljo na spletišču organa EBA.

Smernica 8: komunikacijske dejavnosti

8.1. Pristojni organi bi morali ves čas ohranjati zaupnost in celovitost informacij, ki jih hranijo in izmenjujejo z organom EBA in ECB, ter organu EBA in ECB ustrezno potrditi svojo istovetnost. Pristojni organi bi zlasti 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 organu EBA/ECB in da bi se pripomoglo k zmanjšanju tveganja prekinitve delovanja, bi pristojni organi morali podpreti ustrezna komunikacijska sredstva.

Priloga – Predloga poročila za ponudnike plačilnih storitev

Prvo poročilo

Prvo poročilo	v 4 urah po tem, ko je bil incident razvrščen v kategorijo večjih incidentov	Ponastavi izbor na spustnem seznamu
Datum poročila *(DD/MM/LLLL)*		Ura *(UU:MM)*
Referenčna oznaka incidenta		

A – Prvo poročilo												
A 1 – SPLOŠNI PODATKI												
Vrsta poročila												
Vrsta poročila												
Ponudnik plačilnih storitev, na katerega je incident vplival												
Ime ponudnika plačilnih storitev												
Nacionalna identifikacijska številka ponudnika plačilnih storitev												
Vodja skupine, če je ustrezno												
Država, na katero je incident vplival (ali več takih držav)	☐ AT	☐ DE	☐ ER	☐ IE	☐ LV	☐ RT						
	☐ BE	☐ DK	☐ LI	☐ IS	☐ MT	☐ RO						
	☐ BG	☐ EE	☐ GR	☐ IT	☐ NL	☐ SE						
	☐ CY	☐ ES	☐ HR	☐ LT	☐ NO	☐ SI						
	☐ CZ	☐ FI	☐ HU	☐ LU	☐ PL	☐ SK						
Glavna kontaktna oseba					E-naslov			Telefon				
Druga kontaktna oseba					E-naslov			Telefon				
Subjekt, ki poroča (ta razdelek izpolnite pri delegiranem poročanju, tj. če subjekt, ki poroča, ni ponudnik plačilnih storitev, na katerega je incident vplival)												
Ime subjekta, ki poroča												
Nacionalna identifikacijska številka												
Glavna kontaktna oseba					E-naslov			Telefon				
Druga kontaktna oseba					E-naslov			Telefon				
A 2 – ODKRITJE in RAZVRSTITEV INCIDENTA												
Datum in ura odkritja incidenta *(DD/MM/LLLL UU:MM)*												
Datum in ura razvrstitve incidenta *(DD/MM/LLLL UU:MM)*												
Incident je odkril					Če ste izbrali možnost „Drugo“, pojasnite:							
Vrsta incidenta												
Merila, ki so podlaga za poročilo o večjih incidentih	☐ Transakcije, na katere je	☐ storitev, na katere je	☐ Čas nedelovanja storitve	☐ Kršitev varnosti omrežnih ali informacijskih sistemov	☐ Gospodarski učinek	☐ Visoka raven notranjega stopnjevanja	☐ Drugi ponudniki plačilnih storitev ali relevantne infrastrukture, na katere bi lahko incident vplival	☐ Učinek na ugled				
Kratek in splošen opis incidenta												
Vpliv v drugih državah članicah EU, če je ustrezno												
Poročanje drugim organom					Če je odgovor pritrdilen, pojasnite:							
Razlogi za zamudo ob predložitvi prvega poročila												

Vmesno poročilo

Poročilo o večjem incidentu

Vmesno poročilo	največ 3 delovne dni po predložitvi prvega poročila	Ponastavi izbor na spustnem seznamu

Datum poročila *(DD/MM/LLLL)* | Ura *(UU:MM)*

Referenčna oznaka incidenta

B – Vmesno poročilo

B 1 – SPLOŠNI PODATKI

Podrobnejši opis incidenta:	
Za katero težavo gre?	
Kako je nastal incident?	
Kako se je razvil?	
Kakšne so posledice (zlasti za uporabnike plačilnih storitev)?	
Ali so bili uporabniki plačilnih storitev obveščeni o incidentu?	Če je odgovor pritrdilen, pojasnite:
Ali obstaja povezava s kakim predhodnim incidentom?	Če je odgovor pritrdilen, pojasnite:
Ali so bili prizadeti ali vpleteni drugi ponudniki storitev/tretje osebe?	Če je odgovor pritrdilen, pojasnite:
Ali se je začelo izvajati krizno upravljanje (notranje in/ali zunanje)?	Če je odgovor pritrdilen, pojasnite:
Datum in ura nastopa incidenta (če sta že ugotovljena) *(DD/MM/LLLL UU:MM)*	
Datum in ura razrešitve ali predvidene razrešitve incidenta *(DD/MM/LLLL UU:MM)*	
Funkcionalna področja, na katera je incident vplival	☐ Avtentikacija/odobritev ☐ Komunikacijske ☐ Kliring ☐ Neposredna poravnava ☐ Posredna poravnava ☐ Drugo — Če ste izbrali možnost „Dru
Spremembe prejšnjih poročil	

