EBA/GL/2017/10

19/12/2017

Ghid

privind raportarea incidentelor majore în temeiul Directivei (UE) 2015/2366 (DSP 2)

1. Conformitate și obligații de raportare

Statutul prezentului ghid

1. Prezentul document conține orientări emise în temeiul articolului 16 din Regulamentul (UE) nr. 1093/2010[1]. În conformitate cu articolul 16 alineatul (3) din Regulamentul (UE) nr. 1093/2010, autoritățile competente și instituțiile financiare trebuie să depună toate eforturile necesare pentru a respecta orientările.

2. Ghidul prezintă punctul de vedere al ABE privind practicile adecvate în materie de supraveghere în cadrul Sistemului european al supraveghetorilor financiari sau privind modul în care ar trebui aplicat dreptul Uniunii într-un anumit domeniu. Autoritățile competente cărora li se aplică ghidul, astfel cum sunt definite la articolul 4 alineatul (2) din Regulamentul (UE) nr. 1093/2010, trebuie să se conformeze și să îl integreze în practicile lor, după caz (de exemplu, prin modificarea cadrului legislativ sau a procedurilor de supraveghere ale acestora), inclusiv în cazurile în care anumite puncte din cuprinsul documentului sunt adresate în primul rând instituțiilor.

Cerințe de raportare

3. În conformitate cu articolul 16 alineatul (3) din Regulamentul (UE) nr. 1093/2010, autoritățile competente trebuie să notifice ABE dacă se conformează sau intenționează să se conformeze prezentului ghid sau, în caz contrar, motivele neconformării, până la 19/02/2018. În absența unei notificări până la acest termen, ABE va considera că autoritățile competente nu s-au conformat. Notificările se trimit prin intermediul formularului disponibil pe site-ul ABE la adresa compliance@eba.europa.eu , cu mențiunea „EBA/GL/2017/10”. Notificările trebuie trimise de persoane care au autoritatea de a raporta cu privire la respectarea ghidului în numele autorităților competente. Orice schimbare cu privire la starea de conformare trebuie adusă, de asemenea, la cunoștința ABE.

4. Notificările vor fi publicate pe site-ul ABE, în conformitate cu articolul 16 alineatul (3).

[1] Regulamentul (UE) nr. 1093/2010 al Parlamentului European și al Consiliului din 24 noiembrie 2010 de instituire a Autorității europene de supraveghere (Autoritatea bancară europeană), de modificare a Deciziei nr. 716/2009/CE și de abrogare a Deciziei 2009/78/CE a Comisiei (JO L 331, 15.12.2010, p.12).

2. Obiect, domeniu de aplicare și definiții

Obiect

5. Prezentul ghid a fost elaborat ca urmare a mandatului acordat ABE în temeiul articolului 96 alineatul (3) din Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010, și de abrogare a Directivei 2007/64/CE (DSP 2).

6. În mod specific, prezentul ghid enunță criteriile pentru clasificarea incidentelor operaționale sau de securitate majore de către prestatorii de servicii de plată, precum și formatul și procedurile pe care aceștia trebuie să le urmeze pentru a comunica astfel de incidente, astfel cum este prevăzut la articolul 96 alineatul (1) din directiva menționată anterior, autorității competente din statul membru de origine.

7. În plus, prezentul ghid tratează modul în care aceste autorități competente trebuie să evalueze relevanța incidentului și detaliile din rapoartele referitoare la incident pe care, în conformitate cu articolul 96 alineatul (2) din directiva menționată anterior, acestea le vor comunica altor autorități naționale.

8. În plus, prezentul ghid tratează, de asemenea, problema comunicării către ABE și BCE a detaliilor relevante ale incidentelor raportate în scopul promovării unei abordări comune și consecvente.

Domeniu de aplicare

9. Prezentul ghid se aplică în legătură cu clasificarea și raportarea incidentelor operaționale sau de securitate majore în conformitate cu articolul 96 din Directiva (UE) 2015/2366.

10. Prezentul ghid se aplică în cazul tuturor incidentelor încadrate în definiția „incidentului operațional sau de securitate major”, care cuprinde atât evenimente externe, cât și interne care ar putea fi rău intenționate sau accidentale.

11. Prezentul ghid se aplică, de asemenea, în cazul în care incidentul operațional sau de securitate major se produce în afara Uniunii (de exemplu, atunci când se produce un incident în societatea-mamă sau într-o filială înființată în afara Uniunii) și afectează serviciile de plată prestate de către un prestator de servicii de plată aflat în Uniune în mod direct (un serviciu aferent plăților este prestat de către societatea afectată din afara Uniunii) sau în mod indirect (capacitatea prestatorului de servicii de plată de a-și desfășura în continuare activitatea de plată este pusă în pericol într-un alt mod ca urmare a incidentului).

