

EBI/PN/2021/03

2021. gada 10. jūnijs

Pārskatītas pamatnostādnes

paziņošanai par būtiskiem incidentiem atbilstīgi MPD2

1. Atbilstība un ziņošanas pienākums

Šo pamatnostādņu statuss

1. Šajā dokumentā ir ietvertas pamatnostādnes, kas izdotas saskaņā ar EBI regulas 16. pantu¹. Kompetentajām iestādēm un finanšu iestādēm saskaņā ar EBI regulas 16. panta 3. punktu jādara viss iespējamais, lai ievērotu pamatnostādnes.
2. Pamatnostādnēs izklāstīts EBI skatījums uz atbilstošām uzraudzības praksēm Eiropas finanšu uzraudzības sistēmā vai par to, kā konkrētā jomā jāpiemēro Savienības tiesību akti. Kompetentajām iestādēm, kas minētas EBI regulas 4. panta 2. punktā un uz kurām attiecas šīs pamatnostādnes, tās ir jāievēro, iekļaujot tās attiecīgi savā praksē (piemēram, veicot grozījumus savā tiesiskajā regulējumā vai uzraudzības procesos), tostarp tad, ja pamatnostādnes ir paredzētas galvenokārt iestādēm.

Ziņošanas pienākums

3. Saskaņā ar EBI regulas 16. panta 3. punktu kompetentajām iestādēm līdz (07.11.2021) ir jāpaziņo EBI, vai tās ievēro vai paredz ievērot šīs pamatnostādnes, un, ja ne, jānorāda neievērošanas iemesli. Ja attiecīgajā termiņā šāds paziņojums nebūs saņemts, EBI uzskatīs, ka kompetentās iestādes šīs pamatnostādnes neievēro. Paziņojumi jānosūta, iesniedzot EBI tīmekļa vietnē pieejamo veidlapu ar norādi "EBA/GL/2021/03". Personām, kuras iesniedz paziņojumus, ir jābūt pilnvarotām to pārstāvēto kompetento iestāžu vārdā ziņot par prasību izpildi. Par jebkurām atbilstības statusa izmaiņām arī ir jāziņo EBI.
4. Paziņojumus publicēs EBI tīmekļa vietnē saskaņā ar 16. panta 3. punktu.

¹ Eiropas Parlamenta un Padomes Regula (ES) Nr. 1093/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/78/EK (OV L 331, 15.12.2010., 12. lpp.).

2. Priekšmets, darbības joma un definīcijas

Priekšmets

5. Šīs pamatnostādnes izriet no pilnvarām, kas EBI piešķirtas 96. panta 3. punktā Eiropas Parlamenta un Padomes 2015. gada 25. novembra Direktīvā (ES) 2015/2366 par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/EK un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK (MPD2).
6. Jo īpaši šajās pamatnostādnēs ir precizēti kritēriji, pēc kuriem maksājumu pakalpojumu sniedzējiem ir jāklasificē būtiski operacionālie vai drošības incidenti, kā arī formāts un procedūras, kas tiem jāievēro, paziņojot par šādiem incidentiem piederības dalībvalsts kompetentajai iestādei, kā ir paredzēts MPD2 96. panta 1. punktā.
7. Šajās pamatnostādnēs ir arī noteikts, kā šīs kompetentās iestādes izvērtē incidenta būtiskumu un incidenta ziņojumu elementus, kurus saskaņā ar MPD2 96. panta 2. punktu tās dara zināmus citām valsts iestādēm.
8. Turklāt šajās pamatnostādnēs ir izskatīts jautājums par EBI un ECB informēšanu par būtiskajiem paziņoto incidentu elementiem, lai sekmētu vienotu un konsekventu pieeju.

Piemērošanas joma

9. Šīs pamatnostādnes piemēro attiecībā uz būtisku operacionālo vai drošības incidentu klasifikāciju un paziņošanu par tiem saskaņā ar MPD2 96. pantu.
10. Šīs pamatnostādnes piemēro attiecībā uz visiem incidentiem, kuri atbilst “būtiska operacionālā vai drošības incidenta” definīcijai, kas aptver gan ārējus, gan iekšējus notikumus, kuri var būt ļaunprātīgi vai nejauši.
11. Šīs pamatnostādnes piemēro arī gadījumos, kad būtisks operacionālais vai drošības incidents rodas ārpus Savienības (piem., kad incidents rodas mātesuzņēmumā vai meitasuzņēmumā, kas atrodas ārpus Savienības) un ietekmē maksājumu pakalpojumus, ko sniedz Savienībā esošs maksājumu pakalpojumu sniedzējs vai nu tieši (ar maksājumu saistītu pakalpojumu sniedz ietekmētais uzņēmums, kas nav Savienības uzņēmums), vai netieši (incidenta rezultātā maksājumu pakalpojumu sniedzēja spēja turpināt veikt maksājumu darbības ir apdraudēta citā veidā).
12. Šīs pamatnostādnes ir piemērojamas arī būtiskiem incidentiem, kas ietekmē funkcijas, kuras maksājumu pakalpojumu sniedzēji kā ārpalpojumu nodrošina trešām personām.

Adresāti

13. Pirmā pamatnostādņu kopuma (4. nodaļa) adresāts ir maksājumu pakalpojumu sniedzēji (MPS), kā definēts MPD2 4. panta 11. punktā un kā minēts Regulas (ES) Nr. 1093/2010 4. panta 1. punktā.
14. Otrā un trešā pamatnostādņu kopuma (5. un 6. sadaļa) adresāts ir kompetentās iestādes, kā definēts Regulas (ES) Nr. 1093/2010 4. panta 2. punkta i) apakšpunktā.

Definīcijas

15. Ja nav norādīts citādi, termini, kas lietoti un definēti MPD2 tāda pati nozīme ir arī šajās pamatnostādnēs. Papildus šajās pamatnostādnēs piemēro šādas definīcijas.

Operacionālais vai drošības incidents	Vienreizējs notikums vai vairāki saistīti notikumi, kurus maksājumu pakalpojumu sniedzējs nav plānojis un kuri negatīvi ietekmē vai, iespējams, ietekmēs ar maksājumiem saistīto pakalpojumu integritāti, pieejamību, konfidencialitāti un/vai autentiskumu.
Integritāte	Īpašība, kas nozīmē, ka tiek garantēta aktīvu (arī datu) precizitāte un pilnīgums.
Pieejamība	Īpašība, kas nozīmē, ka ar maksājumiem saistītie pakalpojumi ir pieejami maksājumu pakalpojumu lietotājiem, un viņi tos var lietot pieņemamā līmenī, kuru iepriekš noteicis maksājuma pakalpojuma sniedzējs.
Konfidencialitāte	Īpašība, kas nozīmē, ka informācija nav pieejama vai nav izpaužama personām, organizācijām vai procesiem, kuriem nav atbilstoša pilnvarojuma.
Autentiskums	Īpašība, kas nozīmē, ka izcelsme atbilst apgalvotajam.
Ar maksājumiem saistīti pakalpojumi	Kāds no darījumdarbības veidiem MPD2 4. panta 3) punkta izpratnē, kā arī visi tehniskā atbalsta uzdevumi, kas nepieciešami maksājumu pakalpojumu pareizai sniegšanai.

3. Īstenošana

Piemērošanas datums

16. Šīs pamatnostādnes ir piemērojamas no 2022. gada 1. janvāra.

Atcelšana

17. No 2022. gada 1. janvāra atceļ šādas pamatnostādnes:

Pamatnostādnes paziņošanai par būtiskiem incidentiem saskaņā ar Direktīvu (ES) 2015/2366 (MPD2) (EBI/GL/2017/10)

4. Pamatnostādnes, kuru adresāts ir maksājumu pakalpojumu sniedzēji un kas attiecas uz paziņošanu viņu piederības dalībvalsts kompetentajai iestādei par būtiskiem operacionālajiem vai drošības incidentiem

1. pamatnostādne. Būtiska incidenta klasifikācija

1.1. Maksājumu pakalpojumu sniedzējiem kā būtiski ir jāklasificē tādi operacionālie vai drošības incidenti, kuri atbilst

- a. vienam vai vairākiem kritērijiem “augstākas ietekmes līmenī” vai
- b. trim vai vairākiem kritērijiem “zemākas ietekmes līmenī”,

kā noteikts 1.4. pamatnostādnē un atbilstoši šajās pamatnostādnēs izklāstītajam novērtējumam.

1.2. Maksājumu pakalpojumu sniedzējiem ir jānovērtē operacionālais vai drošības incidents atbilstoši šādiem kritērijiem un indikatoriem, uz kuriem tie ir balstīti:

i. Ietekmētie darījumi

Maksājumu pakalpojumu sniedzējiem ir jānosaka ietekmēto darījumu kopējā vērtība, kā arī apdraudēto maksājumu skaits procentos no to maksājumu darījumu ierastā līmeņa, kurus veic, izmantojot ietekmētos maksājumu pakalpojumus.

ii. Ietekmētie maksājumu pakalpojumu lietotāji

Maksājumu pakalpojumu sniedzējiem ir jānosaka ietekmēto maksājumu pakalpojuma lietotāju skaits gan absolūtā izteiksmē, gan procentos no maksājumu pakalpojumu lietotāju kopējā skaita.

iii. Tīkla vai informācijas sistēmu drošības pārkāpums

Maksājumu pakalpojumu sniedzējiem ir jānosaka, vai kāda ļaunprātīgā darbība ir ietekmējusi tīkla vai informācijas sistēmu darbību saistībā ar maksājumu pakalpojumu nodrošināšanu.

iv. Pakalpojuma dīkstāve

Maksājumu pakalpojumu sniedzējiem ir jānosaka laikposms, kurā pakalpojums, iespējams, nebūs pieejams maksājumu pakalpojumu lietotājam vai kurā maksājumu pakalpojumu sniedzējs nevarēs izpildīt maksājuma uzdevumu MPD2 4. panta 13. punkta izpratnē.

v. Ekonomiskā ietekme

Maksājumu pakalpojumu sniedzējiem ir holistiski jānosaka monetārās izmaksas, kas ir saistītas ar incidentu, un ir jāņem vērā gan absolūtais skaitlis, gan attiecīgā gadījumā šo izmaksu relatīvā nozīme attiecībā uz maksājumu pakalpojumu sniedzēja lielumu (t. i., maksājumu pakalpojumu sniedzēja 1. līmeņa pamatkapitālu).

vi. Augsts iekšējās eskalācijas līmenis

Maksājumu pakalpojumu sniedzējiem ir jānosaka, vai par šo incidentu ir ziņots vai varētu tikt ziņots to izpilddirektoriem.

vii. Citi potenciāli ietekmētie maksājumu pakalpojumu sniedzēji vai attiecīgās infrastruktūras

Maksājumu pakalpojumu sniedzējiem ir jānosaka sistēmiskās sekas, kādas varētu būt šim incidentam, t. i., tā potenciāls papildus sākotnēji ietekmētajam maksājumu pakalpojumu sniedzējam ietekmēt arī citus maksājumu pakalpojumu sniedzējus, finanšu tirgus infrastruktūras un/vai maksājumu shēmas.

viii. Ietekme uz reputāciju

Maksājumu pakalpojumu sniedzējiem ir jānosaka, kā šis incidents var samazināt lietotāju uzticēšanos pašam maksājumu pakalpojumu sniedzējam un vispārīgi — pamatpakalpojumam vai tirgum kopumā.

1.3. Maksājumu pakalpojumu sniedzējiem ir jāaprēķina indikatoru vērtība atbilstoši šādai metodoloģijai:

i. Ietekmētie darījumi:

Parasti maksājumu pakalpojumu sniedzējiem jēdziens “ietekmētie darījumi” ir jāizprot kā visi pašmāju un pārrobežu darījumi, kurus incidents ir tieši vai netieši ietekmējis vai varētu ietekmēt, jo īpaši tie darījumi, kurus nav bijis iespējams uzsākt vai apstrādāt, kuriem tika izmainīts maksājuma ziņojuma saturs un kuri tika pasūtīti krāpnieciski (neatkarīgi no tā, vai līdzekļi ir atgūti vai nav) vai arī ja incidents jebkādā veidā ir liedzis vai traucējis pienācīgu izpildi.

Par operacionālajiem incidentiem, kuri skar spēju uzsākt un/vai apstrādāt darījumus, maksājumu pakalpojumu sniedzējiem ir jāziņo vienīgi tad, ja incidents ilgst vairāk par vienu stundu. Incidenta ilgums ir jāmēra no brīža, kad incidents radies, līdz brīdim, kad regulārās darbības/operācijas atkal tiek nodrošinātas tādā pašā līmenī, kā pirms incidenta.