B 2 – RAZVRSTITEV INCIDENTA/INFORMACIJE O INCIDENTU

Transakcije, na katere je incident vplival [2]	Stopnja učinka Število transakcij, na katere je incident vplival Kot % rednega števila transakcij Vrednost transakcij, na katere je incident vplival, v EUR Trajanje incidenta (velja le za operativne incidente) Pripombe:
Uporabniki plačilnih storitev, na katere je incident vplival [3]	Stopnja učinka Število uporabnikov plačilnih storitev, na katere je incide Kot % skupnega števila uporabnikov plačilnih storitev
Kršitev varnosti omrežnih ali informacijskih sistemov	Opišite, kako je incident vplival na omrežne in informacijske sisteme.
Čas nedelovanja storitve	Skupno trajanje nedelovanja storitve — Dnevi: Ure: Minute:
Gospodarski učinek	Stopnja učinka Neposredni stroški v EUR Posredni stroški v EUR
Visoka raven notranjega stopnjevanja	Opišite raven notranjega stopnjevanja incidenta in navedite, ali je sprožil oziroma ali bo verjetno sprožil krizni način delovanja (ali enakovreden način), ter v tem primeru ta način opišite.
Drugi ponudniki plačilnih storitev ali relevantne infrastrukture, na katere bi la	Opišite, kako bi incident lahko vplival na druge ponudnike plačilnih storitev in/ali infrastrukturo.
Učinek na ugled	Opišite, kako bi incident lahko vplival na ugled ponudnika plačilnih storitev (npr. poročanje medijev, objava pravnih ukrepov ali kršitve zakona itd.).

B 3 – OPIS INCIDENTA

Vrsta incidenta	
Vzrok incidenta	☐ V fazi preiskave ☐ Zlonamerno dejanje ☐ Neuspešen postopek ☐ Nedelovanje sistema ☐ Človeške napake ☐ Zunanji dogodki ☐ Drugo — Če ste izbrali možnost „Drugo“, pojas
Ali je incident na vas vplival neposredno ali posredno prek drugega ponudnika storitev?	Če je odgovor „Posredno“, navedite ime ponudnika storitev:

B 4 – UČINEK INCIDENTA

Splošni učinek	☐ Integriteta ☐ Razpoložljivost	☐ Zaupnost ☐ Avtentičnost
Poslovni kanali, na katere je incident vplival	☐ Podružnice ☐ E-bančništvo ☐ E-trgovanje	☐ Telefonsko bančništvo ☐ Mobilno bančništvo ☐ Bankomati
	Če ste izbrali možnost „Drugo“, pojasnite:	☐ Prodajno mesto ☐ Drugo
Plačilne storitve, na katere je incident vplival	☐ Polog gotovine na plačilni račun ☐ Dvig gotovine s plačilnega računa ☐ Dejavnosti, ki so potrebne za upravljanje plačilnega računa ☐ Pridobivanje plačilnih instrumentov	☐ Kreditna plačila ☐ Direktne obremenitve ☐ Kartična plačila ☐ Izdaja plačilnih instrumentov
		☐ Denarna nakazila ☐ Storitve odreditve ☐ Storitve zagotavljanja informacij o računih

B 5 – BLAŽITEV INCIDENTA

Katera dejanja/ukrepi se izvajajo ali načrtujejo za okrevanje po incidentu?	
Ali sta bila aktivirana načrta za zagotavljanje neprekinjenega poslovanja in/ali za okrevanje po incidentu?	
Če sta bila, kdaj? *(DD/MM/LLLL, UU:MM)*	
Če je odgovor pritrdilen, načrta opišite.	

Končno poročilo

Poročilo o večjem incidentu

Izberite vrsto poročila:

v 20 dneh po predložitvi vmesnega poročila

Opišite:
(pri incidentih, prerazvrščenih iz kategorije večjih incidentov)

Ponastavi izbor na spustnem seznamu

Datum poročila *(DD/MM/LLLL)*
Referenčna oznaka incidenta

Ura *(UU:MM)*

C – Končno poročilo

Če ni bilo poslano nobeno vmesno poročilo, izpolnite tudi razdelek E.

C 1 – SPLOŠNI PODATKI

Posodobitev informacij iz prvega poročila in vmesnega poročila (ali poročil)

Spremembe prejšnjih poročil	
Druge ustrezne informacije	
Ali so vzpostavljene vse prvotne kontrole? Če je odgovor nikalen, navedite kontrole in dodaten čas, potreben za njihovo vzpostavitev.	