Destinatari

12. Primul set de orientări (secțiunea 4) se adresează prestatorilor de servicii de plată definiți la articolul 4 alineatul (11) din Directiva (UE) 2015/2366 și menționați la articolul 4 alineatul (1) din Regulamentul (UE) 1093/2010.

13. Al doilea și al treilea set de orientări (secțiunile 5 și 6) se adresează autorităților competente definite la articolul 4 alineatul (2) litera (i) din Regulamentul (UE) nr. 1093/2010.

Definiții

14. Cu excepția cazului în care se prevede altfel, termenii utilizați și definiți în Directiva (UE) 2015/2366 au același înțeles în cuprinsul ghidului. În plus, în sensul prezentului ghid, se aplică următoarele definiții:

Incident operațional sau de securitate	Un eveniment unic sau o serie de evenimente corelate neprevăzute de către prestatorul serviciului de plată, care are/au sau va/vor avea probabil un impact negativ asupra integrității, disponibilității, confidențialității, autenticității și/sau continuității serviciilor aferente plăților.
Integritate	Proprietatea de a asigura precizia și caracterul complet al activelor (inclusiv al datelor).
Disponibilitate	Proprietatea serviciilor aferente plăților de a fi accesibile și utilizabile de către utilizatorii serviciilor de plată.
Confidențialitatea	Proprietatea de a nu pune la dispoziție sau de a nu prezenta informații persoanelor, entităților sau proceselor neautorizate.
Autenticitate	Proprietatea unei surse de a fi ceea ce se pretinde a fi.
Continuitate	Proprietatea proceselor, sarcinilor și activelor unei organizații, care sunt necesare pentru prestarea serviciilor aferente plăților, de a fi pe deplin accesibile și de a se desfășura, respectiv de a funcționa, la niveluri prestabilite acceptabile.
Servicii aferente plăților	Orice activitate economică în sensul articolului 4 alineatul (3) din DSP 2 și toate sarcinile tehnice de asistență necesare pentru prestarea corectă a serviciilor de plată.

3. Punere în aplicare

Data punerii în aplicare

15. Prezentul ghid se aplică începând cu 13 ianuarie 2018.

4. Orientări adresate prestatorilor de servicii de plată referitor la notificarea autorității competente din statul membru de origine al acestora cu privire la incidente operaționale sau de securitate majore

Orientarea 1: Clasificarea incidentelor majore

1.1. Prestatorii de servicii de plată trebuie să clasifice drept incidente majore acele incidente operaționale sau de securitate care îndeplinesc

a. unul sau mai multe criterii din categoria „Nivel de impact ridicat” sau

b. trei sau mai multe criterii din categoria „Nivel de impact scăzut”,

astfel cum sunt prevăzute în Orientarea 1.4, și în urma evaluării prevăzute în prezentul ghid.

1.2. Prestatorii de servicii de plată trebuie să evalueze un incident operațional sau de securitate pe baza următoarelor criterii și a indicatorilor aferenți:

i. Operațiuni afectate

Prestatorii serviciilor de plată trebuie să stabilească valoarea totală a operațiunilor afectate, precum și numărul plăților compromise ca procent din nivelul obișnuit al operațiunilor de plată executate cu serviciile de plată afectate.

ii. Utilizatori ai serviciilor de plată afectați

Prestatorii de servicii de plată trebuie să stabilească numărul utilizatorilor serviciilor de plată afectați în termeni absoluți și ca procent din numărul total al utilizatorilor serviciilor de plată.

iii. Timpul de indisponibilitate a serviciului

Prestatorii de servicii de plată trebuie să stabilească perioada de timp în care serviciul va fi probabil indisponibil pentru utilizatorul serviciilor de plată sau în care ordinul de plată, în sensul articolului 4 alineatul (13) din DSP 2, nu poate fi executat de către prestatorul de servicii de plată.

iv. Impactul economic

Prestatorii de servicii de plată trebuie să stabilească la nivel global costurile financiare asociate incidentului și să ia în calcul atât valoarea absolută, cât și, dacă este cazul, importanța relativă a acestor costuri în raport cu dimensiunea prestatorului de servicii de plată (mai exact, cu fondurile proprii de nivelul 1 ale prestatorului de servicii de plată).