Turklāt maksājumu pakalpojumu sniedzējiem jēdziens “maksājumu darījumu ierastais līmenis” ir jāizprot kā to ikdienas pašmāju un pārrobežu maksājumu darījumu vidējais skaits gadā, kurus veic, izmantojot tos pašus maksājumu pakalpojumus, kurus ietekmēja incidents, par atsauces periodu aprēķiniem ņemot iepriekšējo gadu. Ja maksājumu pakalpojumu sniedzēji neuzskata, ka šis rādītājs ir reprezentatīvs (piem., sezonālātes dēļ), viņiem tā vietā ir jāizmanto cits, reprezentatīvāks rādītājs un atbilstošajā veidnes laukā (sk. pielikumu) ir jāsniedz kompetentajai iestādei šādas pieejas pamatojums.

ii. Ietekmētie maksājumu pakalpojumu lietotāji

Maksājumu pakalpojumu sniedzējiem ir jāizprot jēdziens “ietekmētie maksājumu pakalpojumu lietotāji” kā visi klienti (pašmāju un ārzemju, patērētāji un uzņēmumi), kuriem ar ietekmēto maksājumu pakalpojumu sniedzēju ir noslēgts līgums, kas tiem piešķir piekļuvi ietekmētajam maksājumu pakalpojumam, un kuri ir cietuši vai, visticamāk, cietīs no incidenta sekām. Maksājumu pakalpojumu sniedzējiem aplēses ir jābalsta uz iepriekšējām norisēm, lai noteiktu to maksājumu pakalpojumu lietotāju skaitu, kuri, iespējams, incidenta pastāvēšanas laikā ir izmantojuši minēto maksājumu pakalpojumu.

Grupu gadījumā katram maksājumu pakalpojumu sniedzējam ir jāņem vērā tikai paša maksājumu pakalpojumu lietotāji. Ja maksājumu pakalpojumu sniedzējs piedāvā darbības pakalpojumus citiem, šim maksājumu pakalpojumu sniedzējam ir jāņem vērā tikai savi maksājumu pakalpojumu lietotāji (ja tādi ir) un tiem maksājumu pakalpojumu sniedzējiem, kuri saņem minētos darbības pakalpojumus, ir jānovērtē incidents saistībā ar saviem maksājumu pakalpojumu lietotājiem.

Par operacionālajiem incidentiem, kuri skar spēju uzsākt un/vai apstrādāt darījumus, maksājumu pakalpojumu sniedzējiem ir jāziņo vienīgi tad, ja incidents skar maksājumu pakalpojumu lietotāju un ilgst vairāk par vienu stundu. Incidenta ilgums ir jāmēra no brīža, kad incidents radies, līdz brīdim, kad regulārās darbības/operācijas atkal tiek nodrošinātas tādā pašā līmenī, kā pirms incidenta.

Turklāt maksājumu pakalpojumu sniedzējiem kā kopējais maksājumu pakalpojumu lietotāju skaits ir jāpieņem to pašmāju un pārrobežu maksājumu pakalpojumu lietotāju kopskaits, ar kuriem incidenta laikā ir bijušas noslēgtas līgumattiecības (vai arī visnesenākais pieejamais rādītājs) un kuriem ir pieeja ietekmētajam maksājumu pakalpojumam neatkarīgi no to lieluma un no tā, vai tie ir uzskatāmi par aktīviem vai pasīviem maksājumu pakalpojumu lietotājiem.

iii. Tīkla vai informācijas sistēmu drošības pārkāpums

Maksājumu pakalpojumu sniedzējiem ir jānosaka, vai kāda ļaunprātīgā darbība ir ietekmējusi ar maksājumu pakalpojumu nodrošināšanu saistītā tīkla vai informācijas sistēmu pieejamību, autentiskumu, integritāti vai konfidencialitāti.

iv. Pakalpojuma dīkstāve

Maksājumu pakalpojumu sniedzējiem ir jāņem vērā laikposms, kurā jebkurš uzdevums, process vai kanāls, kas ir saistīts ar maksājumu pakalpojumu sniegšanu, nav vai varētu nebūt pieejams, tādējādi liedzot i) uzsākt un/vai veikt maksājumu pakalpojumu un/vai ii) piekļūt maksājumu kontam. Maksājumu pakalpojumu sniedzējiem pakalpojuma dīkstāve ir jāaprēķina no brīža, kad dīkstāve sākas, un viņiem ir jāņem vērā gan laikposmi, kuros tie ir atvērti darījumdarbībai, kas nepieciešama maksājumu pakalpojumu izpildei, gan arī laikposmi ārpus darba laika un uzturēšanas laikposmi, ja tas ir atbilstoši un piemērojami. Ja maksājumu pakalpojumu sniedzēji nevar noteikt, kad pakalpojuma dīkstāve ir sācijas, viņiem izņēmuma kārtā pakalpojuma dīkstāve ir jāaprēķina no brīža, kad tas tika konstatēts.

v. *Ekonomiskā ietekme*

Maksājumu pakalpojumu sniedzējiem ir jāņem vērā izmaksas, kas var būt gan tieši, gan netieši saistītas ar incidentu. Cita starpā maksājumu pakalpojumu sniedzējiem ir jāņem vērā ekspropriētie līdzekļi vai aktīvi, aparatūras vai programmatūras aizstāšanas izmaksas, citas tiesu vai atlīdzināšanas izmaksas, maksas, kas piemērotas līgumsaistību neizpildes dēļ, sankcijas, ārējas saistības un zaudētie ieņēmumi. Attiecībā uz netiešajām izmaksām maksājumu pakalpojumu sniedzējiem ir jāņem vērā tikai tās izmaksas, kas jau ir zināmas vai, ļoti iespējams, radīsies.

vi. *Augsts iekšējās eskalācijas līmenis*

Maksājumu pakalpojumu sniedzējiem ir jāapsver, vai incidents ietekmē ar maksājumiem saistītus pakalpojumus tā, ka tā rezultātā ir vai, iespējams, tiks informēta pārvaldības iestāde, kā ir noteikts EBA pamatnostādņēs par IKT un drošības risku pārvaldību, saskaņā ar EBI IKT un drošības risku pārvaldības pamatnostādņu 60. pamatnostādnes d) punktu par incidentu ārpus jebkuras periodiskas paziņošanas procedūras un pastāvīgi incidenta pastāvēšanas laikā. Tāpat maksājumu pakalpojumu sniedzējiem ir jāapsver, vai incidents ietekmē ar maksājumiem saistītus pakalpojumus tā, ka tā rezultātā ir noteikts vai, iespējams, tiks noteikts krīzes režīms.

vii. *Citi potenciāli ietekmētie maksājumu pakalpojumu sniedzēji vai attiecīgās infrastruktūras*

Maksājumu pakalpojumu sniedzējiem ir jānovērtē incidenta ietekme uz finanšu tirgu, ar ko saprot finanšu tirgus infrastruktūras un/vai maksājumu shēmas, kuras atbalsta to un pārējos maksājumu pakalpojumu sniedzējus. It īpaši maksājumu pakalpojumu sniedzējiem ir jānovērtē, vai incidents varētu tikt replicēts citiem maksājumu pakalpojumu sniedzējiem neatkarīgi no tā, vai tas ir ietekmējis vai, iespējams, ietekmēs finanšu tirgus infrastruktūru nevainojamu funkcionēšanu un vai tas ir negatīvi ietekmējis vai, iespējams, negatīvi ietekmēs finanšu sistēmas stabilu darbību kopumā. Maksājumu pakalpojumu sniedzējiem ir jāņem vērā dažādas dimensijas, piemēram, vai ietekmētais komponents/programmatūra ir patentēti vai vispārpieejami, vai negatīvi ietekmētais tīkls ir iekšējs vai ārējs un vai maksājumu pakalpojumu sniedzējs ir pārtraucis vai, iespējams, pārtrauks pildīt savus pienākumus tajās finanšu tirgus infrastruktūrās, kurās tas ir dalībnieks.

viii. *Ietekme uz reputāciju*

Maksājumu pakalpojumu sniedzējiem ir jāņem vērā atpazīstamības līmenis, kuru (pēc to rīcībā esošās informācijas) incidents ir panācis vai, iespējams, panāks tirgū. It īpaši maksājumu pakalpojumu sniedzējiem ir jāņem vērā varbūtība, ka incidents var izraisīt kaitējumu sabiedrībai, kā piemērots rādītājs tā potenciālam ietekmēt viņu reputāciju. Maksājumu pakalpojumu sniedzējiem ir jāņem vērā, vai: i) maksājumu pakalpojumi lietotāji un/vai citi maksājumu pakalpojumu sniedzēji ir sūdzējušies par incidenta negatīvajām sekām, ii) incidents ir ietekmējis redzamu ar maksājumu pakalpojumu saistītu procesu un tādēļ tas ir ticis vai varētu tikt atspoguļots plašsaziņas līdzekļos (ņemot vērā ne tikai tradicionālos plašsaziņas līdzekļus, piemēram, laikrakstus, bet arī blogus, sociālos tīklus utt.), iii) netiek vai, iespējams, netiks īstenotas saskaņā ar līgumiem noteiktās saistības, kuru rezultātā pret

maksājumu pakalpojumu sniedzēju tiek uzsākta tiesvedība, iv) nav ievērotas normatīvās prasības, kā rezultātā tiek noteikti uzraudzības pasākumi vai sankcijas, kas ir vai, iespējams, būs publiski pieejamas, un v) iepriekš ir noticis tāda paša veida incidents.

- 1.4. Maksājumu pakalpojumu sniedzējiem ir jānovērtē incidents, attiecībā uz katru atsevišķo kritēriju nosakot, vai līdz incidenta atrisināšanai ir sasniegtas vai, iespējams, tiks sasniegtas attiecīgās robežvērtības, kas noteiktas 1. tabulā.

1. tabula. Robežvērtības

Kritēriji	Zemāks ietekmes līmenis	Augstāks ietekmes līmenis
Ietekmētie darījumi	> 10 % no maksājumu pakalpojumu sniedzēja ierastā darījumu līmeņa (darījumu skaita ziņā) kā arī incidenta ilgums > 1 stunda* vai > 500 000 EUR kā arī incidenta ilgums > 1 stunda*	> 25 % no maksājumu pakalpojumu sniedzēja ierastā darījumu līmeņa (darījumu skaita ziņā) vai > 15 000 000 EUR
Ietekmētie maksājumu pakalpojumu lietotāji	> 5000 kā arī incidenta ilgums > 1 stunda* vai > 10 % no maksājumu pakalpojumu sniedzēja maksājumu pakalpojumu lietotājiem kā arī incidenta ilgums > 1 stunda*	> 50 000 vai > 25 % no maksājumu pakalpojumu sniedzēja maksājumu pakalpojumu lietotājiem
Pakalpojuma dīkstāve	> 2 stundas	Nepiemēro
Tīkla vai informācijas sistēmu drošības pārkāpums	Jā	Nepiemēro
Ekonomiskā ietekme	Nepiemēro	> maks. (0,1% 1. līmeņa pamatkapitāla**, 200 000 EUR) vai > 5 000 000 EUR
Augsts iekšējās eskalācijas līmenis	Jā	Jā, un, iespējams, tiks iedarbināts krīzes režīms (vai tam pielīdzināms režīms)
Citi potenciāli ietekmētie maksājumu pakalpojumu sniedzēji vai attiecīgās infrastruktūras	Jā	Nepiemēro
Ietekme uz reputāciju	Jā	Nepiemēro

* Robežvērtība, kura attiecas uz incidenta ilgumu, kas ir vairāk par vienu stundu, ir piemērojama tikai operacionālajiem incidentiem, kuri ietekmē maksājumu pakalpojumu sniedzēja spēju uzsākt un/vai apstrādāt darījumu.

**1. līmeņa pamatkapitāls, kā noteikts 25. pantā Eiropas Parlamenta un Padomes 2013. gada 26. jūnija Regulā (ES) Nr. 575/2013 par prudenciālajām prasībām attiecībā uz kredītiestādēm un ieguldījumu brokeru sabiedrībām, un ar ko groza Regulu (ES) Nr. 648/2012.

- 1.5. Maksājumu pakalpojumu sniedzējiem ir jāizmanto aplēses, ja tiem nav faktisku datu, ar ko pamatot savus slēdzienus, neatkarīgi no tā, vai līdz incidenta atrisināšanai ir sasniegta vai, iespējams, tiks sasniegta konkrēta robežvērtība (piem., tas var notikt sākotnējās izmeklēšanas posmā).
- 1.6. Maksājumu pakalpojumu sniedzējiem pastāvīgi incidenta pastāvēšanas laikā ir jāveic šis novērtējums, lai identificētu iespējamās statusa izmaiņas augšup (no nebūtiska uz būtisku) vai lejup (no būtiska uz nebūtisku). Par jebkuru incidenta pārklasificēšanu no būtiska uz nebūtisku saskaņā ar 2.21. pamatnostādne noteiktajām prasībām un bez nepamatotas kavēšanās ir jāpaziņo kompetentajai iestādei.