C 2 – ANALIZA TEMELJNEGA VZROKA IN NADALJNJE SPREMLJANJE

Kaj je bil temeljni vzrok (če je znan)?	☐ Zlonamerno dejanje ☐ Neuspešen ☐ Nedelovanje sistema ☐ Človeška napaka ☐ Zunanji dogodek ☐ Drugo
Navedite:	☐ Zlonamerna koda ☐ Zbiranje informacij ☐ Vdori ☐ Porazdeljeni napad za zavrnitev storitve (D/DoS) ☐ Namerna notranja dejanja ☐ Namerno povzročena zunanja fizična škoda ☐ Varnost vsebine informacij ☐ Goljufivo ravnanje ☐ Drugo ☐ Pomanjkljivo spremljanje in nadzor ☐ Težave s komunikacijo ☐ Nedopustne operacije ☐ Neustrezno upravljanje sprememb ☐ Neustreznost notranjih postopkov in dokumentacije ☐ Težave z okrevanjem ☐ Drugo ☐ Nedelovanje ☐ Nedelovanje ☐ Težave s ☐ Nedelovanje programske opreme/aplikacije ☐ Fizična škoda ☐ Drugo ☐ Nenamerna ☐ Opustitev ☐ Nezadostni viri ☐ Drugo ☐ Napaka dobavitelja/ponudnika tehničnih storitev ☐ Višja sila ☐ Drugo
	Če ste izbrali možnost „Drugo", pojasnite:
Drugi pomembni podatki o temeljnem vzroku	
Glavna korektivna dejanja/ukrepi, ki se izvajajo ali načrtujejo, da bi se preprečila ponovitev incidenta v prihodnosti, če so ti je znani	

C 3 – DODATNE INFORMACIJE

Ali so bili za namene obveščanja z incidentom seznanjeni drugi ponudniki pl	Če je odgovor pritrdilen, navedite podrobnosti:
Ali je bil zoper ponudnika plačilnih storitev sprožen kak pravni postopek?	Če je odgovor pritrdilen, navedite podrobnosti:
Ocenjevanje učinkovitosti izvedenega dejanja	Navedite podrobnosti:

NAVODILA ZA IZPOLNJEVANJE PREDLOGE

Ponudniki plačilnih storitev (PPS) bi morali izpolniti ustrezen oddelek predloge, odvisno od trenutne faze poročanja: oddelek A za prvo poročilo, oddelek B za vmesna poročila in oddelek C za končno poročilo. PPS bi za predložitev prvega, vmesnih in končnega poročila v zvezi z istim incidentom morali uporabiti isto predlogo. Če ni jasno določeno drugače, so vsa polja obvezna.

Naslov

Prvo poročilo: pomeni prvo obvestilo, ki ga PPS predloži pristojnemu organu v matični državi članici.

Vmesno poročilo: vsebuje podrobnejši opis incidenta in njegove posledice. To je posodobljeno prvo poročilo (in kadar je ustrezno, predhodno vmesno poročilo) o istem incidentu.

Končno poročilo: pomeni zadnje poročilo, ki ga PPS predloži v zvezi z incidentom, (i) ker je analiza temeljnih vzrokov že opravljena in se ocene lahko nadomestijo z dejanskimi podatki ali (ii) ker incident več ne velja za večjega in ga je treba na novo razvrstiti.

Prerazvrstitev incidenta v kategorijo incidentov, ki ne veljajo za večje: incident ne izpolnjuje več meril za razvrstitev med večje incidente in ni pričakovati, da jih bo izpolnil pred razrešitvijo. PPS bi morali pojasniti razloge za to prerazvrstitev.

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

Referenčna oznaka incidenta (uporabi se v vmesnih in končnem poročilu ter pri posodobitvi prvega): referenčna oznaka, ki jo izda pristojni organ ob predložitvi prvega poročila za nedvoumno opredelitev incidenta. Vsak pristojni organ bi moral kot predpono vpisati dvomestno kodo ISO [2] svoje države članice.

A - Prvo poročilo

A 1 - Splošni podatki

Vrsta poročila:

Individualno: poročilo se nanaša na enega PPS.

Konsolidirano: poročilo se nanaša na več PPS znotraj ene države članice, na katere je vplival isti večji operativni ali varnostni incident, ki uporabljajo konsolidirano poročanje. Polja v rubriki „PPS, na katere je incident vplival“ naj ostanejo prazna (razen polja „Država, na katero je incident vplival (ali več takih držav)“), seznam PPS, vključenih v poročilo, pa naj se zagotovi tako, da se izpolni ustrezna preglednica (Konsolidirano poročilo – Seznam PPS).

PPS, na katerega je incident vplival: pomeni PPS, ki se spopada z incidentom.

Ime PPS: polno ime PPS, ki je vključen v postopek poročanja, kot je navedeno v veljavnem uradnem nacionalnem registru PPS.

Nacionalna identifikacijska številka PPS: edinstvena nacionalna identifikacijska številka, ki jo uporablja pristojni organ matične države članice v nacionalnem registru za nedvoumno opredelitev PPS.

Vodja skupine: pri skupinah subjektov, kot so opredeljene v členu 40(4) PSD2, navedite ime glavnega subjekta.