v. Nivelul ridicat de escaladare internă

Prestatorii serviciilor de plată trebuie să stabilească dacă acest incident a fost sau va fi probabil raportat directorilor lor.

vi. Alți prestatori de servicii de plată sau infrastructuri relevante care ar putea fi afectate

Prestatorii de servicii de plată trebuie să stabilească implicațiile sistemice pe care le va avea probabil incidentul, mai exact potențialul acestuia de a se propaga asupra altor prestatori de servicii de plată, infrastructuri ale pieței financiare și/sau scheme de plată cu cardul.

vii. Impactul asupra reputației

Prestatorii de servicii de plată trebuie să stabilească modul în care incidentul poate submina încrederea utilizatorilor în prestatorul de servicii de plată însuși și, la modul mai general, în serviciul aferent sau piața în ansamblu.

1.3. Prestatorii de servicii de plată trebuie să calculeze valoarea indicatorilor conform următoarei metodologii:

i. Operațiuni afectate

Ca și regulă generală, prestatorii de servicii de plată trebuie să înțeleagă ca fiind „operațiuni afectate" toate operațiunile interne și transfrontaliere care au fost sau vor fi probabil afectate în mod direct sau indirect de incident și, în mod specific, acele operațiuni care nu au putut fi inițiate sau procesate, cele al căror conținut al mesajului de plată a fost modificat și cele care au fost dispuse în mod fraudulos (indiferent dacă fondurile au fost recuperate sau nu).

Mai mult, prestatorii de servicii de plată trebuie să înțeleagă faptul că nivelul obișnuit al operațiunilor de plată este media anuală zilnică a operațiunilor interne și transfrontaliere executate cu aceleași servicii de plată care au fost afectate de incident, anul anterior fiind perioada de referință pentru calcule. Dacă prestatorii de servicii de plată nu consideră că această cifră este reprezentativă (de exemplu, din cauza caracterului sezonier), aceștia trebuie să utilizeze, în schimb, un alt indicator mai reprezentativ și să prezinte autorității naționale justificarea aferentă pentru această abordare în câmpul corespunzător al modelului (a se vedea anexa 1).

ii. Utilizatori ai serviciilor de plată afectați

Prestatorii de servicii de plată trebuie să înțeleagă ca fiind „utilizatori ai serviciilor de plată afectate" toți clienții (de la nivel intern sau din străinătate, consumatori sau întreprinderi) care au un contract cu prestatorul serviciului de plată afectat, care le acordă acestora accesul la serviciul de plată afectat, și care au suportat sau vor suporta probabil

consecințele incidentului. Prestatorii de servicii de plată trebuie să recurgă la estimări bazate pe activitatea anterioară pentru a stabili numărul utilizatorilor serviciilor de plată care este posibil să fi folosit serviciul de plată pe durata incidentului.

În cazul grupurilor, fiecare prestator de servicii de plată trebuie să aibă în vedere doar utilizatorii serviciilor de plată proprii. În cazul unui prestator de servicii de plată care oferă servicii operaționale altor persoane, acesta trebuie să aibă în vedere doar utilizatorii de servicii de plată proprii (dacă există), iar prestatorii de servicii de plată care beneficiază de respectivele servicii operaționale trebuie să evalueze incidentul în legătură cu utilizatorii serviciilor de plată proprii.

Mai mult, prestatorii de servicii de plată trebuie să considere numărul total al utilizatorilor serviciilor de plată ca fiind valoarea agregată a utilizatorilor serviciilor de plată interni și transfrontalieri cu care au raporturi contractuale la momentul incidentului (sau, alternativ, cea mai recentă valoare disponibilă) și care au acces la serviciul de plată afectat, indiferent de dimensiunea acestora sau dacă aceștia sunt considerați utilizatori activi sau pasivi ai serviciilor de plată.

iii. Timpul de indisponibilitate a serviciului

Prestatorii de servicii de plată trebuie să aibă în vedere perioada de timp în care orice sarcină, proces sau canal asociat prestării serviciilor de plată este sau va fi probabil indisponibil și, astfel, împiedică (i) inițierea și/sau executarea unui serviciu de plată și/sau (ii) accesul la un cont de plăți. Prestatorii de servicii de plată trebuie să calculeze timpul de indisponibilitate a serviciului de la momentul inițial al indisponibilității și trebuie să ia în considerare atât intervalele de timp în care ei funcționează în măsura necesară executării serviciilor de plată, cât și orele în care nu funcționează, precum și perioadele de întreținere, dacă este cazul și dacă există. Dacă prestatorii de servicii de plată nu pot să stabilească momentul inițial al indisponibilității serviciului, ei trebuie să calculeze în mod excepțional timpul de indisponibilitate a serviciului de la momentul în care s-a depistat indisponibilitatea.