2. pamatnostādne. Paziņošanas process

- 2.1. Maksājumu pakalpojumu sniedzējiem ir jāapkopo visa būtiskā informācija, jā sagatavo ziņojums par incidentu, aizpildot pielikumā doto veidni, un tas jāiesniedz savas piederības dalībvalsts kompetentajai iestādei. Maksājumu pakalpojumu sniedzējiem ir jā aizpilda visi veidnes lauki atbilstoši pielikumā dotajiem norādījumiem.
- 2.2. Maksājumu pakalpojumu sniedzējiem ir jāizmanto viena un tā pati veidne viena incidenta sākotnējam, starpposma un nobeiguma ziņojumiem. Tādējādi maksājumu pakalpojumu sniedzējiem ir pakāpeniski jā aizpilda viena veidlapa un vajadzības gadījumā jā aktualizē informācija, kas iesniegta iepriekšējos ziņojumos.
- 2.3. Maksājumu pakalpojumu sniedzējiem savas piederības dalībvalsts kompetentajai iestādei attiecīgajā gadījumā ir jā iesniedz arī tās informācijas eksemplārs, kuru tas sniedza (vai sniegs) saviem lietotājiem, kā paredzēts MPD2 96. panta 1. punkta 2. rindkopā, tiklīdz tā kļūst pieejama.
- 2.4. Maksājumu pakalpojumu sniedzējiem, ja to pieprasa viņu piederības dalībvalsts kompetentā iestāde, jā iesniedz jebkuri papildu dokumenti, kas papildina informāciju, kura iesniegta ar standartizēto veidni. Maksājumu pakalpojumu sniedzējiem ir jā veic papildu pasākumi, atbildot uz savas piederības dalībvalsts kompetentās iestādes jebkādiem pieprasījumiem sniegt papildinformāciju vai skaidrojumu saistībā ar jau iesniegtu dokumentāciju.
- 2.5. Jebkura papildinformācija, kas iekļauta dokumentos, kurus maksājumu pakalpojumu sniedzēji iesniedz kompetentajai iestādei, vai nu pēc paša maksājumu pakalpojumu sniedzēja iniciatīvas vai pēc kompetentās iestādes pieprasījuma saskaņā ar 2.4. pamatnostādni, maksājumu pakalpojumu sniedzējam ir jāatspoguļo veidnē saskaņā ar 2.1. pamatnostādni.

- 2.6. Maksājumu pakalpojumu sniedzējiem vienmēr ir jā saglabā tās informācijas konfidencialitāte un integritāte, ar kuru tie apmainās, kā arī ir pienācīgi jāapstiprina savs autentiskums savas piederības dalībvalsts kompetentajai iestādei.

Sākotnējais ziņojums

- 2.7. Maksājumu pakalpojumu sniedzējiem ir jāiesniedz savas piederības dalībvalsts kompetentajai iestādei sākotnējais ziņojums, kad pirmoreiz ir konstatēts būtisks operacionālais vai drošības incidents. Kompetentajām iestādēm jāapstiprina, ka sākotnējais ziņojums ir saņemts bez nepamatotas kavēšanās, un jāpiešķir tam unikāls atsauces kods, kas nepārprotami identificē incidentu. Maksājumu pakalpojumu sniedzējam šis atsauces kods ir jānorāda, aktualizējot vai nu sākotnējo, vai starpposma un nobeiguma ziņojumu saistībā ar to pašu incidentu, ja vien starpposma un nobeiguma ziņojums netiek iesniegts kopā ar sākotnējo ziņojumu.
- 2.8. Maksājumu pakalpojumu sniedzējiem sākotnējais ziņojums ir jānosūta savas piederības dalībvalsts kompetentajai iestādei četru stundu laikā, pēc tam, kad operacionālais vai drošības incidents ir klasificēts kā būtisks. Ja ir zināms, ka kompetentās iestādes ziņošanas kanāli šajā laikā nav pieejami vai nedarbojas, maksājumu pakalpojumu sniedzējiem sākotnējais ziņojums ir jānosūta tiklīdz kanāli kļūst atkal pieejami/atsāk darboties.
- 2.9. Maksājumu pakalpojumu sniedzējiem incidents saskaņā ar 1.1. un 1.4. pamatnostādni jāklasificē laikus uzreiz pēc incidenta konstatēšanas, bet ne vēlāk, kā 24 stundas pēc incidenta konstatēšanas, un bez nepamatotas kavēšanās pēc tam, kad maksājumu pakalpojuma sniedzējam ir pieejama informācija, kas nepieciešama incidenta klasificēšanai. Ja incidenta klasificēšanai ir nepieciešams vairāk laika, maksājumu pakalpojumu sniedzējiem sākotnējā ziņojumā, kurš iesniegts kompetentajai iestādei, ir jāpaskaidro iemesls.
- 2.10. Maksājumu pakalpojumu sniedzējiem ir jāiesniedz sākotnējais ziņojums savas piederības dalībvalsts kompetentajai iestādei arī tad, ja iepriekš nebūtisks incidents ir ticis pārkvalificēts par būtisku incidentu. Šajā konkrētajā gadījumā maksājumu pakalpojumu sniedzējiem sākotnējais ziņojums ir jānosūta kompetentajai iestādei, tiklīdz ir konstatēta statusa maiņa, vai, ja ir zināms, ka tajā laikā kompetentās iestādes ziņošanas kanāli nav pieejami vai nedarbojas, — tiklīdz tie atkal kļūst pieejami / atsāk darboties.
- 2.11. Maksājumu pakalpojumu sniedzējiem sākotnējā ziņojumā jāsniedz virsraksta līmeņa informācija (t. i., veidnes A sadaļa), norādot dažas incidenta pamatiezīmes un tā paredzamās sekas, pamatojoties uz informāciju, kas ir pieejama nekavējoties pēc tam, kad incidents klasificēts kā būtisks. Ja faktiski dati nav pieejami, maksājumu pakalpojumu sniedzējiem ir jāizmanto aplēses.

Starpposma ziņojums

- 2.12. Maksājumu pakalpojumu sniedzējiem pēdējais starpposma ziņojums ir jāiesniedz tad, kad ir atjaunotas ierastās darbības un darījumdarbība norit normāli, informējot par to kompetento

iestādi. Maksājumu pakalpojumu sniedzējiem ir jāuzskata, ka darījumdarbība atkal norit normāli, ja darbība/funkcijas ir atjaunotas tādā pašā pakalpojumu/nosacījumu līmenī kā to noteicis maksājumu pakalpojumu sniedzējs vai kā noteikts ārējā nolīgumā par pakalpojumu līmeni (apstrādes laiki, darbspēja, drošības prasības utt.), un ja vairs netiek īstenoti ārkārtas pasākumi. Starpposma ziņojumā jāiekļauj sīkāks incidenta un tā seku apraksts (veidnes B sadaļa).

- 2.13. Ja ierastās darbības vēl nav atjaunotas, maksājumu pakalpojumu sniedzējiem ir jāiesniedz kompetentajai iestādei starpposma ziņojums trīs darbdienu laikā pēc sākotnējā ziņojuma iesniegšanas.
- 2.14. Maksājumu pakalpojumu sniedzējiem ir jāaktualizē informācija, kas jau ir iesniegta veidnes A un B sadaļā, kad pēc iepriekšējā ziņojuma ir notikušas būtiskas izmaiņas (piem., vai incidents ir eskalējies vai samazinājies, informācija par jauniem identificētiem cēloņiem vai veiktajām darbībām, lai problēmu novērstu). Tostarp, ja incidents nav novērsts trīs darbdienu laikā, kā dēļ maksājumu pakalpojumu sniedzējiem būtu jāiesniedz papildu starpposma ziņojums. Jebkurā gadījumā maksājumu pakalpojumu sniedzējiem papildu starpposma ziņojums ir jāiesniedz pēc savas piederības dalībvalsts kompetentās iestādes pieprasījuma.
- 2.15. Tāpat kā sākotnējo ziņojumu gadījumā, ja nav pieejami faktiski dati, maksājumu pakalpojumu sniedzējiem ir jāizmanto aplēses.
- 2.16. Ja darījumdarbība atgriežas ierastajā ritmā, pirms ir pagājušas četras stundas kopš incidents ir klasificēts kā būtisks, maksājumu pakalpojumu sniedzējiem ir jācenšas vienlaikus iesniegt gan sākotnējo, gan starpposma ziņojumu (t. i., aizpildot veidnes A un B sadaļu) pirms četru stundu termiņa beigām.

Nobeiguma ziņojums

- 2.17. Maksājumu pakalpojumu sniedzējiem ir jāiesniedz nobeiguma ziņojums, kad ir veikta pirmcēloņa analīze (neatkarīgi no tā, vai seku mazināšanas pasākumi jau ir veikti un vai ir identificēts galīgais pirmcēlonis) un ir pieejami faktiskie dati, lai aizstātu jebkādas potenciālās aplēses.
- 2.18. Maksājumu pakalpojumu sniedzējiem noslēguma ziņojums kompetentajai iestādei ir jāiesniedz ne vēlāk kā 20 darbdienu laikā pēc tam, kad var uzskatīt, ka darījumdarbība ir atgriezies ierastajā gaitā. Maksājumu pakalpojumu sniedzējiem, kuriem ir nepieciešams šā termiņa pagarinājums (piem., kad vēl nav pieejami faktiskie ietekmes rādītāji vai nav vēl apzināti pirmcēloņi), ir jāsaņem ar kompetento iestādi, pirms ir iestājies minētais termiņš, un ir jānorāda pienācīgs kavējuma pamatojums, kā arī jauns paredzamais noslēguma ziņojuma datums.
- 2.19. Ja maksājumu pakalpojumu sniedzēji var iesniegt visu informāciju, kas nepieciešama noslēguma ziņojumā (t. i., veidnes C sadaļā), četrās stundās kopš incidents klasificēts, kā

būtisks, tiem ir jācenšas sākotnējā ziņojumā kopumā iesniegt informāciju, kas saistīta ar sākotnējo, starposma un nobeiguma ziņojumu.

- 2.20. Maksājumu pakalpojumu sniedzējiem nobeiguma ziņojumā ir jāiekļauj pilnīga informācija, t. i., i) faktiskie rādītāji par ietekmi, nevis aplēses (kā arī citi atjauninājumi, kas nepieciešami veidnes A un B sadaļā), un ii) veidnes C sadaļa, kurā norāda pirmcēloni, ja tas ir jau noskaidrots, kā arī kopsavilkumu par pasākumiem, kuri ir jau pieņemti vai kurus ir plānots pieņemt, lai likvidētu problēmu un novērstu tās atkārtosanos turpmāk.
- 2.21. Maksājumu pakalpojumu sniedzējiem ir jānosūta nobeiguma ziņojums arī tad, ja incidenta nepārtrauktas novērtēšanas rezultātā tie konstatē, ka incidents, par kuru jau ir paziņots, vairs neatbilst kritērijiem, pēc kuriem to atzīst par būtisku, un nav sagaidāms, ka tas atbildīs minētajiem kritērijiem, pirms incidents tiks atrisināts. Šajā gadījumā maksājumu pakalpojumu sniedzējiem nobeiguma ziņojums ir jānosūta, tiklīdz šis apstāklis ir konstatēts, bet jebkurā gadījumā — līdz nākamā ziņojuma iesniegšanas galīgajam termiņam. Šajā konkrētajā gadījumā tā vietā, lai aizpildītu veidnes C sadaļu, maksājumu pakalpojumu sniedzējiem ir jāatzīmē lodziņš “incidents pārklasificēts kā nebūtisks” un jāpaskaidro iemesli, kas pamato šādu pārklasificēšanu.

3. pamatnostādne. Deleģētā un konsolidētā paziņošana

- 3.1. Ja kompetentā iestāde to pieļauj, maksājumu pakalpojumu sniedzēji, kas saskaņā ar MPD2 vēlas deleģēt ziņošanas pienākumus trešai personai, informē par to piederības dalībvalsts kompetento iestādi un nodrošina, ka tiek izpildīti šādi nosacījumi:
- a. ar oficiālu līgumu vai attiecīgajā gadījumā esošas grupas iekšējo vienošanos, kas attiecas uz deleģēto ziņošanu, starp maksājumu pakalpojumu sniedzēju un trešo personu nepārprotami ir noteikta visu personu pienākumu sadale. It īpaši tajā skaidri noteikts tas, ka, neraugoties uz ziņošanas pienākuma iespējamo deleģēšanu, ietekmētais maksājumu pakalpojumu sniedzējs ir pilnībā atbildīgs par MPD2 96. pantā noteikto prasību izpildi un par tās informācijas saturu, kas iesniegta piederības dalībvalsts kompetentajai iestādei;
 - b. deleģēšana atbilst prasībām attiecībā uz tādu svarīgu darbības funkciju uzticēšanu ārpalpojumu sniedzējiem, kas noteiktas
 - i. MPD2 19. panta 6. punktā attiecībā uz maksājumu iestādēm un elektroniskās naudas iestādēm un ir piemērojamas mutatis mutandis saskaņā ar Direktīvas 2009/110/EK 3. pantu, vai
 - ii. EBI pamatnostādnēs par ārpalpojumu nolīgumiem (EBA/GL/2019/02) attiecībā uz visiem maksājumu pakalpojumu sniedzējiem;

- c. informāciju piederības dalībvalsts kompetentajai iestādei iesniedz iepriekš un jebkurā gadījumā, ja piemērojams, ievērojot kompetentās iestādes noteiktos termiņus un procedūras;
- d. tiek pienācīgi nodrošināta jutīgu datu konfidencialitāte un kompetentajai iestādei iesniegtās informācijas kvalitāte, konsekvence, integritāte un uzticamība.