Država, na katero je incident vplival (ali več takih držav): država ali države, v katerih se je incident materializiral (npr. več podružnic PPS, ki so v različnih državah, na katere je incident vplival), ne glede na resnost incidenta v drugi ali drugih državah. To ni nujno matična država članica.

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

[2] Glej oznake držav ISO-alpha-2 po ISO 3166 na https://www.iso.org/iso-3166-country-codes.html.

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

Telefon: telefonska številka, na katero se lahko po potrebi naslovijo vse zahteve za dodatna pojasnila. To je lahko zasebna telefonska številka ali telefonska številka podjetja.

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 v imenu PPS, na katerega je incident vplival, poroča tretja oseba, 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 e-naslov ali e-naslov podjetja.

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

Subjekt, ki poroča: ta oddelek je treba izpolniti, če obveznost poročanja izpolnjuje tretja oseba v imenu ponudnika plačilnih storitev, na katerega je incident vplival, če je ustrezno.

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

Nacionalna identifikacijska številka: edinstvena nacionalna identifikacijska številka, ki se uporablja v državi, v kateri je tretja oseba, za nedvoumno določitev subjekta, ki poroča o incidentu. Če je tretja oseba, ki poroča, ponudnik plačilnih storitev, bi morala biti nacionalna identifikacijska številka edinstvena nacionalna identifikacijska številka ponudnika plačilnih storitev, ki jo uporablja pristojni organ matične države članice v nacionalnem registru.

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 e-naslov ali e-naslov podjetja.

Telefon: telefonska številka, na katero se lahko po potrebi naslovijo vse zahteve za dodatna pojasnila. To je lahko zasebna telefonska številka ali telefonska številka podjetja.

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 e-naslov ali e-naslov podjetja.

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

A 2 - Odkritje in razvrstitev incidenta

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

Datum in ura razvrstitve incidenta: datum in ura, ko je bil varnostni ali operativni incident razvrščen v kategorijo večjih incidentov.

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

Vrsta incidenta: s čim večjo gotovostjo navedite, če je ta informacija na voljo, ali gre za operativni ali varnostni incident.

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

Varnostni: nepooblaščen dostop, uporaba, razkritje, motnja, sprememba ali uničenje sredstev PPS, ki vpliva na celovitost, razpoložljivost, zaupnost in/ali avtentičnost s plačilom povezanih

storitev. To se lahko zgodi med drugim, kadar pri PPS pride do kršitve varnosti omrežnih ali informacijskih sistemov.

Merila, ki so podlaga za poročilo o večjih incidentih: navedite, katera merila so podlaga za pripravo poročila o večjih incidentih. Izbrati je mogoče med več merili: transakcije, na katere je incident vplival, uporabniki plačilnih storitev, na katere je incident vplival, čas nedelovanja storitve, kršitev varnosti omrežnih ali informacijskih sistemov, gospodarski učinek, visoka raven notranjega stopnjevanja, drugi ponudniki plačilnih storitev ali ustrezne infrastrukture, na katere bi lahko incident vplival, in/ali učinek na ugled.

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

Vpliv v drugih državah članicah EU, če je ustrezno: na kratko pojasnite vpliv, ki ga je imel incident na drugo državo članico EU (npr. na uporabnike plačilnih storitev, ponudnike plačilnih storitev in/ali plačilno infrastrukturo). Če je to izvedljivo v veljavnih rokih za poročanje, predložite prevod v angleščino.

Poročanje drugim organom: navedite, ali je bilo/bo o incidentu poročano drugim organom v ločenih okvirih poročanja o incidentu, če je to znano v času poročanja. Če je tako, navedite zadevne organe.

Razlogi za zamudo ob predložitvi prvega poročila: pojasnite, zakaj ste potrebovali več kot 24 ur za razvrstitev incidenta.

B Vmesno poročilo

B 1 – Splošni podatki

Podrobnejši opis incidenta: opišite glavne značilnosti incidenta, pri čemer navedite vsaj informacije o specifični težavi in njenem ozadju, opišite, kako se je incident začel in razvijal ter kakšne so njegove posledice, zlasti za uporabnike plačilnih storitev, itd. Navedite tudi informacije o komuniciranju z uporabniki plačilnih storitev, če je to primerno.

Ali obstaja povezava s kakim predhodnim incidentom? Navedite, ali je incident povezan s predhodnimi incidenti, če je ta informacija na voljo. Če je bil incident povezan s predhodnimi incidenti, navedite, s katerimi.

Ali so bili prizadeti ali vpleteni drugi ponudniki storitev/tretje osebe? Navedite, ali je incident vplival na druge ponudnike storitev/tretje osebe oziroma ali so bili vanj vpleteni, če je ta informacija na voljo. Če je incident vplival na druge ponudnike storitev/tretje osebe ali so bili vanj vpleteni, jih navedite in podajte več informacij.

Ali se je začelo izvajati krizno upravljanje (notranje in/ali zunanje)? Navedite, ali se začelo izvajati krizno upravljanje (notranje in/ali zunanje). Če se je začelo izvajati krizno upravljanje, navedite več informacij.