iv. Impactul economic

Prestatorii de servicii de plată trebuie să aibă în vedere atât costurile care pot fi legate în mod direct de incident, cât și cele care sunt legate în mod indirect de incident. Printre altele, prestatorii de servicii de plată trebuie să țină cont de fondurile sau activele expropriate, costurile de înlocuire a echipamentelor hardware sau software, alte costuri realizate în scopuri judiciare sau costuri de remediere, taxe aplicate ca urmare a neconformității cu obligațiile contractuale, sancțiuni, datorii externe și venituri pierdute. În ceea ce privește costurile indirecte, prestatorii de servicii de plată trebuie să le aibă în vedere doar pe cele care sunt deja cunoscute sau foarte probabil de a se concretiza.

v. *Nivelul ridicat de escaladare internă*

Prestatorii de servicii de plată trebuie să aibă în vedere dacă, în urma impactului incidentului asupra serviciilor aferente plăților, responsabilul pentru sistemele informatice (sau o persoană cu o funcție similară) a fost sau va fi probabil informat cu privire la incident

în afara oricărei proceduri de notificare periodice și în permanență pe durata existenței incidentului. În plus, prestatorii de servicii de plată trebuie să aibă în vedere dacă, în urma impactului incidentului asupra serviciilor aferente plăților, a fost sau este susceptibilă de a fi declanșată o stare de criză.

vi. *Alți prestatori de servicii de plată sau infrastructuri relevante care ar putea fi afectate*

Prestatorii de servicii de plată trebuie să evalueze impactul incidentului asupra pieței financiare, care este înțeleasă ca fiind infrastructurile pieței financiare și/sau schemele de plată cu cardul care îi susțin pe ei și pe alți prestatori de servicii de plată. În mod specific, prestatorii de servicii de plată trebuie să evalueze dacă incidentul a apărut sau va apărea probabil în mod similar la alți prestatori de servicii de plată, dacă acesta a afectat sau va afecta probabil funcționarea fără probleme a infrastructurilor pieței financiare și dacă a compromis sau va compromite probabil funcționarea corectă a sistemului financiar în ansamblu. Prestatorii de servicii de plată trebuie să aibă în vedere diferite aspecte, precum dacă o componentă/un echipament software afectată/afectat este supusă/supus unor drepturi de proprietate sau este disponibilă/disponibil în general, dacă rețeaua compromisă este internă sau externă și dacă prestatorul de servicii de plată a încetat sau va înceta probabil să își îndeplinească obligațiile în infrastructurile pieței financiare al cărei membru este acesta.

vii. *Impactul asupra reputației*

Prestatorii de servicii de plată trebuie să aibă în vedere nivelul de vizibilitate pe care, după cunoștința lor, incidentul l-a atins sau îl va atinge probabil pe piață. În mod specific, prestatorii de servicii de plată trebuie să considere probabilitatea ca incidentul să provoace daune societății ca fiind un indicator bun al potențialului acestuia de a afecta reputația lor. Prestatorii de servicii de plată trebuie să țină cont dacă (i) incidentul a afectat un proces vizibil și, prin urmare, este susceptibil de a dobândi sau a dobândit deja acoperire mediatică (având în vedere nu doar mass-media tradițională, precum ziarele, ci și blog-uri, rețele de socializare etc.), (ii) au fost sau vor fi probabil omise obligațiile de reglementare, (iii) au fost sau vor fi probabil încălcate sancțiuni sau (iv) a apărut același tip de incident în trecut.

1.4. Prestatorii de servicii de plată trebuie să evalueze un incident prin a stabili, pentru fiecare criteriu în parte, dacă pragurile relevante din tabelul 1 sunt sau vor fi probabil atinse înainte de soluționarea incidentului.

Tabelul 1: Praguri

Criterii	Nivel de impact redus	Nivel de impact ridicat
Operațiuni afectate	> 10 % din nivelul obișnuit al operațiunilor prestatorului de servicii de plată (sub aspectul numărului de operațiuni) **și** > 100 000 EUR	> 25 % din nivelul obișnuit al operațiunilor prestatorului de servicii de plată (sub aspectul numărului de operațiuni) **sau** > 5 milioane EUR
Utilizatori ai serviciilor de plată afectați	> 5 000 **și** > 10 % dintre utilizatorii serviciilor de plată ai prestatorului de servicii de plată	> 50 000 **sau** > 25% dintre utilizatorii serviciilor de plată ai prestatorului de servicii de plată
Timpul de indisponibilitate a serviciului	> 2 ore	Nu este cazul
Impactul economic	Nu este cazul	> Max. (0,1 % fonduri proprii de nivelul 1,* 200 000 EUR) **sau** > 5 milioane EUR
Nivelul ridicat de escaladare internă	Da	Da, și este probabil să se impună o stare de criză (sau o stare echivalentă)
Alți prestatori de servicii de plată sau infrastructuri relevante care ar putea fi afectate	Da	Nu este cazul
Impactul asupra reputației	Da	Nu este cazul