3.2. Maksājumu pakalpojumu sniedzējiem, kas vēlas, lai ieceltā trešā persona izpilda ziņošanas pienākumus konsolidētā veidā (t. i., iesniedzot vienu ziņojumu, kas attiecas uz vairākiem maksājumu pakalpojumu sniedzējiem, kurus ietekmējis viens un tas pats būtiskais operacionālais vai drošības incidents), ir jāinformē piederības dalībvalsts kompetentā iestāde, norādot kontaktinformāciju, kas iekļaujama veidnes sadaļā "Ietekmētais MPS", un jāpārliedz, ka ir izpildīti šādi nosacījumi:

- a. šo nosacījumu iekļauj līgumā par deleģēto ziņošanu;
- b. nosaka to, ka konsolidētā ziņošana ir atkarīga no tā, ka incidentu izraisa trešās personas sniegto pakalpojumu pārtraukums;
- c. ierobežo konsolidēto ziņošanu līdz maksājumu pakalpojumu sniedzējiem, kas ir izveidoti vienā un tajā pašā dalībvalstī;
- d. nodrošina visu to maksājumu pakalpojumu sniedzēju sarakstu, kurus ietekmējis incidents;
- e. nodrošina, ka trešā puse novērtē incidenta būtiskumu ikvienam ietekmētajam maksājumu pakalpojumu sniedzējam un konsolidētajā ziņojumā iekļauj tikai tos maksājumu pakalpojumu sniedzējus, kuriem incidents ir klasificēts, kā būtisks; turklāt nodrošina, lai šaubu gadījumā maksājumu pakalpojumu sniedzējs tiktu iekļauts konsolidētajā ziņojumā, kamēr nav pierādījumu, kas apliecinātu pretējo;
- f. nodrošina ka, ja veidnē ir lauki, kuros nav iespējams sniegt kopīgu atbildi (piem., veidnes B2, B4 vai C3 sadaļa), trešā persona vai nu i) aizpilda to individuāli par katru ietekmēto maksājumu pakalpojumu sniedzēju, papildus precizējot katra tā maksājumu pakalpojumu sniedzēja identitāti, uz kuru informācija attiecas, vai ii) lieto kumulatīvas vērtības, kas konstatētas vai aplēstas attiecībā uz maksājumu pakalpojumu sniedzējiem;
- g. trešā persona vienmēr informē maksājumu pakalpojumu sniedzējus par būtisku informāciju attiecībā uz incidentu un par visu saziņu, kas tai var būt ar kompetento iestādi, kā arī par tās saturu, taču tikai tiktāl, cik ir iespējams, nepārkāpjot konfidencialitāti saistībā ar informāciju, kas attiecas uz citiem maksājumu pakalpojumu sniedzējiem.

- 3.3. Maksājumu pakalpojumu sniedzēji ziņošanas pienākumus nedrīkst deleģēt, ja tie iepriekš nav informējuši piederības dalībvalsts kompetento iestādi vai pēc tam, kad ir saņemta informācija, ka vienošanās par ārpalpojumiem neatbilst 3.1. pamatnostādnes b) punktā izvirzītajām prasībām.
- 3.4. Maksājumu pakalpojumu sniedzēji, kas vēlas atsaukt deleģētos ziņošanas pienākumus, par šo lēmumu informē piederības dalībvalsts kompetento iestādi, ievērojot minētās kompetentās iestādes noteiktos termiņus un procedūras. Maksājumu pakalpojumu sniedzējiem ir jāinformē piederības dalībvalsts kompetentā iestāde arī par būtiskām norisēm, kas ietekmē iecelto trešo personu un tās spēju pildīt ziņošanas pienākumus.
- 3.5. Maksājumu pakalpojumu sniedzējiem ir pilnībā jāievēro savi ziņošanas pienākumi bez iespējas vērsties pēc ārējas palīdzības, ja ieceltā trešā persona neinformē piederības dalībvalsts kompetento iestādi par būtisku operacionālo vai drošības incidentu saskaņā ar MPD2 96. pantu un šīm pamatnostādnēm. Maksājumu pakalpojumu sniedzējiem ir arī jānodrošina, ka nerodas situācija, kad par incidentu paziņo divreiz — gan minētais maksājumu pakalpojumu sniedzējs, gan trešā persona.
- 3.6. Maksājumu pakalpojumu sniedzējiem ir jāpārlicinās, ka situācijā, kad incidentu ir izraisījis traucējums tehnisko pakalpojumu sniedzēja nodrošinātajos pakalposumos (vai infrastruktūrā), kas ietekmē vairākus MPS, deleģētā ziņošana attiecas uz maksājumu pakalpojumu sniedzēja individuālajiem datiem (izņemot, ja tiek iesniegts konsolidētais ziņojums).

4. pamatnostādne. Operacionālā un drošības politika

- 4.1. Maksājumu pakalpojumu sniedzējiem ir jānodrošina, ka vispārējā operacionālā un drošības politika skaidri definē visus pienākumus saistībā ar ziņošanu par incidentiem saskaņā ar MPD2, kā arī ieviestos procesus, lai īstenotu šajās pamatnostādnēs definētās prasības.

5. Pamatnostādnes, kuru adresāts ir kompetentās iestādes un kas attiecas uz kritērijiem, kā novērtēt incidenta būtiskumu, un incidentu ziņojuma elementiem, kas jādara zināmi citām valsts iestādēm

5. pamatnostādne. Incidenta būtiskuma novērtējums

5.1. Piederības dalībvalsts kompetentajām iestādēm ir jānovērtē būtisku operacionālo vai drošības incidentu nozīmīgums attiecībā uz citām valsts iestādēm, pamatojoties uz pašu ekspertu slēdzieniem un kā minētā incidenta nozīmīguma primāros rādītājus izmantojot šādus kritērijus:

- a. incidenta cēloņi ietilpst citas valsts iestādes normatīvo uzdevumu lokā (t. i., to kompetences jomā);
- b. incidenta sekām ir ietekme uz citas valsts iestādes mērķiem (piem., finanšu stabilitātes aizsardzību);
- c. incidents ietekmē vai varētu ietekmēt maksājumu pakalpojumu lietotājus plašā mērogā;
- d. incidents ir plaši atspoguļots vai, iespējams, tiks plaši atspoguļots plašsaziņas līdzekļos.

5.2. Piederības dalībvalsts kompetentās iestādes šo novērtējumu veic pastāvīgi incidenta pastāvēšanas laikā, lai identificētu iespējamās pārmaiņas, kas var padarīt par nozīmīgu incidentu, kurš iepriekš netika par tādu uzskatīts.

6. pamatnostādne. Informācija, kas jādara zināma

6.1. Neietekmējot citas normatīvās prasības sniegt ar incidentu saistītu informāciju citām valsts iestādēm, kompetentajām iestādēm informācija par būtiskiem operacionālajiem vai drošības incidentiem ir jādara zināma attiecīgajām valsts iestādēm, kas identificētas, piemērojot 5.1. pamatnostādni, vismaz sākotnējā ziņojuma saņemšanas laikā (vai arī tāda ziņojuma laikā, kas noteicis, ka informācija ir jādara zināma) un tad, kad tām ir paziņots, ka darījumdarbība atkal norit ierastajā gaitā (t. i., pēc starpposma ziņojuma saņemšanas).

6.2. Kompetentajām iestādēm ir jāiesniedz attiecīgajām valsts iestādēm informācija, kas nepieciešama, lai skaidri atspoguļotu notikušo un iespējamās sekas. Lai to paveiktu, tām ir

jāsniedz vismaz informācija, kuru maksājumu pakalpojumu sniedzējs ir sniedzis šādos veidnes laukos (vai nu sākotnējā, vai starpposma ziņojumā):

- datums un laiks, kad incidents klasificēts kā būtisks;
- incidenta konstatēšanas datums un laiks;
- incidenta sākšanās datums un laiks;
- datums un laiks, kad incidents tika novērsts vai kad ir paredzams, ka tas tiks novērsts;
- īss incidenta apraksts (tostarp detalizētā apraksta nekonfidencialās ziņas);
- īss apraksts par veiktajiem vai plānotajiem pasākumiem ar mērķi atgūties no incidenta;
- apraksts par to, kā incidents varētu ietekmēt citus maksājumu pakalpojumu sniedzējus un/vai infrastruktūras;
- atspoguļošanas plašsaziņas līdzekļos (ja tāda bijusi) apraksts;
- incidenta cēlonis.

6.3. Kompetentajām iestādēm pēc vajadzības dati ir jāpadara anonīmi un jāizslēdz tāda informācija, uz kuru varētu attiekties konfidencialitātes vai intelektuālā īpašuma ierobežojumi, pirms jebkāda ar incidentu saistītā informācija tiek nodota attiecīgajām valsts iestādēm. Taču kompetentajām iestādēm ir attiecīgajām valsts iestādēm jā dara zināms ziņojumu iesniegušā maksājumu pakalpojumu sniedzēja nosaukums un adrese, ja minētās valsts iestādes var garantēt, ka tiks saglabāta informācijas konfidencialitāte.

6.4. Kompetentajām iestādēm vienmēr ir jā saglabā tās uzglabātās un kopīgotās informācijas konfidencialitāte un integritāte, kā arī pienācīgi jā autentificējas attiecībā uz attiecīgajām valsts iestādēm. It īpaši kompetentajām iestādēm attiecībā uz visu informāciju, kuru tās saņem saskaņā ar šīm pamatnostādnēm, ir jā piemēro dienesta noslēpuma pienākumi, kas noteikti MPD2, neietekmējot piemērojamos Savienības tiesību aktus un valstu prasības.

6. Pamatnostādnes, kuru adresāts ir kompetentās iestādes un kas attiecas uz kritērijiem, kā novērtēt incidentu ziņojumu atbilstošos elementus, kuri jādara zināmi EBI un ECB, un uz saziņas formātu un procedūrām

7. pamatnostādne. Informācija, kas jādara zināma

- 7.1. Kompetentajām iestādēm vienmēr ir jāiesniedz EBI un ECB visi ziņojumi, ko tās ir saņēmušas no maksājumu pakalpojumu sniedzējiem (vai to vārdā), kurus ir ietekmējis būtisks operacionālais vai drošības incidents, izmantojot standartizēto datni, kas pieejama EBI tīmekļa vietnē.

8. pamatnostādne. Komunikācija

- 8.1. Kompetentajām iestādēm vienmēr ir jā saglabā uzglabātās un kopīgotās informācijas konfidencialitāte un integritāte, kā arī pienācīgi jāautenticējas attiecībā uz EBI un ECB. It īpaši kompetentajām iestādēm attiecībā uz visu informāciju, kuru tās saņem saskaņā ar šīm pamatnostādnēm, ir jāpiemēro dienesta noslēpuma pienākumi, kas noteikti MPD2, neietekmējot piemērojamos Savienības tiesību aktus un valstu prasības.
- 8.2. Lai novērstu kavējumus, nosūtot ar incidentiem saistīto informāciju EBI/ECB, un samazinātu darbības pārtraukuma riskus, kompetentajām iestādēm ir jāatbalsta attiecīgi komunikācijas veidi.

Pielikums. Ziņošanas veidne maksājumu pakalpojumu sniedzējiem

Sākotnējais ziņojums

Sākotnējais ziņojums		četrus stundu laikā pēc tam, kad incidents klasificēts, kā būtisks		Atiestatīt/Noizīlamo izvēlni	
Ziņojuma datums (DD/MM/GGGG)		Laiks (HH/MM)			
Incidenta atsaucējs kods					
A — sākotnējais ziņojums					
A 1 — VISPĀRĒJI DATI					
Pārskata veids					
Ietekmētais maksājumu pakalpojumu sniedzējs (MPS)					
MPS nosaukums					
MSP valsts identifikācijas numurs					
Atbilstīgā gadījumā grupas vadošais uzņēmums					
Incidenta ietekmētā valsts/valstis	<input type="checkbox"/> AT <input type="checkbox"/> DE <input type="checkbox"/> FR <input type="checkbox"/> IE <input type="checkbox"/> LV <input type="checkbox"/> PT	<input type="checkbox"/> BE <input type="checkbox"/> DK <input type="checkbox"/> LU <input type="checkbox"/> IS <input type="checkbox"/> MT <input type="checkbox"/> RO	<input type="checkbox"/> BG <input type="checkbox"/> EE <input type="checkbox"/> GR <input type="checkbox"/> IT <input type="checkbox"/> NL <input type="checkbox"/> SE	<input type="checkbox"/> CY <input type="checkbox"/> ES <input type="checkbox"/> HR <input type="checkbox"/> LT <input type="checkbox"/> NO <input type="checkbox"/> SI	<input type="checkbox"/> CZ <input type="checkbox"/> FI <input type="checkbox"/> HU <input type="checkbox"/> LU <input type="checkbox"/> PL <input type="checkbox"/> SK
Galvenā kontaktpersona		E-pasts		Tālrunis	
Sekundārā kontaktpersona		E-pasts		Tālrunis	
Iestāde, kas ziņo (aizpildiet šo iedaļu tikai tad, ja deleģētās ziņošanas gadījumā iestāde, kas ziņo, nav ietekmētais MPS)					
Ziņošanas vienības nosaukums					
Valsts identifikācijas numurs					
Galvenā kontaktpersona		E-pasts		Tālrunis	
Sekundārā kontaktpersona		E-pasts		Tālrunis	
A 2 — INCIDENTA KONSTATĒŠANA UN KLASIFIKĀCIJA					
Incidenta konstatēšanas datums un laiks (DDMMGGGG HHMM)					
Incidenta klasificēšanas datums un laiks (DDMMYYYY HHMM)					
Incidentu konstatēja	Ja "cits", lūdzu, paskaidrojiet:				
Incidenta veids					
Kritēriji, kuru dēļ tiek ziņots, kā par būtisku incidentu	<input type="checkbox"/> ietekmētie darījumi <input type="checkbox"/> ietekmētie maksājumu pakalpojumu lietotāji <input type="checkbox"/> pakalpojuma diskvāle <input type="checkbox"/> tīkla vai in formācijas sistēmu drošības pārkāpums <input type="checkbox"/> ekonomiskā ietekme <input type="checkbox"/> augsti iekšējais eskalācijas līmenis <input type="checkbox"/> citi potenciāli ietekmētie MPS vai attiecīgās infrastruktūras <input checked="" type="checkbox"/> ietekme uz reputāciju				
Incidenta īss un vispārīgs apraksts					
Ietekme citā ES dalībvalstī, ja ir piemērojams					
Ziņošana citām iestādēm		E-pasts		Tālrunis	
Iemesli, kādēļ sākotnējais ziņojums iesniegts novēloti	Ja "jā", lūdzu, paskaidrojiet:				