Datum in ura začetka incidenta: datum in ura, ko se je incident začel, če sta znana.

Datum in ura razrešitve ali predvidene razrešitve incidenta: navedite datum in uro opravljene ali predvidene vzpostavitve nadzora nad incidentom in običajnega poslovanja.

Funkcionalna področja, na katera je incident vplival: navedite korak ali korake plačilnega postopka, na katere je incident vplival, kot so avtentikacija/odobritev, komunikacijske dejavnosti, kliring, neposredna poravnava, posredna poravnava in drugo.

Avtentikacija/odobritev: postopki, ki PPS omogočajo, da preveri istovetnost uporabnika plačilnih storitev ali upravičenost uporabe posameznega plačilnega instrumenta, vključno z uporabo uporabnikovih osebnih varnostnih elementov in soglasjem uporabnika plačilnih storitev (ali tretje osebe, ki deluje v njegovem imenu) glede prenosa sredstev.

Komunikacijske dejavnosti: pretok informacij za namene identifikacije, avtentikacije, priglasitve in obveščanja 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.

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 drug 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.

Spremembe prejšnjih poročil: navedite spremembe informacij, ki so bile podane v prejšnjih poročilih v zvezi z istim incidentom (npr. prvo, ali kadar je ustrezno, vmesno poročilo).

B 2 – Razvrstitev incidenta/Informacije o incidentu

Transakcije, na katere je incident vplival: PPS 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 z isto plačilno storitvijo, na katero je vplival incident, ter skupno vrednost transakcij. PPS bi morali navesti konkretne vrednosti teh spremenljivk, bodisi dejanske podatke bodisi ocene. PPS 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, ki jih ni bilo mogoče odrediti ali obdelati, tiste, pri katerih se je spremenila vsebina plačilnega sporočila, in tiste, ki so bile naročene goljufivo (ne glede na to ali so bila sredstva povrnjena). 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 referenčno obdobje za izračun predhodno leto. Če PPS 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. Kadar incident vpliva na plačilne transakcije v drugih valutah kakor v eurih, bi morali PPS pri izračunavanju mejnih vrednosti in poročanju o vrednosti transakcij, na katere je incident vplival, znesek transakcij v drugi valuti pretvoriti v eure na podlagi dnevnih referenčnih tečajev ECB na dan pred predložitvijo poročila o incidentu.

Uporabniki plačilnih storitev, na katere je incident vplival: PPS 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. Navesti bi morali konkretne vrednosti teh spremenljivk, bodisi dejanske podatke bodisi ocene. PPS bi morali „uporabnike plačilnih storitev, na katere je incident vplival“, razumeti kot vse stranke (domače ali tuje, potrošnike ali podjetja), ki imajo s PPS, 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 moral vsak PPS upoštevati samo svoje uporabnike plačilnih storitev. Kadar PPS ponuja operativne storitve drugim, bi moral upoštevati samo svoje uporabnike plačilnih storitev (če obstajajo), ponudniki plačilnih storitev, ki prejemajo te operativne storitve, pa bi morali incident prav tako oceniti v povezavi s svojimi uporabniki plačilnih storitev. Poleg tega bi PPS 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 ali je to veljajo za aktivne ali pasivne uporabnike plačilnih storitev.

Kršitev varnosti omrežnih ali informacijskih sistemov: PPS bi morali ugotoviti, ali je kakšno zlonamerno dejanje ogrozilo dostopnost, avtentičnost, celovitost ali zaupnost omrežnih ali informacijskih sistemov (vključno s podatki) v zvezi z izvajanjem plačilnih storitev.

Čas nedelovanja storitve: PPS 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. Navesti bi morali konkretne vrednosti te spremenljivke, bodisi dejanske podatke bodisi ocene. PPS 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 izvedbo plačilne storitve in/ali (ii) dostop do plačilnega računa. PPS bi morali čas nedelovanja storitve šteti od trenutka, ko nastopi nedelovanje, pri tem pa upoštevati tako časovne intervale, ki zajemajo poslovni čas, v katerem običajno poteka izvajanje plačilnih storitev, kakor ure, v katerih se ne posluje, in obdobja izvajanja vzdrževalnih del, kadar je to ustrezno in primerno. Če PPS ne morejo določiti, kdaj je nastopilo nedelovanje, bi morali čas nedelovanja storitve izjemoma šteti od trenutka, ko je bilo nedelovanje zaznano.