*Fondurile proprii de nivelul 1, astfel cum sunt definite la articolul 25 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și societățile de investiții și de modificare a Regulamentului (UE) nr. 648/2012.

1.5. Prestatorii de servicii de plată trebuie să recurgă la estimări dacă nu dețin date efective pentru a-și susține aprecierile cu privire la faptul dacă un prag dat este sau va fi probabil atins înainte ca incidentul să fie soluționat (de exemplu, aceasta s-ar putea întâmpla în etapa inițială de investigare).

1.6. Prestatorii de servicii de plată trebuie să efectueze această analiză în permanență pe durata existenței incidentului pentru a identifica orice posibilă schimbare de stare, în sus (de la un incident minor la unul major) sau în jos (de la un incident major la unul minor).

Orientarea 2: Procesul de notificare

2.1. Prestatorii de servicii de plată trebuie să colecteze toate informațiile relevante, să elaboreze un raport referitor la incident cu ajutorul modelului prezentat în anexa 1 și să îl prezinte autorității competente din statul membru de origine. Prestatorii de servicii de plată trebuie să completeze modelul urmând instrucțiunile prezentate în anexa 1.

2.2. Prestatorii de servicii de plată trebuie să utilizeze același model pentru a informa autoritatea competentă pe durata existenței incidentului (mai exact, pentru elaborarea rapoartelor intermediare și finale, astfel cum este descris la punctele 2.7-2.21). Prestatorii de servicii de plată trebuie să completeze modelul progresiv, depunând toate eforturile, pe măsură ce sunt puse la dispoziție mai multe informații în cursul investigațiilor lor interne.

2.3. Prestatorii de servicii de plată trebuie să prezinte, de asemenea, autorității competente din statul lor membru de origine, dacă este cazul, o copie a informațiilor furnizate (sau care vor fi furnizate) utilizatorilor lor, astfel cum este prevăzut la articolul 96 alineatul (1) al doilea paragraf din DSP 2, de îndată ce acestea sunt disponibile.

2.4. Prestatorii de servicii de plată trebuie să pună la dispoziția autorității competente din statul membru de origine, dacă există și dacă se consideră că acest lucru este relevant pentru autoritatea competentă, orice informații suplimentare prin anexarea oricăror documente suplimentare la modelul standardizat ca anexă unică sau anexe diverse.

2.5. Prestatorii de servicii de plată trebuie să îndeplinească orice solicitări de furnizare de informații suplimentare sau clarificări din partea autorității competente din statul membru de origine cu privire la documentația care a fost deja transmisă.

2.6. Prestatorii de servicii de plată trebuie să păstreze în permanență confidențialitatea și integritatea informațiilor schimbate cu autoritatea competentă din statul lor membru de origine și, de asemenea, să se legitimeze în mod corespunzător în fața autorității competente din statul lor membru de origine.

Raportul inițial

2.7. Prestatorii de servicii de plată trebuie să prezinte un raport inițial autorității competente din statul membru de origine atunci când este depistat pentru prima dată un incident operațional sau de securitate major.

2.8. Prestatorii de servicii de plată trebuie să trimită raportul inițial autorității competente în decurs de 4 ore de la momentul depistării pentru prima dată a incidentului operațional sau de securitate major sau, în cazul în care se cunoaște că la momentul respectiv canalele de raportare ale autorității de raportare nu sunt disponibile sau operaționale, de îndată ce acestea devin din nou disponibile/operaționale.

2.9. Prestatorii de servicii de plată trebuie să prezinte, de asemenea, un raport inițial autorității competente din statul membru de origine atunci când un incident cunoscut anterior ca fiind minor devine unul major. În acest caz specific, prestatorii de servicii de plată trebuie să trimită raportul inițial autorității competente de îndată ce se identifică o schimbare de stare sau, în cazul în care se cunoaște că la momentul respectiv canalele de raportare ale autorității competente nu sunt disponibile sau operaționale, de îndată ce acestea devin disponibile/operaționale din nou.