Starpposma ziņojums

Ziņojums par būtisku incidentu	
Starpposma ziņojums	ne vairāk kā 3 darbdienu pēc sākotnējā ziņojuma iesniegšanas
Atiestatīt nolaižamo izvēlni	
Ziņojuma datums (DDMMGGGG)	Laiks (HH:MM)
Incidenta atsauces kods	
B — Starpposma ziņojums	
B 1 — VISPĀRĒJI DATI	
Sīkākā incidenta apraksts:	
Kāda ir konkrētā problēma?	
Kā incidents sākās?	
Kā tas attīstījās?	
Kādas ir sekas (it īpaši maksājumu pakalpojumu lietotājiem)?	
Vai maksājumu pakalpojumu lietotājiem ir paziņots par incidentu?	<input type="checkbox"/> Ja "jā", lūdzu, paskaidrojiet:
Vai tas bija saistīts ar iepriekšējo(-iem) incidentu(-iem)?	<input type="checkbox"/> Ja "jā", lūdzu, paskaidrojiet:
Vai tika ietekmēti vai bija iesaistīti citi pakalpojumu sniedzēji/trešās puses?	<input type="checkbox"/> Ja "jā", lūdzu, paskaidrojiet:
Vai tika uzsākta krīzes pārvaldība (iekšējā un/vai ārējā)?	<input type="checkbox"/> Ja "jā", lūdzu, paskaidrojiet:
Incidenta sākuma datums un laiks (ja ir jau identificēts) (DDMMGGGG HH:MM)	
Datums un laiks, kad incidents tika novērsti vai ir paredzams, ka tas tiks novērsti (DDMMGGGG HH:MM)	
Ietekmētās funkcionālās jomas	<input type="checkbox"/> Autentifikācija/autorizācija <input type="checkbox"/> Tiešie norēķini <input type="checkbox"/> Komunikācija <input type="checkbox"/> Netiešie norēķini <input type="checkbox"/> Kārtings <input type="checkbox"/> Cits
Iepriekšējos ziņojumos veiktas izmaiņas	
B 2 — INCIDENTA KLASIFIKĀCIJA UN INFORMĀCIJA PAR INCIDENTU	
Ietekmētie darījumi ⁽²⁾	Ietekmes līmenis Ietekmēto darījumu skaits Kā % no ierastā darījumu skaita Ietekmēto darījumu vērtība EUR Incidenta ilgums (piemērojams tikai operacionālajiem incidentiem) Komentāri:
Ietekmētie maksājumu pakalpojumu lietotāji ⁽³⁾	Ietekmes līmenis Ietekmēto maksājumu pakalpojumu lietotāju skaits Kā % no visiem maksājumu pakalpojumu lietotājiem
Tīkla vai informācijas sistēmu drošības pārkāpums	Aprakstiet, kā tika ietekmēts tīkls vai informācijas sistēmas
Pakalpojuma diskontinuitāte	Kopējais pakalpojuma diskontinuitātes laiks: Dienas: Stundas: Minūtes:
ekonomiskā ietekme	Ietekmes līmenis Tiešās izmaksas, EUR Netiešās izmaksas, EUR
augsts iekšējās eskalācijas līmenis	Aprakstiet incidenta iekšējās eskalācijas līmeni, norādot, vai tā rezultātā ir noteikts vai, iespējams, tiks noteikts krīzes (vai tai pielīdzināms) režīms, un, ja tā, lūdzu, aprakstiet
Citi potenciāli ietekmētie MPS vai attiecīgās infrastruktūras	Aprakstiet, kā šis incidents varētu ietekmēt citus MPS un/vai infrastruktūras
Ietekme uz reputāciju	Aprakstiet, kā incidents varētu ietekmēt MPS reputāciju (piem., informācija plašsaziņas līdzekļos, publikācijas par tiesvedību vai normatīvo aktu pārkāpumiem)
B 3 — INCIDENTA APRAKSTS	
Incidenta veids	<input type="checkbox"/> Tiek izmeklēts
Incidenta cēlonis	<input type="checkbox"/> Launprātīga darbība <input type="checkbox"/> Procesa kļūme <input type="checkbox"/> Sistēmas kļūme <input type="checkbox"/> Cilveka kļūdas <input type="checkbox"/> Ārēji notikumi <input type="checkbox"/> Cits
Vai incidents jūs ietekmēja tieši vai netieši — ar pakalpojumu sniedzēja starpniecību?	Ja netieši, lūdzu, norādiet pakalpojumu sniedzēja nosaukumu:
B 4 — INCIDENTA IETEKME	
Kopējā ietekme	<input type="checkbox"/> Integritāte <input type="checkbox"/> Konfidencialitāte <input type="checkbox"/> Pieejamība <input type="checkbox"/> Autentiskums
Ietekmētie komercanāli	<input type="checkbox"/> Filiales <input type="checkbox"/> Telefonbanka <input type="checkbox"/> Pārdošanas vietas <input type="checkbox"/> Bankas pakalpojumi tiešsaistē <input type="checkbox"/> Mobilā banka <input type="checkbox"/> Cits <input type="checkbox"/> E-komercija <input type="checkbox"/> Bankomāti
Ietekmētie maksājumu pakalpojumi	<input type="checkbox"/> Iekšējais naudas izsūtījumu konts <input type="checkbox"/> Kredīta pārveidumi <input type="checkbox"/> Norēķins <input type="checkbox"/> Skaidras naudas izņemšana no maksājumu konta <input type="checkbox"/> Tiešā debeta maksājumi <input type="checkbox"/> Maksājuma <input type="checkbox"/> Rīcībai ar maksājumu kontu nepieciešamās darbības <input type="checkbox"/> Kredīta pārveidumi <input type="checkbox"/> Konta informācijas pakalpojumi <input type="checkbox"/> Maksājumu instrumentu iegūšana <input type="checkbox"/> Maksājumu instrumentu izdošana
B 5 — INCIDENTA SEKU MAZINĀŠANA	
Kādas darbības/pasākumi līdz šim ir veikti vai ir plānoti, lai atgūtos pēc incidenta?	
Vai ir aktivizēts uzņēmējdarbības nepārtrauktības plāns un/vai negadījuma seku novēršanas plāns?	
Ja tā, kad? ddmmgggg, hh:mm	
Ja tā, lūdzu, aprakstiet	

VEIDNES AIZPILDĪŠANAS NORĀDĪJUMI

Maksājumu pakalpojumu sniedzējiem (MPS) ir jāaizpilda atbilstošās veidnes sadaļas atkarībā no aktuālā ziņošanas posma: A sadaļa — sākotnējam ziņojumam, B sadaļa — starpposma ziņojumiem, bet C sadaļa — nobeiguma ziņojumam. MPS ir jāizmanto viena un tā pati veidne viena incidenta sākotnējam, starpposma un nobeiguma ziņojumam. Visi lauki ir jāaizpilda obligāti, ja vien nav skaidri norādīts citādi.

Virsraksts

Sākotnējais ziņojums ir pirmais paziņojums, ko MPS iesniedz piederības dalībvalsts kompetentajai iestādei.

Starpposma ziņojumā ir iekļauts sīkāks incidenta un tā seku apraksts. Tas ir aktualizēts sākotnējais ziņojums (un, ja ir piemērojams, iepriekšējais starpposma ziņojums) par to pašu incidentu.

Nobeiguma ziņojums ir pēdējais ziņojums, ko MPS sūta par minēto incidentu, jo i) ir veikta pirmcēloņu analīze un aplēses var aizstāt ar faktiskiem datiem vai ii) incidents vairs nav uzskatāms par būtisku un ir jāpārklasificē.

Incidents pārklasificēts par nebūtisku: incidents vairs neatbilst kritērijiem, lai tiktu atzīts par būtisku, un nav paredzams, ka tas atbildīs minētajiem kritērijiem, pirms tas tiks atrisināts. MPS ir jāpaskaidro šīs pārklasificēšanas iemesli.

Ziņojuma datums un laiks: precīzs datums un laiks, kad ziņojums tiek iesniegts kompetentajai iestādei.

Incidenta atsauces kods (izmantojams starpposma un nobeiguma ziņojumos, kā arī sākotnējā ziņojuma atjauninājumiem): atsauces kodu kompetentā iestāde izsniedz sākotnējā ziņojuma sagatavošanas brīdī, lai nepārprotami identificētu incidentu. Katrai kompetentajai iestādei sākumā jāiekļauj attiecīgās dalībvalsts divciparu ISO kods².

A - Sākotnējais ziņojums

A 1 - Vispārēji dati

Ziņojuma veids:

Individuāls: ziņojums attiecas uz vienu MPS.

Konsolidēts: ziņojums attiecas uz vairākiem MPS vienā dalībvalstī, kurus ir skāris viens un tas pats operacionālais vai drošības incidents, kuri izmanto konsolidēto ziņošanu. Lauki "Ietekmētais MPS" jāatstāj neaizpildīti (izņemot lauku "Incidenta ietekmētā(-ās) valsts/valstis"), un ziņojumā ir jāietver MPS saraksts, aizpildot atbilstošo tabulu (Konsolidētais ziņojums — MPS saraksts).

Ietekmētais MPS: attiecas uz MPS, kuram radies incidents.

MPS nosaukums: tā MPS pilns nosaukums, kuram ir jāveic ziņošanas procedūra, kā norādīts atbilstošajā oficiālajā valsts MPS reģistrā.

MPS nacionālais identifikācijas numurs: unikāls nacionālais identifikācijas numurs, kuru piederības dalībvalsts izmanto valsts reģistrā, lai nepārprotami identificētu MPS.

Grupās galvenā vienība: vienību grupas gadījumā, kā ir noteikts MPD2 4. panta 40. punktā, lūdzu, norādiet galvenās vienības nosaukumu.

Incidenta ietekmētā(-ās) valsts/valstis: valsts vai valstis, kurās ir materializējusies incidenta ietekme (piem., ir ietekmētas MPS vairākas filiāles, kuras atrodas dažādās valstīs), neraugoties uz incidenta smagumu citā(-s) valstī/valstīs. Tā var būt vai var nebūt tā pati valsts, kas ir piederības dalībvalsts.

Primārā kontaktpersona: ietekmētā MPS tās personas vārds un uzvārds, kas ir atbildīga par ziņošanu par incidentu, vai, ja ietekmētā MPS uzdevumā ziņošanu veic trešais pakalpojuma

² Lūdzu skatīt alfa 2 valstu kodus saskaņā ar ISO-3166 <https://www.iso.org/iso-3166-country-codes.html>

sniedzējs, tad ietekmētā MPS par incidenta pārvaldību/riska nodaļu vai tamlīdzīgu jomu atbildīgās personas vārds un uzvārds.

E-pasts: e-pasta adrese, uz kuru pēc vajadzības var nosūtīt pieprasījumus sniegt papildu skaidrojumus. Tā var būt vai nu personiskā, vai uzņēmuma e-pasta adrese.

Tālrunis: tālruņa numurs, uz kuru pēc vajadzības būtu jāzvana, lai pieprasītu sniegt papildu skaidrojumus. Tas var būt vai nu personiskais, vai uzņēmuma tālruņa numurs.

Sekundārā kontaktpersona: tādas citas personas vārds un uzvārds, ar kuru kompetentā iestāde var sazināties, lai uzzinātu par incidentu, ja primārā kontaktpersona nav sasniedzama. Gadījumā, ja ietekmētā MPS uzdevumā ziņojumu iesniedz cits pakalpojuma sniedzējs, tādas citas personas vārds un uzvārds ietekmētajā MPS, kas pārstāv incidenta pārvaldības/riska nodaļu vai tamlīdzīgu jomu.