Gospodarski učinek: PPS bi morali navesti, ali je incident dosegel mejno vrednost oziroma ali jo bo verjetno dosegel ter s tem povezane podatke: neposredne in posredne stroške. Navesti bi morali konkretne vrednosti teh spremenljivk, bodisi dejanske podatke bodisi ocene. Upoštevati bi morali tako stroške, ki so neposredno povezani z incidentom, kakor stroške, ki so z incidentom povezani posredno. Med drugim bi morali upoštevati razlaščena sredstva, stroške nadomestitve strojne ali programske opreme, druge forenzične ali sanacijske stroške, nadomestila zaradi neizpolnjevanja pogodbenih obvez, sankcije, zunanje obveznosti in izpad prihodkov. V zvezi s posrednimi stroški bi morali upoštevati samo tiste, ki so že znani ali se bodo zelo verjetno materializirali. Kadar so stroški v drugih valutah kakor eurih, bi morali PPS pri izračunavanju mejne vrednosti in poročanju o vrednosti gospodarskega učinka stroške v drugi valuti pretvoriti v eure na podlagi dnevnih referenčnih tečajev ECB na dan pred predložitvijo poročila o incidentu.

> **Neposredni stroški:** stroški (v eurih), ki jih je neposredno povzročil incident, vključno s stroški odprave incidenta (npr. razlaščena sredstva, stroški nadomestitve strojne ali programske opreme, nadomestila zaradi neizpolnjevanja pogodbenih obvez).
>
> **Posredni stroški:** stroški (v eurih), ki jih je posredno povzročil incident (npr. odškodnine strankam/stroški za nadomestila, morebitni pravni stroški).

Visoka raven notranjega stopnjevanja: PPS bi morali upoštevati, ali je zaradi vpliva na s plačilom povezane storitve upravljalni organ, kot je opredeljen v Smernicah EBA o upravljanju tveganj, povezanih z IKT in varnostjo, bil obveščen oziroma ali bo verjetno obveščen o incidentu v skladu s smernico 60(d) iz Smernic EBA o upravljanju tveganj, povezanih z IKT in varnostjo, izven postopka periodičnega obveščanja in neprekinjeno ves čas trajanja incidenta. PPS bi morali upoštevati tudi, ali je zaradi učinka incidenta na s plačilom povezane storitve bil sprožen oziroma ali bo verjetno sprožen krizni način delovanja.

Drugi ponudniki plačilnih storitev ali relevantne infrastrukture, na katere bi lahko incident vplival: PPS bi morali oceniti učinek incidenta na finančni trg, ki zajema infrastrukture finančnega trga in/ali plačilne sheme, ki zagotavljajo podporo njim in preostalim ponudnikom plačilnih storitev. Zlasti bi morali oceniti, ali se je incident ponovil pri drugih PPS 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 PPS prenehal oziroma ali bo verjetno prenehal izpolnjevati svoje obveznosti znotraj infrastruktur finančnega trga, katerih član je.

Učinek na ugled: PPS bi morali upoštevati stopnjo opaznosti, 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 možnost, da incident povzroči družbeno škodo. PPS bi morali upoštevati, ali (i) so se uporabniki plačilnih storitev in/ali drugi ponudniki plačilnih storitev pritožili zaradi škodljivega učinka incidenta, (ii) je incident vplival na viden proces, povezan s plačilno storitvijo, in bodo zato verjetno o njem poročali mediji ali so že (ob upoštevanju ne samo tradicionalnih medijev, kot so časopisi, ampak tudi blogov, socialnih omrežij itd.; vendar poročanje medijev ne pomeni le negativnih komentarjev sledilcev, temveč mora obstajati utemeljeno poročilo ali večje število negativnih komentarjev/opozoril), (iii) pogodbene obveznosti niso bile izpolnjene ali pa verjeno ne bodo izpolnjene, kar vodi v objavo pravnih ukrepov proti ponudniku plačilnih storitev, (iv) niso bile izpolnjene regulativne zahteve, kar vodi v naložitev nadzornih ukrepov ali sankcij, ki so bili ali bodo verjetno javno dostopni, ali (v) se je podoben incident že zgodil.

B 3 – Opis incidenta

Vrsta incidenta: operativni ali varnostni. Dodatna pojasnila so na voljo v ustreznem polju v prvem poročilu.

Vzrok incidenta: navedite vzrok incidenta, če je že znan, sicer najverjetnejši vzrok. Izbrati je mogoče več možnosti.

V fazi preiskave: obkljukajte okvirček, kadar je vzrok trenutno neznan.

Zlonamerno dejanje: dejanja, ki namenoma ciljajo na PPS. Vključujejo zlonamerno kodo, zbiranje informacij, vdore, porazdeljeni napad za zavrnitev storitve (D/DoS), namerna notranja dejanja, namerno povzročeno zunanjo fizično škodo, varnost vsebine informacij, goljufivo ravnanje in drugo. Več podrobnosti najdete v oddelku C2 te predloge.

Neuspešen postopek: vzrok incidenta je slaba zasnova ali izvedba 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, izvedbo, komponentami, specifikacijami, integracijo ali kompleksnostjo sistemov, omrežij, infrastrukture in podatkovnih zbirk, ki podpirajo plačilno dejavnost.

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

Zunanji dogodki: vzrok je povezan z dogodki, nad katerimi organizacija navadno nima neposrednega nadzora (npr. naravne nesreče, neuspešno delovanje ponudnika tehničnih storitev).