2.10. Prestatorii de servicii de plată trebuie să includă informațiile principale (mai exact, secțiunea A din model) în rapoartele lor inițiale, prezentând astfel unele caracteristici de bază ale incidentului și consecințele prevăzute ale acestuia pe baza informațiilor disponibile imediat după depistarea sau reclasificarea acestuia. Prestatorii de servicii de plată trebuie să recurgă la estimări atunci când nu sunt disponibile date efective. Prestatorii de servicii de plată trebuie să includă, de asemenea, în raportul lor inițial data următoarei actualizări, care ar trebui să aibă loc în cel mai scurt timp posibil și să nu depășească, în niciun caz, 3 zile lucrătoare.

Raportul intermediar

2.11. Prestatorii de servicii de plată trebuie să prezinte rapoarte intermediare de fiecare dată când consideră că există o actualizare relevantă a stării și, ca cerințe minime, până la data următoarei actualizări indicată în raportul anterior (raportul inițial sau raportul intermediar anterior).

2.12. Prestatorii de servicii de plată trebuie să prezinte autorității competente un prim raport intermediar cu o descriere mai detaliată a incidentului și a consecințelor acestuia (secțiunea B din model). Mai mult, prestatorii de servicii de plată trebuie să elaboreze rapoarte intermediare suplimentare prin actualizarea informațiilor furnizate deja în secțiunile A și B din model cel puțin atunci când au cunoștință despre informații relevante noi sau schimbări semnificative de la data notificării anterioare (de exemplu, dacă incidentul a crescut sau a scăzut în intensitate, sunt identificate cauze noi sau sunt luate măsuri pentru rezolvarea problemei). În orice caz, prestatorii de servicii de plată trebuie să elaboreze un raport intermediar la solicitarea autorității competente din statul membru de origine.

2.13. La fel ca și în cazul rapoartelor inițiale, atunci când datele efective nu sunt disponibile, prestatorii de servicii de plată trebuie să recurgă la estimări.

2.14. Mai mult decât atât, prestatorii de servicii de plată trebuie să precizeze în fiecare raport data următoarei actualizări, care ar trebui să aibă loc în cel mai scurt timp posibil și să nu depășească, în niciun caz, 3 zile lucrătoare. În cazul în care prestatorul de servicii de plată nu poate să respecte data estimată a următoarei actualizări, acesta trebuie să contacteze autoritatea competentă pentru a explica motivele întârzierii, să propună un nou termen de prezentare plauzibil (care să nu depășească 3 zile lucrătoare) și să trimită un nou raport intermediar exclusiv cu actualizarea informațiilor privind data estimată a următoarei actualizări.

2.15. Prestatorii de servicii de plată trebuie să trimită ultimul raport intermediar atunci când au fost reluate activitățile obișnuite și activitatea economică a revenit la normal, informând autoritatea competentă cu privire la această situație. Prestatorii de servicii de plată trebuie să considere că activitatea economică a revenit la normal atunci când activitatea/operațiunile este/sunt reluată/reluate la același nivel de executare/în aceleași condiții prevăzut/prevăzute de prestatorul de servicii de plată sau prevăzut/prevăzute la

nivel extern într-un acord privind nivelul serviciilor în ceea ce privește timpii de prelucrare, capacitatea, cerințele de securitate etc. și când nu se mai aplică măsurile de urgență.

2.16. În cazul în care activitatea economică a revenit la normal în decurs de cel mult 4 ore de la momentul depistării incidentului, prestatorii de servicii de plată trebuie să aibă în vedere prezentarea în mod simultan a raportului inițial și a ultimului raport intermediar (mai exact, completarea secțiunilor A și B din model) înainte de termenul de 4 ore.

Raportul final

2.17. Prestatorii de servicii de plată trebuie să trimită un raport final atunci când a fost efectuată analiza cauzelor fundamentale (indiferent dacă au fost deja implementate măsurile de atenuare a incidentului sau dacă a fost identificată cauza fundamentală finală) și când există cifre efective disponibile pentru a înlocui orice estimări.

2.18. Prestatorii de servicii de plată trebuie să transmită raportul final autorității competente în decurs de maxim 2 săptămâni de la data la care se consideră că activitatea a revenit la normal. Prestatorii de servicii de plată care au nevoie de o prelungire a termenului (de exemplu, dacă nu sunt încă disponibile cifre efective cu privire la impact) trebuie să contacteze autoritatea competentă înainte de încheierea termenului și să ofere o justificare adecvată a întârzierii, precum și o nouă dată estimată de transmitere a raportului final.