E-pasts: citas kontaktpersonas e-pasta adrese, uz kuru pēc vajadzības var nosūtīt pieprasījumus sniegt papildu skaidrojumus. Tā var būt vai nu personiskā, vai uzņēmuma e-pasta adrese.

Tālrunis: citas kontaktpersonas tālruņa numurs, uz kuru zvanīt, lai pēc vajadzības pieprasītu sniegt papildu skaidrojumus. Tas var būt vai nu personiskais, vai uzņēmuma tālruņa numurs.

Ziņošanas iestāde: šo sadaļu aizpilda gadījumā, ja ietekmētā MPS uzdevumā ziņošanas pienākumus pilda trešā persona, ja ir piemērojams.

Ziņošanas iestādes nosaukums: tās iestādes pilns nosaukums, kas ziņo par incidentu, kā norādīts atbilstošajā oficiālajā valsts komercgrāmatā.

Valsts identifikācijas numurs: unikāls valsts identifikācijas numurs, kuru valsts, kurā atrodas trešā persona, izmanto, lai nepārprotami identificētu iestādi, kura ziņo par incidentu. Ja ziņojošā trešā persona ir MPS, valsts identifikācijas numuram ir jābūt MPS unikālajam identifikācijas numuram, kuru piederības dalībvalsts kompetentā iestāde izmanto valsts reģistrā.

Primārā kontaktpersona: tās personas vārds un uzvārds, kas ir atbildīga par ziņošanu par incidentu.

E-pasts: e-pasta adrese, uz kuru pēc vajadzības var nosūtīt pieprasījumus sniegt papildu skaidrojumus. Tā var būt vai nu personiskā, vai uzņēmuma e-pasta adrese.

Tālrunis: tālruņa numurs, uz kuru pēc vajadzības būtu jāzvana, lai pieprasītu sniegt papildu skaidrojumus. Tas var būt vai nu personiskais, vai uzņēmuma tālruņa numurs.

Sekundārā kontaktpersona: tādas citas personas vārds un uzvārds iestādē, kas ziņo par incidentu, ar kuru kompetentā iestāde var sazināties, ja primārā kontaktpersona nav sasniedzama.

E-pasts: citas kontaktpersonas e-pasta adrese, uz kuru pēc vajadzības var nosūtīt pieprasījumus sniegt papildu skaidrojumus. Tā var būt vai nu personiskā, vai uzņēmuma e-pasta adrese.

Tālrunis: citas kontaktpersonas tālruņa numurs, uz kuru zvanīt, lai pēc vajadzības pieprasītu sniegt papildu skaidrojumus. Tas var būt vai nu personiskais, vai uzņēmuma tālruņa numurs.

A 2 - Incidenta konstatēšana un klasificēšana

Incidenta konstatēšanas datums un laiks: datums un laiks, kad incidents pirmoreiz tika konstatēts.

Incidenta klasificēšanas datums un laiks: datums un laiks, kad drošības vai operacionālais incidents tika klasificēts, kā būtisks.

Incidentu konstatēja: jānorāda, vai incidentu konstatēja maksājumu pakalpojumu lietotājs, tas konstatēts MPS ietvaros (piem., veicot iekšējās revīzijas funkciju) vai kāda cita ārēja persona (piem., pakalpojumu sniedzējs). Ja tas nebija neviens no uzskaitītajiem, lūdzu, atbilstošajā laukā sniedziet paskaidrojumu.

Incidenta veids: norādiet, vai pēc jūsu ieskatiem un, ja ir pieejama informācija, tas ir operacionālais vai drošības incidents.

Operacionālais: incidents, kas izriet no neatbilstošiem vai kļūdainiem procesiem, cilvēku un sistēmu kļūdām vai nepārvaramas varas apstākļiem, kuri ietekmē ar maksājumiem saistītu apstākļu integritāti, pieejamību, konfidencialitāti un/vai autentiskumu.

Drošības: neatļauta piekļuve MPS aktīviem, neatļauta to izmantošana, izpaušana, pārtraukšana, modificēšana vai iznīcināšana, kā rezultātā var būt ietekmēta ar maksājumiem saistītu pakalpojumu integritāte, pieejamība, konfidencialitāte un/vai autentiskums. Cita starpā tas var notikt, ja MPS piedzīvo tīkla vai informācijas sistēmu drošības pārkāpumu.

Kritēriji, kuru dēļ tiek ziņots par būtisku incidentu: lūdzu, norādiet, kuru kritēriju dēļ tiek ziņots par būtisku incidentu. Var izvēlēties vairākus kritērijus: ietekmēti darījumi, ietekmēti maksājumu pakalpojumu lietotāji, pakalpojuma dīkstāve, tīkla vai informācijas sistēmu drošības pārkāpums, ekonomiskā ietekme, augsts iekšējās eskalācijas līmenis, varētu tikt ietekmēti citi MPS vai attiecīgās infrastruktūras un/vai ietekmēta reputācija.

Īss, vispārīgs incidenta apraksts: lūdzu, īsi aprakstiet būtiskākās incidenta problēmas, norādot iespējamās cēloņus, tūlītējo ietekmi utt.

Ietekme citās ES dalībvalstīs, ja ir piemērojams: lūdzu, īsumā skaidrojiet ietekmi, kāda incidentam ir citā ES dalībvalstī (piem., kā tas ietekmē maksājumu pakalpojumu lietotājus, MPS un/vai maksājumu infrastruktūras). Ja ir iespējams piemērojamajos ziņošanas termiņos, lūdzu, nodrošiniet tulkojumu angļu valodā.

Ziņošana citām iestādēm: lūdzu, norādiet, vai par incidentu ir/tiks ziņots citām iestādēm atsevišķos ziņošanas par incidentu ietvaros, ja ziņošanas laikā tas ir zināms. Ja tā ir, lūdzu norādiet attiecīgās iestādes.

Sākotnējā ziņojuma novēlotas iesniegšanas iemesli: lūdzu, skaidrojiet iemeslus, kādēļ jums bija nepieciešams vairāk par 24 stundām, lai klasificētu incidentu.

B Starposma ziņojums

B 1 – Vispārēji dati

Sīkākais incidenta apraksts: lūdzu, aprakstiet incidenta galvenās pazīmes, ietverot vismaz informāciju par konkrēto problēmu un ar to saistīto pamatinformāciju, aprakstu, kā incidents ir sācies un, kā attīstījies, tā sekas, it īpaši maksājumu pakalpojumu lietotājiem utt. Lūdzu, sniedziet arī informāciju par saziņu ar maksājumu pakalpojumu lietotājiem, ja ir attiecināms.

Vai tas bija saistīts ar iepriekšēju(-iem) incidentu(-iem)? Lūdzu, norādiet, vai šis incidents ir saistīts ar iepriekšējiem incidentiem, ja tāda informācija ir pieejama. Ja incidents ir saistīts ar iepriekšējiem incidentiem, lūdzu, norādiet, ar kuriem.

Vai citi pakalpojumu sniedzēji/trešās personas tika ietekmētas vai bija iesaistītas? Lūdzu norādiet, vai incidents ietekmēja vai tajā bija iesaistīti citi pakalpojumu sniedzēji/trešās personas, ja informācija ir pieejama. Ja incidents ietekmēja citus pakalpojumu sniedzējus/trešās personas, vai tie bija tajā iesaistīti, lūdzu norādiet to sarakstu un sniedziet vairāk informācijas.

Vai tika uzsākta krīzes pārvaldība (iekšējā un/vai ārējā)? Lūdzu norādiet, vai tika uzsākta krīzes pārvaldība (iekšējā un/vai ārējā). Ja krīzes pārvaldība tika uzsākta, lūdzu, sniedziet vairāk informācijas.

Incidentā sākuma datums un laiks: datums un laiks, kad incidents sākās, ja zināms.

Datums un laiks, kad incidents tika novērsts vai kad ir paredzams, ka tas tiks novērsts: norādiet datumu un laiku, kad incidents tika novērsts vai kad ir paredzams, ka tas tiks kontrolēts, un kad darījumdarbība atkal noritēja vai kad ir paredzēts, ka tā noritēs kā ierasts.

Ietekmētās funkcionālās jomas: norādiet maksājumu procesa soli vai soļus, kurus incidents ietekmēja, piemēram, autentifikāciju/autorizāciju, saziņu, klīringu, tiešos norēķinus, netiešos norēķinus un citus.

Autentifikācija/autorizācija: procedūras, kas ļauj MPS pārbaudīt maksājumu pakalpojumu lietotāja identitāti vai konkrēta maksājumu instrumenta lietošanas derīgumu, tostarp lietotāja personalizēto drošības datu lietošanu un maksājumu pakalpojumu sniedzēja (vai trešās personas, kas rīkojas šā lietotāja vārdā) piekrišanu pārskaitīt līdzekļus.

Saziņa: informācijas plūsma identificēšanas, autentifikācijas, paziņošanas un informēšanas nolūkā starp MPS, kas apkalpo kontu, un maksājuma sākšanas pakalpojumu sniedzējiem, konta informācijas pakalpojumu sniedzējiem, maksātājiem, saņēmējiem un citiem MPS.

Klīrings: pārskaitījumu rīkojumu pārskaitīšanas, salīdzināšanas un — atsevišķos gadījumos — apstiprināšanas process pirms norēķiniem, potenciāli ietverot rīkojumu ieskaitu un norēķina gala posteņu noteikšanu.

Tiešais norēķins: darījuma vai apstrādes pabeigšana ar mērķi dzēst dalībnieku saistības, pārskaitot līdzekļus, kad šo darbību veic pats ietekmētais MPS.

Netiešais norēķins: darījuma vai apstrādes pabeigšana ar mērķi dzēst dalībnieku pienākumus, pārskaitot līdzekļus, kad šo darbību veic cits MPS ietekmētā MPS vārdā.

Cits: ietekmētā funkcionālā joma, kas nav neviena no iepriekš uzskaitītajām. Papildu dati jānorāda brīvajā teksta laukā.

Iepriekšējos ziņojumos veiktās izmaiņas: lūdzu norādīt izmaiņas, kas veiktas iepriekšējos ziņojumos par to pašu incidentu sniegtajā informācijā (piem., sākotnējā vai, ja ir attiecināms, starpposma ziņojumā).

B 2 – Incidenta klasifikācija / Informācija par incidentu

Ietekmētie darījumi: MPS ir jānorāda, kuras robežvērtības, ja tādas ir, incidents sasniedz vai, iespējams, sasniegs, kā arī saistītie rādītāji — ietekmēto darījumu skaits, ietekmētie darījumi procentuāli no kopējā to maksājumu darījumu skaita, kas veikti, izmantojot tos pašus maksājumu pakalpojumus, kurus incidents ir ietekmējis, kā arī kopējā darījumu vērtība. MPS ir jāsniedz konkrētas šo mainīgo vērtības, kas var būt gan faktiskie skaitļi, gan aplēses. Parasti MPS jēdziens “ietekmētie darījumi” ir jāizprot kā visi pašmāju un pārrobežu darījumi, kurus incidents ir tieši vai netieši ietekmējis vai, iespējams, ietekmēs, jo īpaši tie darījumi, kurus nav bijis iespējams uzsākt vai apstrādāt, kuriem tika izmainīts maksājuma ziņojuma saturs un kuri tika pasūtīti krāpnieciski (neatkarīgi no tā, vai līdzekļi ir atgūti vai nav). Turklāt MPS jēdziens “maksājumu darījumu ierastais līmenis” ir jāizprot kā to ikdienas pašmāju un pārrobežu maksājumu darījumu vidējais skaits gadā, kurus veic, izmantojot tos pašus maksājumu pakalpojumus, kurus ietekmēja incidents, par atsaucē periodu aprēķiniem ņemot iepriekšējo gadu. Ja MPS neuzskata, ka šis rādītājs ir reprezentatīvs (piem., sezonālības dēļ), viņiem tā vietā ir jāizmanto cits, reprezentatīvāks rādītājs un laukā “Komentāri” ir jāsniedz kompetentajai iestādei šādas pieejas pamatojums. Gadījumos, kad incidents ietekmē maksājumu darījumus valūtā, kas nav euro, aprēķinot robežvērtības un ziņojot par ietekmēto darījumu vērtību, MPS darījumu, kuri nav euro, summa ir jākonvertē euro, izmantojot ECB dienas atsaucē valūtas kursu dienā, kad tiek veikta ziņojuma par incidentu iesniegšana.