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 storitev?: navedite, ali je bil incident neposredno usmerjen na PPS ali nanj vpliva posredno prek tretje osebe, če so te informacije na voljo. V primeru posrednega učinka navedite ime ponudnika storitev (ali več njih).

B 4 – Učinek incidenta

Splošni učinek: navedite, na katere razsežnosti je vplival operativni ali varnostni incident. Izbrati je mogoče več možnosti.

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

Razpoložljivost: lastnost s plačilom povezanih storitev, ki so v celoti dostopne in jih lahko uporabniki plačilnih storitev uporabljajo v skladu s sprejemljivimi, predhodno opredeljenimi ravnmi.

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.

Poslovni kanali, na katere je incident vplival: navedite kanal interakcije z uporabniki plačilnih storitev, na katerega je incident vplival (ali več takih kanalov). Obkljukate lahko več okvirčkov.

Podružnice: kraj poslovanja (ki ni glavni sedež), ki je del PPS, 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 PPS z glavnim sedežem v drugi državi članici, bi se morale šteti za eno podružnico.

E-bančništvo: uporaba računalnikov za izvajanje finančnih transakcij po internetu.

Telefonsko bančništvo: uporaba telefonov za izvajanje finančnih transakcij.

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

Bankomati: elektromehanska naprava, ki uporabnikom plačilnih storitev omogoča dvigovanje gotovine s svojih računov in/ali dostop do drugih storitev.

Prodajno mesto:: fizični prostor trgovca, pri katerem se odredi plačilna transakcija.

E-trgovanje: plačilna transakcija se odredi na virtualnem prodajnem mestu (npr. plačila, odrejena po internetu z uporabo kreditnih plačil, plačilnih kartic, prenosi elektronskega denarja med dvema računoma z elektronskim denarjem).

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. Obkljukate lahko več okvirčkov.

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

Dvig gotovine s plačilnega računa: zahteva, ki jo prejme PPS od uporabnika plačilne storitve, da se temu 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 izvesti na plačilnem računu, da bi ga aktivirali, deaktivirali in/ali vzdrževali (npr. odpiranje, blokiranje).

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

Kreditna plačila: 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 PPS, 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 prejemniku plačila, PPS 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.

Izdajanje plačilnih instrumentov: plačilna storitev, pri kateri PPS 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 ustrezen znesek prenese 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: plačilna storitev za odreditev plačilnega naloga na zahtevo uporabnika plačilnih storitev v zvezi s plačilnim računom, odprtem pri drugem PPS.

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

B 5 – Blažitev incidenta

Katera dejanja/ukrepi se izvajajo ali načrtujejo za okrevanje po incidentu?: navedite podrobne informacije o sprejetih ali načrtovanih ukrepih za začasno razrešitev incidenta.

Ali sta bila aktivirana načrta za zagotavljanje neprekinjenega poslovanja in/ali za okrevanje po incidentu?: navedite, ali sta bila, in v tem primeru podajte vse podrobnosti o tem, kaj se je zgodilo (tj. kdaj sta bila aktivirana in kaj sta vsebovala).

C – Končno poročilo

C 1 – Splošni podatki

Posodobitev informacij iz prvega poročila in vmesnega poročila (ali poročil) (povzetek): navedite dodatne informacije o incidentu, vključno s specifičnimi spremembami informacij, podanih v vmesnem poročilu. Vključite tudi vse druge ustrezne informacije.

Ali so vzpostavljene vse prvotne kontrole?: navedite, ali je PPS med trajanjem incidenta moral ukiniti ali oslabiti kakšne kontrole. Če je tako, navedite, ali so vse kontrole spet vzpostavljene, in če niso, v praznem besedilnem polju pojasnite, katere niso bile vzpostavljene in koliko časa bo trajalo, da se vzpostavijo.

C 2 – Analiza temeljnega vzroka in nadaljnje spremljanje

Kaj je bil temeljni vzrok, če je že znan?: navedite temeljni vzrok incidenta, če je že znan, sicer najverjetnejši vzrok. Izbrati je mogoče več možnosti. (Upoštevajte, da je treba razlikovati med temeljnim vzrokom in učinkom incidenta.)

Zlonamerno dejanje: notranja in zunanja dejanja, ki namenoma ciljajo na PPS. Ta so razdeljena v naslednje kategorije:

Zlonamerna koda: npr. virus, črv, trojanski konj, vohunska programska oprema.

Zbiranje informacij: npr. skeniranje, vohljanje, socialni inženiring.

Vdori: npr. vrivanje v privilegirani račun, vrivanje v neprivilegirani račun, vdor v aplikacijo, robot.

Porazdeljeni napad za zavrnitev storitve (D/DoS): poskus ohromitve spletne storitve tako, da se preobremeni s prometom iz več virov.

Namerna notranja dejanja: npr. sabotaža, kraja.

Namerno povzročena zunanja fizična škoda: npr. sabotaža, fizični napad na prostore/podatkovna središča.

Varnost vsebine informacij: nepooblaščen dostop do informacij, nepooblaščena sprememba informacij.