2.19. În cazul în care prestatorii de servicii de plată pot să ofere toate informațiile necesare în raportul final (mai exact, secțiunea C din model) în decurs de 4 ore de la momentul depistării incidentului, aceștia trebuie să aibă în vedere prezentarea în raportul lor inițial a informațiilor legate de raportul inițial, ultimul raport intermediar și raportul final.

2.20. Prestatorii de servicii de plată trebuie să urmărească să includă în rapoartele lor finale informații complete, mai exact (i) cifre efective privind impactul, nu estimări (precum și orice alte actualizări necesare în secțiunile A și B din model) și (ii) secțiunea C din model, care include cauza fundamentală, dacă aceasta este deja cunoscută, precum și o prezentare succintă a măsurilor adoptate sau prevăzute a fi adoptate pentru a elimina problema și a preveni reapariția acesteia în viitor.

2.21. Prestatorii de servicii de plată trebuie să trimită un raport final și atunci când, ca urmare a evaluării permanente a incidentului, aceștia identifică faptul că un incident deja raportat nu mai îndeplinește criteriile pentru a fi considerat major și nu se preconizează că acesta le va îndeplini înainte de soluționarea incidentului. În acest caz, prestatorii de servicii de plată trebuie să trimită raportul final de îndată ce se depistează această situație și, în orice caz, până la data estimată a următorului raport. În această situație specifică, în loc să se completeze secțiunea C din model, prestatorii de servicii de plată trebuie să selecteze caseta „incident reclasificat drept minor” și să explice motivele acestei declasări.

Orientarea 3: Raportarea delegată și consolidată

3.1. În cazul în care acest lucru este permis de către autoritatea competentă, prestatorii de servicii de plată care doresc să delege obligațiile de raportare în temeiul DSP 2 unei părți terțe trebuie să informeze autoritatea competentă din statul membru de origine și să asigure îndeplinirea următoarelor condiții:

a. Contractul oficial sau, după caz, acordurile interne existente în cadrul unui grup, care stă/stau la baza raportării delegate dintre prestatorul de servicii de plată și partea terță definește/definesc în mod clar alocarea responsabilităților tuturor părților. În mod specific, acesta prevede în mod clar faptul că, indiferent de o posibilă delegare a obligațiilor de raportare, prestatorul de servicii de plată afectat rămâne pe deplin responsabil și răspunzător pentru îndeplinirea cerințelor prevăzute la articolul 96 din DSP 2 și pentru conținutul informațiilor prezentate autorității competente din statul membru de origine.

b. Delegarea respectă cerințele privind externalizarea funcțiilor operaționale importante, astfel cum sunt prevăzute la

i. articolul 19 alineatul (6) din DSP 2 în legătură cu instituții de plată și instituții emitente de monedă electronică, aplicabile mutatis mutandis în conformitate cu articolul 3 din Directiva 2009/110/CE (Directiva privind moneda electronică); sau

ii. Ghidul CEBS intitulat „Guidelines on outsourcing in relation to credit institutions” (Ghidul privind externalizarea în legătură cu instituțiile de credit).

c. Informațiile sunt prezentate în avans autorității competente din statul membru de origine și, în orice caz, cu respectarea oricăror termene și proceduri instituite de autoritatea competentă, după caz.

d. Se asigură în mod corespunzător confidențialitatea datelor sensibile, precum și calitatea, consecvența, integritatea și fiabilitatea informațiilor care vor fi prezentate autorității competente.

3.2. Prestatorii de servicii de plată care doresc să permită părții terțe desemnate să îndeplinească obligațiile de raportare în mod consolidat (mai exact, prin prezentarea unui singur raport care face referire la mai mulți prestatori de servicii de plată afectați de același incident operațional sau de securitate major) trebuie să informeze autoritatea competentă din statul membru de origine, să includă informațiile de contact incluse la secțiunea „Prestatori de servicii de plată (PSP) afectați” din model și să se asigure de îndeplinirea următoarelor condiții:

a. Includerea acestei dispoziții în contractul care stă la baza raportării delegate.

b. Supunerea raportării consolidate condiției ca incidentul să fie cauzat de o întrerupere a serviciilor prestate de către partea terță.

c. Limitarea raportării consolidate la prestatorii de servicii de plată stabiliți în același stat membru.

d. Asigurarea faptului că partea terță evaluează semnificația incidentului pentru fiecare prestator de servicii de plată afectat și că include în raportul consolidat doar prestatorii de servicii de plată pentru care incidentul a fost clasificat drept unul major. Mai mult decât atât, asigurarea faptului că, în caz de îndoială, un prestator de servicii de plată este inclus în raportul consolidat atâta timp cât nu există dovezi în sens contrar.