Ietekmētie maksājumu pakalpojumu lietotāji: MPS ir jānorāda robežvērtības, ja tādas ir, kuras incidentā ir sasniegtas vai, iespējams, tiks sasniegtas, kā arī saistītie rādītāji — kopējais ietekmēto maksājumu pakalpojumu lietotāju skaits un ietekmēto maksājumu pakalpojumu lietotāju skaits procentuāli no kopējā maksājumu pakalpojumu lietotāju skaita. MPS ir jāsniedz konkrētas šo mainīgo vērtības, kas var būt gan faktiskie skaitļi, gan aplēses. MPS ir jāizprot jēdziens “ietekmētie maksājumu pakalpojumu lietotāji” kā visi klienti (pašmāju un ārzemju, patērētāji un uzņēmumi), kuriem ar ietekmēto MPS ir noslēgts līgums, kas tiem piešķir piekļuvi ietekmētajam maksājumu pakalpojumam, un kuri ir cietuši vai, iespējams, cietīs no incidenta sekām. MPS aplēses ir jābalsta uz iepriekšējām norisēm, lai noteiktu to maksājumu pakalpojumu lietotāju skaitu, kuri, iespējams, incidenta pastāvēšanas laikā ir izmantojuši minēto maksājumu pakalpojumu. Grupu gadījumā katram MPS ir jāņem vērā tikai paša maksājumu pakalpojumu lietotāji. Ja MPS piedāvā darbības pakalpojumus citiem, šim MPS ir jāņem vērā tikai savi maksājumu pakalpojumu lietotāji (ja tādi ir) un tiem MPS, kuri saņem šos darbības pakalpojumus, ir jānovērtē incidents saistībā ar saviem maksājumu pakalpojumu lietotājiem. Turklāt MPS kā kopējais maksājumu pakalpojumu lietotāju skaits ir jāpieņem to pašmāju un pārrobežu maksājumu pakalpojumu lietotāju kopskaits, ar kuriem incidenta laikā ir bijušas noslēgtas līgumattiecības (vai arī visnesenākais pieejamais rādītājs) un kuriem ir pieeja ietekmētajam maksājumu pakalpojumam neatkarīgi no to lieluma un no tā, vai tie ir uzskatāmi par aktīviem vai pasīviem maksājumu pakalpojumu lietotājiem.

Tīkla vai informācijas sistēmu drošības pārkāpums: MPS ir jānosaka, vai kāda ļaunprātīgā darbība ir ietekmējusi ar maksājumu pakalpojumu nodrošināšanu saistītā tīkla vai informācijas sistēmu pieejamību, autentiskumu, integritāti vai konfidencialitāti.

Pakalpojuma dīkstāve: MPS ir jānorāda, vai incidentā ir sasniegta vai, iespējams, tiks sasniegta robežvērtība, kā arī saistītais rādītājs — kopējais pakalpojuma dīkstāve. MPS ir jāsniedz konkrētas šā mainīgā vērtības, kas var būt gan faktiskie skaitļi, gan aplēses. MPS ir jāņem vērā laikposms, kurā jebkurš uzdevums, process vai kanāls, kas ir saistīts ar maksājumu pakalpojumu sniegšanu, nav vai, iespējams, nebūs pieejams, tādējādi liedzot i) uzsākt un/vai veikt maksājumu pakalpojumu un/vai ii) piekļūt maksājumu kontam. MPS pakalpojuma dīkstāve ir jāaprēķina no brīža, kad dīkstāve sākas, un viņiem ir jāņem vērā gan laikposmi, kuros tie ir atvērti darījumdarbībai, kas nepieciešama maksājumu pakalpojumu izpildei, gan arī laikposmi ārpus darba laika un uzturēšanas laikposmi, ja tas ir atbilstoši un piemērojami. Ja maksājumu pakalpojumu sniedzēji nevar noteikt, kad pakalpojuma dīkstāve ir sācies, viņiem izņēmuma kārtā pakalpojuma dīkstāve ir jāaprēķina no brīža, kad tas tika konstatēts.

Ekonomiskā ietekme: MPS ir jānorāda, vai incidentā ir sasniegta vai, iespējams, tiks sasniegta robežvērtība, kā arī saistītie rādītāji — tiešās izmaksas un netiešās izmaksas. MPS ir jāsniedz konkrētas šo mainīgo vērtības, kas var būt gan faktiskie skaitļi, gan aplēses. MPS ir jāņem vērā izmaksas, kas var būt gan tieši, gan netieši saistītas ar incidentu. Cita starpā MPS ir jāņem vērā ekspropriētie līdzekļi vai aktīvi, aparatūras vai programmatūras aizstāšanas izmaksas, citas tiesu vai atlīdzināšanas izmaksas, maksas, kas piemērotas līgumsaistību neizpildes dēļ, sankcijas, ārējas saistības un zaudētie ieņēmumi. Attiecībā uz netiešajām izmaksām MPS ir jāņem vērā tikai tās izmaksas, kas jau ir zināmas vai, ļoti iespējams, radīsies. Gadījumos, kad izmaksas ir valūtā, kas nav euro, aprēķinot robežvērtību un ziņojot par ekonomiskās ietekmes vērtību, MPS izmaksu, kuras nav euro, summa ir jākonvertē euro, izmantojot ECB dienas atsauces valūtas kursu dienā, kad tiek veikta ziņojuma par incidentu iesniegšana.

Tiešās izmaksas: incidenta tieši radītās izmaksas (EUR), tostarp līdzekļi, kas nepieciešami incidenta novēršanai (piem., ekspropriēti līdzekļi vai aktīvi, aparatūras un programmatūras nomaiņas izmaksas, izdevumi attiecībā uz līgumsaistību neizpildi).

Netiešās izmaksas: incidenta netieši radītās izmaksas (EUR) (piem., atlīdzības/kompensācijas klientiem izmaksas, iespējamie tiesvedības izdevumi).

Augsts iekšējās eskalācijas līmenis: MPS ir jāapsver, vai incidents ietekmē ar maksājumiem saistītus pakalpojumus tā, ka tā rezultātā ir vai, iespējams, tiks informēta pārvaldības iestāde, kā ir noteikts pamatnostādņēs par IKT un drošības risku pārvaldību, saskaņā ar EBI IKT un drošības risku pārvaldības pamatnostādņu 60. pamatnostādnes d) punktu par incidentu ārpus jebkuras periodiskas paziņošanas procedūras un pastāvīgi incidenta pastāvēšanas laikā. Tāpat maksājumu pakalpojumu sniedzējiem ir jāapsver, vai incidents ietekmē ar maksājumiem saistītus pakalpojumus tā, ka tā rezultātā ir noteikts vai, iespējams, tiks noteikts krīzes režīms.

Citi potenciāli ietekmētie MPS vai attiecīgās infrastruktūras: MPS ir jānovērtē incidenta ietekme uz finanšu tirgu, ar ko saprot finanšu tirgus infrastruktūras un/vai karšu maksājumu shēmas, kuras atbalsta tos un citus MPS. It īpaši MPS ir jānovērtē, vai incidents, iespējams, tiks replicēts citiem MPS neatkarīgi no tā, vai tas ir ietekmējis vai, iespējams, ietekmēs finanšu tirgus infrastruktūru nevainojamu funkcionēšanu un vai tas ir negatīvi ietekmējis vai, iespējams, negatīvi ietekmēs finanšu sistēmas stabilitu darbību kopumā. MPS ir jāņem vērā dažādas dimensijas, piemēram, vai ietekmētais komponents/programmatūra ir patentēti vai vispārpieejami, vai negatīvi ietekmētais tīkls ir iekšējs vai ārējs un vai MPS ir pārtraucis vai, iespējams, pārtrauks pildīt savus pienākumus tajās finanšu tirgus infrastruktūrās, kurās tas ir dalībnieks.

Ietekme uz reputāciju: MPS ir jāņem vērā atpazīstamības līmenis, kuru (pēc to rīcībā esošās informācijas) incidents ir panācis vai, iespējams, panāks tirgū. It īpaši MPS ir jāņem vērā varbūtība, ka incidents izraisīs kaitējumu sabiedrībai kā piemērots rādītājs tā potenciālam ietekmēt viņu reputāciju. MPS ir jāņem vērā, vai: i) maksājumu pakalpojumi lietotāji un/vai citi MPS ir sūdzējušies par incidenta negatīvajām sekām, ii) incidents ir ietekmējis redzamu ar maksājumu pakalpojumu saistītu procesu un

tādēļ tas ir ticis vai varētu tikt atspoguļots plašsaziņas līdzekļos (ņemot vērā ne tikai tradicionālos plašsaziņas līdzekļus, piemēram, avīzes, bet arī blogus, sociālos tīklus utt.; taču atspoguļošana plašsaziņas līdzekļos šajā kontekstā nenozīmē tikai dažus negatīvus sekotāju komentārus, ir jābūt derīgam ziņojumam vai ievērojamam skaitam negatīvu komentāru/brīdinājumu), iii) netiek vai, iespējams, netiks īstenotas saskaņā ar līgumiem noteiktās saistības, kuru rezultātā pret maksājumu pakalpojumu sniedzēju tiek uzsākta tiesvedība, iv) nav ievērotas normatīvās prasības, kā rezultātā tiek noteikti uzraudzības pasākumi vai sankcijas, kas ir vai, iespējams, būs publiski pieejamas, un v) līdzīgs incidents ir noticis jau iepriekš.

B 3 – Incidenta apraksts

Incidenta veids: operacionālais vai drošības. Papildu skaidrojums ir sniegts sākotnējā ziņojuma attiecīgajā laukā.

Incidenta cēlonis: norādiet incidenta cēloni un, ja tas vēl nav zināms, visticamāko cēloni. Var izvēlēties vairākas atbildes.

Notiek izmeklēšana: lūdzu, atzīmējiet lodziņu, ja cēlonis vēl nav zināms.

Ļaunprātīga darbība: ar nodomu uz MPS mērķētas darbības. Tas ietver ļaunprātīgu kodu, informācijas vākšanu, ielaušanās, izplatīšanas/pakalpojuma atteikumu (I/PA), apzinātas iekšējās darbības, apzinātus ārējos fiziskos bojājumus, informācijas satura drošību, krāpnieciskas darbības un citas. Sīkāku informāciju, lūdzu, skatīt šīs veidnes C2 sadaļā.

Procesa kļūme: incidenta cēlonis ir neatbilstoša maksājuma procesa izstrāde vai izpilde, procesa kontroles un/vai atbalsta procesi (piem., maiņas/migrēšanas, pārbaudes, konfigurēšanas, veikspējas, novērošanas process).

Sistēmas kļūme: incidenta cēlonis ir saistīts ar to sistēmu, tīklu, infrastruktūru un datubāzu nepiemērotu izstrādi, izpildi, komponentiem, specifikācijām, integrāciju vai komplikētību, kas atbalsta maksājuma darbību.

Cilvēka kļūda: incidentu izraisījusi cilvēka netīša kļūda, kas ir vai nu maksājumu procesa daļa (piem., augšupielādē nepareizo maksājumu pakešdatni maksājumu sistēmā), vai ir ar to kādā veidā saistīta (piem., nejauši ir atslēgta elektropadeve un maksājuma darbība ir apturēta).

Ārēji notikumi: cēlonis ir saistīts ar notikumiem, kas galvenokārt ir ārpus organizācijas tiešas kontroles (piem., dabas katastrofas, tehnisko pakalpojumu sniedzēja kļūme).

Cits: incidenta cēlonis, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Vai incidents jūs ietekmēja tieši vai netieši — ar pakalpojumu sniedzēja starpniecību? Lūdzu, norādiet, vai incidenta mērķis bija tieši MPS, vai to skāra netieši ar trešās personas starpniecību, ja šāda informācija ir pieejama. Netiešas ietekmes gadījumā, lūdzu, norādiet pakalpojumu sniedzēja(-u) nosaukumu.

B 4 – Incidenta ietekme

Kopējā ietekme: lūdzu norādiet, kurus aspektus ietekmēja operacionālais vai drošības incidents. Var izvēlēties vairākas atbildes.

Integritāte: īpašība, kas nozīmē, ka tiek garantēta aktīvu (arī datu) precizitāte un pilnīgums.

Pieejamība: ar maksājumiem saistītu pakalpojumu īpašība, kas nozīmē, ka tie ir pilnībā pieejami un maksājuma pakalpojuma lietotāji tos var lietot iepriekš noteiktā pieņemamā līmenī.

Konfidencialitāte: īpašība, kas nozīmē, ka informācija nav pieejama vai nav izpaužama personām, organizācijām vai procesiem, kuriem nav atbilstoša pilnvarojuma.

Autentiskums: īpašība, kas nozīmē, ka izcelsme atbilst apgalvotajam.

Ietekmētie komercanāli: norādiet kanālu vai kanālus, pa kuriem mijiedarbojas ar maksājumu pakalpojumu lietotājiem, kurus ir ietekmējis incidents. Var atzīmēt vairākus lodziņus.

Filiāles: darījumdarbības vieta (kas nav galvenais birojs), kas ir MPS daļa bez juridiskas personas statusa un kas nepastarpināti veic dažus vai vairākus darījumus, kuri veido MPS darījumdarbības neatņemamu sastāvdaļu. Visas darījumdarbības vietas, ko vienā dalībvalstī ir izveidojis MPS, kura mītne atrodas citā dalībvalstī, uzskata par vienu filiāli.

Bankas pakalpojumi tiešsaistē: datoru izmantošana, lai tiešsaistē veiktu finanšu darījumus.

Telefonbanka: tālruņa izmantošana, lai veiktu finanšu darījumus.

Mobilā banka: īpašas bankas pakalpojumu lietotnes izmantošana viedtālrunī vai tamlīdzīgā ierīcē, lai veiktu finanšu darījumus.

Bankomāts: elektromehāniska ierīce, kas ļauj maksājumu pakalpojumu lietotājiem izņemt skaidru naudu no saviem kontiem un/vai piekļūt citiem pakalpojumiem.