Goljufivo ravnanje: nepooblaščena uporaba virov, avtorske pravice, maskiranje, zvabljanje.

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

Neuspešen postopek: vzrok incidenta je slaba zasnova ali izvedba plačilnega postopka, postopkovnih kontrol in/ali podpornih postopkov (npr. postopkov za spremembo/prehod, testiranje, konfiguriranje, zmogljivosti, spremljanje). Ti so razdeljeni v naslednje kategorije:

Pomanjkljivo spremljanje in nadzor: npr. v zvezi s tekočimi operacijami, roki veljavnosti certifikatov, roki veljavnosti licenc, roki veljavnosti popravkov, opredeljenimi najvišjimi vrednostmi, ravnmi zapolnitve podatkovne zbirke, upravljanjem uporabniških pravic, načelom dvojnega nadzora.

Težave s komunikacijo: npr. med udeleženci na trgu ali znotraj organizacije.

Nedopustne operacije: npr. ni izmenjave certifikatov, predpomnilnik je poln.

Neustrezno upravljanje sprememb: npr. neprepoznane konfiguracijske napake, uvajanje, vključno s posodobitvami, težavami z vzdrževanjem, nepričakovanimi napakami.

Neustreznost notranjih postopkov in dokumentacije: npr. nezadostna preglednost glede funkcionalnosti, procesov in nastopa nepravilnega delovanja, neobstoj dokumentacije.

Težave z okrevanjem: npr. upravljanje nepredvidenih dogodkov, neustrezna redundanca.

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

Nedelovanje sistema: vzrok incidenta je povezan z neustrezno zasnovo, izvedbo, komponentami, specifikacijami, integracijo ali kompleksnostjo sistemov, omrežij, infrastrukture in podatkovnih zbirk, ki podpirajo plačilno dejavnost. Ti so razdeljeni v naslednje kategorije:

Nedelovanje strojne opreme: nedelovanje fizične tehnološke opreme, ki izvaja procese in/ali shranjuje podatke, ki jih PPS potrebujejo za izvedbo s plačilom povezane dejavnosti (npr. nedelovanje trdih diskov, podatkovnih središč in druge infrastrukture).

Nedelovanje omrežja: nedelovanje javnih ali zasebnih telekomunikacijskih omrežij, ki omogočajo izmenjavo podatkov in informacij (npr. po internetu) med plačilnim postopkom.

Težave s podatkovno zbirko: podatkovna struktura, v kateri so shranjene osebne in s plačili povezane informacije, potrebne za izvrševanje plačilnih transakcij.

Nedelovanje programske opreme/aplikacije: nedelovanje programov, operacijskih sistemov itd., ki podpirajo plačilne storitve PPS (npr. nepravilno delovanje, neznane funkcije).

Fizična škoda: npr. nenamerna škoda zaradi neustreznih razmer, gradbenih del.

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

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) bodisi je nekako povezana z njim (npr. nenamerna prekinitev električnega napajanja, zaradi česar se plačilna dejavnost začasno ustavi). Te so razdeljene v naslednje kategorije:

Nenamerne: npr. pomote, napake, izpusti, pomanjkanje izkušenj in znanja.

Opustitev: npr. zaradi pomanjkanja spretnosti, znanja, izkušenj, ozaveščenosti.

Nezadostni viri: npr. pomanjkanje človeških virov, nerazpoložljivost osebja.

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

Zunanji dogodek: vzrok je povezan z dogodki, nad katerimi organizacija navadno nima nadzora. Ti so razdeljeni v naslednje kategorije:

Neuspešno delovanje dobavitelja/ponudnika tehničnih storitev: npr. izpad električne energije, izpad interneta, pravne težave, poslovne težave, odvisnost od storitev.

Višja sila: npr. izpad električne energije, požari, naravne nesreče, kot so potresi, poplave, močne padavine, močan veter.

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

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

Druge pomembne informacije o temeljnem vzroku: navedite vse dodatne podrobnosti o temeljnem vzroku, vključno s predhodnimi ugotovitvami na podlagi analize temeljnega vzroka.

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

C 3 – Dodatne informacije

Ali so za namene obveščanja z incidentom seznanjeni drugi PPS?: navedite, s katerimi PPS je bil formalno ali neformalno vzpostavljen stik, da bi jih obvestili o incidentu, ter navedite podatke o PPS, ki so bili obveščeni, informacije, ki so jim bile posredovane, ter temeljne razloge za posredovanje teh informacij.

Ali je zoper PPS sprožen kak pravni postopek?: navedite, ali je bil proti PPS v času priprave končnega poročila zaradi incidenta uveden kak pravni ukrep (npr. je bil priveden pred sodišče ali mu je bilo odvzeto dovoljenje).

Ocena učinkovitosti izvedenih ukrepov: vključite podatke o samoocenjevanju učinkovitosti izvedenih ukrepov med trajanjem incidenta, če so na voljo, vključno s pridobljenimi izkušnjami v zvezi z incidentom.