Pārdošanas punkts: komersanta fiziska telpa, kurā tiek sākti maksājuma darījumi.

E-komercija: maksājumu darījumi tiek sākti virtuālā pārdošanas punktā (piem., maksājumiem, kuri uzsākti internetā, izmantojot kredīta pārvedumus, maksājumu kartes, elektroniskas naudas pārvedumus starp e-naudas kontiem).

Cits: ietekmētais komercijas kanāls, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Ietekmētie maksājumu pakalpojumi: norādiet tos maksājumu pakalpojumus, kuri incidenta rezultātā nedarbojas atbilstoši. Var atzīmēt vairākus lodziņus.

Naudas ieskaitīšana maksājumu kontā: skaidras naudas nodošana MPS, lai to ieskaitītu maksājumu kontā.

Naudas izņemšana no maksājumu konta: pieprasījums, ko MPS saņem no sava maksājumu pakalpojumu lietotāja, izsniegt skaidru naudu un debitēt tā maksājumu kontu par atbilstošu summu.

Rīcībai ar maksājumu kontu nepieciešamās darbības: darbības, kas jāveic maksājumu kontā, lai aktivizētu, deaktivizētu un/vai uzturētu to (piem., atvēršana, bloķēšana).

Maksājumu instrumentu iegūšana: maksājumu pakalpojums, kas ietver MPS vienošanos ar naudas saņēmēju par maksājumu darījumu akceptēšanu un apstrādāšanu, kā rezultātā naudas saņēmējam tiek pārskaitīti naudas līdzekļi.

Kredīta pārvedumi: maksājumu pakalpojums naudas saņēmēja maksājumu konta kredītēšanai, izmantojot maksājumu darījumu vai vairākus maksājuma darījumus no maksātāja maksājumu konta, ko atbilstoši maksātāja sniegtajām norādēm veic MPS, kurš ir maksātāja maksājumu konta turētājs.

Tiešie debeti: maksājumu pakalpojums maksātāja maksājumu konta debetēšanai, kurā maksājuma darījumu uzsāk maksājuma saņēmējs atbilstoši maksātāja piekrišanai, ko tas sniedzis saņēmējam, saņēmēja MPS vai paša MPS sniedzējam.

Karšu maksājumi: maksājumu pakalpojums, kas ir balstīts uz maksājumu kartes shēmas infrastruktūras un darījumdarbības noteikumiem, lai veiktu maksājuma darījumu, izmantojot jebkādu karšu, telekomunikāciju, digitālu vai IT ierīci vai programmatūru, ja tā rezultātā tiek veikts debetkartes vai kredītkartes darījums. Uz kartēm balstīti maksājumu darījumi neietver darījumus, kas balstīti uz cita veida maksājumu pakalpojumiem.

Maksājumu instrumentu izdošana: maksājumu pakalpojums, kas ietver MPS vienošanos ar maksātāju nodrošināt tam maksājumu instrumentu, ar kuru uzsākt un apstrādāt maksātāja maksājumu darījumus.

Naudas pārvedums: maksājumu pakalpojums, ar ko līdzekļus saņem no maksātāja, neizveidojot maksājuma kontus uz maksātāja vai saņēmēja vārda, un kura vienīgais mērķis ir pārskaitīt atbilstošu summu saņēmējam vai citam MPS, kas rīkojas saņēmēja vārdā, un/vai ar kuru šādus līdzekļus saņem saņēmēja vārdā un padara tos saņēmējam pieejamus.

Maksājuma sākšanas pakalpojumi: maksājumu pakalpojums, ar ko uzsāk maksājuma rīkojumu pēc maksājumu pakalpojuma lietotāja pieprasījuma attiecībā uz maksājumu kontu, kura turētājs ir cits MPS.

Konta informācijas pakalpojumi: tiešsaistes maksājumu pakalpojumi, ar ko sniedz konsolidētu informāciju par vienu vai vairākiem maksājumu kontiem, kuru turētājs ir maksājumu pakalpojumu lietotājs vai nu citā MPS, vai vairākos MPS.

B 5 – Incidenta seku mazināšana

Kādas darbības/pasākumi līdz šim ir veikti vai ir plānoti, lai atgūtos pēc incidenta? Lūdzu, norādiet sīkāku informāciju par darbībām, kuras ir veiktas vai ir plānots veikt, lai uz laiku risinātu incidenta radītās sekas.

Vai ir aktivizēts darījumdarbības nepārtrauktības plāns un/vai negadījuma seku novēršanas plāns? Lūdzu, norādiet, vai tā ir, un, ja ir, tad sniedziet visbūtiskākās ziņas par to, kas notika (t. i., kad tie tika aktivizēti un kas tajos bija iekļauts).

C – Nobeiguma ziņojums

C 1 – Vispārēji dati

Sākotnējā ziņojuma un starpposma ziņojuma(-u) informācijas aktualizācija (kopsavilkums): lūdzu sniedziet papildu informāciju par incidentu, ieskaitot konkrētas izmaiņas, kas veiktas informācijā, kura iesniegta starpposma ziņojumā. Lūdzu norādiet arī jebkuru citu saistīto informāciju.

Vai joprojām tiek veiktas visas sākotnējās kontroles? lūdzu norādiet, vai MPS kādā brīdī incidenta laikā ir nācies atcelt vai pavājināt kādas kontroles. Ja tā ir, lūdzu, norādiet, vai visas kontroles ir atjaunotas, brīvajā teksta laukā paskaidrojiet, kuras kontroles ir atjaunotas un kāds ir papildu periods, kas nepieciešams to atjaunošanai.

C 2 – Pirmcēloņu analīze un vēlākie pasākumi

Kāds bija incidenta pirmcēlonis, ja ir jau zināms? Lūdzu, norādiet kas ir incidenta pirmcēlonis vai, ja tas vēl nav zināms, visticamāko pirmcēloni. Var izvēlēties vairākas atbildes. (Lūdzu, ņemiet vērā, ka pirmcēlonim jāatšķiras no incidenta ietekmes.)

Ļaunprātīga darbība: ārējas vai iekšējas ar nodomu uz MPS mērķētas darbības. Tās ir sadalītas šādās kategorijās:

Ļaunprātīgs kods: piem., vīruss, tārps, Trojas zirgs, spieģprogrammatūra.

Informācijas vākšana: piem., skenēšana, okškerēšana, sociālā inženierija.

Ielaušanās: piem., kompromitēts privilēģēts konts, kompromitēts neprivilēģēts konts, kompromitēta lietotne, robotprogrammatūra.

Izplatīšanas/pakalpojuma atteikuma uzbrukums (I/PA): mēģinājums padarīt tiešsaistes pakalpojumu nepieejamu, pārslogojot to ar datplūsmu no vairākiem avotiem.

Apzinātas iekšējās darbības: piem., sabotāža, zādzība.

Apzināti ārējie fiziskie bojājumi: piem., sabotāža, fizisks uzbrukums telpām/datu centriem.

Informācijas satura drošība: neatļauta piekļuve informācijai, neatļauta informācijas grozīšana.

Krāpnieciskas darbības: neatļauta resursu izmantošana, autortiesību pārkāpums, maskēšanās, pikškerēšana.

Cits (lūdzu, precizējiet): incidenta cēlonis, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Procesa kļūme: incidenta cēlonis ir neatbilstoša maksājuma procesa izstrāde vai izpilde, procesa kontroles un/vai atbalsta procesi (piem., maiņas/migrēšanas, pārbaudes, konfigurēšanas, veikspējas, novērošanas process). Tās ir sadalītas šādās kategorijās:

Trūkt novērošanas un kontroles: piem., saistībā ar notiekošajām operācijām, sertifikātu termiņu beigām, licenču termiņu beigām, ielāpu termiņu beigām, definētajām maksimālajām skaitītāju vērtībām, datubāzu aizpildījuma līmeņiem, lietotāju tiesību pārvaldību, dubultās kontroles principu.

Komunikācijas problēmas: piem., starp tirgus dalībniekiem vai organizācijas iekšienē.

Nepareiza ekspluatācija: piem., nav nomainīti sertifikāti, pilna kešatmiņa.

Nepiemērota pārmaiņu pārvaldība: piem., neidentificētas konfigurācijas kļūdas, ieviešana, ieskaitot atjauninājumus, uzturēšanas problēmas, negaidītas kļūdas.

Iekšējo procedūru un dokumentācijas neatbilstība: piem., trūkst pārredzamības saistībā ar funkcionalitāti, procesiem un kļūdu rašanos, dokumentācijas neesamība.

Problēmas saistībā ar atgūšanos: piem., neparedzētu izdevumu pārvaldība, neatbilstīga štatu samazināšana.

Cits (lūdzu, precizējiet): incidenta cēlonis, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Sistēmas kļūme: incidenta cēlonis ir saistīts ar to sistēmu, tīklu, infrastruktūru un datubāzu nepiemērotu izstrādi, izpildi, komponentiem, specifiskajām, integrāciju vai komplikētību, kas atbalsta maksājuma darbību. Tās ir sadalītas šādās kategorijās:

Aparatūras kļūme: fiziskā tehnoloģiju aprīkojuma, kurš tiek izmantots procesu organizēšanai un/vai datu, kuri MPS nepieciešami ar maksājumiem saistītai darbībai, uzglabāšanai, kļūme (piem., cieto disku, datu centru, citas infrastruktūras kļūme).

Tīkla kļūme: publisku vai privātu telekomunikāciju tīklu, kuri maksājuma procesā ļauj veikt datu un informācijas apmaiņu (piem., internetā), kļūme.

Datubāzes problēmas: datu struktūra, kas uzglabā personisku un maksājumu informāciju, kura nepieciešama, lai izpildītu maksājumu darbības.

Programmatūras/lietotnes kļūme: programmu, operētājsistēmu utt., kas nodrošina MPS maksājumu pakalpojumu sniegšanu, kļūmes (piem., nepareiza darbība, nezināma darbība).

Fiziski bojājumi: piem., nejaušs bojājums, ko radījuši neatbilstoši apstākļi, būvdarbi.

Cits (lūdzu, precizējiet): incidenta cēlonis, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Cilvēka kļūda: incidentu izraisījusi cilvēka netīša kļūda, kas ir vai nu maksājumu procesa daļa (piem., augšupielādē nepareizo maksājumu pakešdatni maksājumu sistēmā), vai ir ar to kādā veidā saistīta (piem., nejauši ir atslēgta elektropadeve un maksājuma darbība ir apturēta). Tās ir sadalītas šādās kategorijās:

Nejauša: piem., kļūdas, izlaidumi, pieredzes un zināšanu trūkums.

Bezdarbība: piem., ja trūkst prasmi, zināšanu, pieredzes, saprašanas.

Nepietiekami resursi: piem., trūkst cilvēku resursu, darbinieki nav pieejami.

Cits (lūdzu, precizējiet): incidenta cēlonis, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Ārējs notikums: cēlonis ir saistīts ar notikumiem, kuri parasti ir ārpus organizācijas kontroles. Tie ir sadalīti šādās kategorijās:

Piegādātāja/tehniskā pakalpojuma sniedzēja kļūme: piem., strāvas padeves pārtraukums, interneta pārrāvums, juridiskas problēmas, uzņēmējdarbības problēmas, atkarība no pakalpojumiem.

Nepārvarama vara: piem., strāvas pārrāvums, ugunsgrēks, dabas radīti cēloņi, tādi kā zemestrīces, plūdi, spēcīgi nokrišņi, spēcīgi vēji.

Cits (lūdzu, precizējiet): incidenta cēlonis, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Cits: incidenta cēlonis, kas nav neviens no iepriekš uzskaitītajiem. Papildu dati jānorāda brīvajā teksta laukā.

Cita būtiska informācija par pirmcēloni: lūdzu, sniedziet jebkuru papildu informāciju par pirmcēloni, ieskaitot sākotnējos secinājumus, kas radušies, veicot pirmcēloņa analīzi.

Galvenā veiktā vai plānotā korigējošā rīcība/pasākumi, lai novērstu incidenta atkārtošanos, ja jau ir zināmi: lūdzu, aprakstiet galveno veikto vai plānoto rīcību, lai novērstu incidenta turpmāku atkārtošanos.

C 3 – Papildu informācija

Vai informācija par incidentu ir darīta zināma citiem MPS informācijas nolūkos? lūdzu, sniedziet pārskatu par MPS, ar kuriem ir veikta oficiāla vai neoficiāla saziņa, lai informētu par incidentu, norādot to MPS, kuri ir informēti, datus, informāciju, kas tika darīta zināma, kā arī iemeslus šādas informācijas kopīgošanai.

Vai pret MPS ir vērstas tiesiskas darbības? Lūdzu, norādiet, vai noslēguma ziņojuma aizpildīšanas laikā MPS incidenta rezultātā ir cietis no tiesiskām darbībām (piem., ir iesniegta prasība tiesā vai ir zaudēta licence).

Īstenotās rīcības efektivitātes novērtējums: ja ir pieejams, lūdzu iekļaujiet pašvērtējumu par incidenta laikā īstenotās rīcības efektivitāti, ieskaitot mācības, kas gūtas no incidenta.