e. Asigurarea faptului că, atunci când există unele câmpuri în model în care nu este posibil să se treacă un răspuns obișnuit (de exemplu, secțiunile B 2, B 4 sau C 3), partea terță fie (i) le completează individual pentru fiecare prestator de servicii de plată, specificând în plus identitatea fiecărui prestator de servicii de plată la care se referă informațiile, fie (ii) folosește intervale, în acele câmpuri în care există o astfel de opțiune, reprezentând valorile minime și maxime, astfel cum au fost observate sau estimate pentru diferiți prestatori de servicii de plată.

f. Prestatorii de servicii de plată trebuie să se asigure de faptul că partea terță îi ține la curent în permanență cu privire la toate informațiile relevante legate de incident și la toate interacțiunile pe care partea terță le-ar putea avea cu autoritatea competentă, precum și cu privire la conținutul acestora, însă doar în măsura în care acest lucru este compatibil cu evitarea oricărei încălcări a confidențialității în ceea ce privește informațiile referitoare la alți prestatori de servicii de plată.

3.3. Prestatorii de servicii de plată nu trebuie să își delege obligațiile de raportare înainte de a informa autoritatea competentă din statul membru de origine sau după ce au fost informați cu privire la faptul că acordul de externalizare nu îndeplinește cerințele prevăzute în Orientarea 3.1 litera (b).

3.4. Prestatorii de servicii de plată care doresc să retragă delegarea obligațiilor lor de raportare trebuie să comunice această decizie autorității competente din statul membru de origine în conformitate cu termenele și procedurile prevăzute de către acesta din urmă. Prestatorii de servicii de plată trebuie să informeze, de asemenea, autoritatea competentă din statul membru de origine cu privire la orice evoluție semnificativă care afectează partea terță desemnată și capacitatea acesteia de a-și îndeplini obligațiile de raportare.

3.5. Prestatorii de servicii de plată trebuie să își îndeplinească obligațiile de raportare în mod semnificativ, fără a recurge la asistența externă, ori de câte ori partea terță desemnată nu a informat autoritatea competentă din statul membru de origine cu privire la un incident operațional sau de securitate major în conformitate cu articolul 96 din DSP 2 și cu prezentul

ghid. În plus, prestatorii de servicii de plată trebuie să se asigure de faptul că un incident nu este raportat de două ori, personal de către prestatorul de servicii de plată în cauză și încă o dată de către partea terță.

Orientarea 4: Politica operațională și de securitate

4.1. Prestatorii de servicii de plată trebuie să se asigure de faptul că politica lor operațională și de securitate generală definește în mod clar toate responsabilitățile pentru raportarea incidentelor în temeiul DSP 2 și procesele puse în aplicare pentru îndeplinirea cerințelor prevăzute în prezentul ghid.

5. Orientări adresate autorităților competente referitor la criteriile privind modul de evaluare a relevanței incidentului și la detaliile din rapoartele referitoare la incident care se comunică altor autorități naționale

Orientarea 5: Evaluarea relevanței incidentului

5.1. Autoritățile competente din statul membru de origine trebuie să evalueze relevanța unui incident operațional sau de securitate major pentru alte autorități naționale pe baza propriului aviz de specialitate și folosind următoarele criterii ca indicatori primari ai importanței incidentului respectiv:

a. Cauzele incidentului intră în sfera de reglementare a celeilalte autorități naționale (mai exact, domeniul său de competență).
b. Consecințele incidentului au un impact asupra obiectivelor unei alte autorități naționale (de exemplu, asigurarea stabilității financiare).
c. Incidentul afectează sau ar putea afecta utilizatorii serviciilor de plată pe scară largă.
d. Este posibil ca incidentul să beneficieze de acoperire amplă în mass-media sau acesta a beneficiat de o astfel de acoperire.

5.2. Autoritățile competente din statul membru de origine trebuie să efectueze permanent această evaluare pe durata existenței incidentului pentru a identifica orice posibilă schimbare care ar putea atrage relevanța unui incident care nu era anterior considerat astfel.

Orientarea 6: Informații care trebuie comunicate

6.1. Fără a aduce atingere vreunei cerințe legale de a comunica informații legate de incident altor autorități naționale, autoritățile competente trebuie să prezinte informații despre incidente operaționale sau de securitate majore autorităților naționale identificate în urma aplicării Orientării 5.1 (mai exact, „alte autorități naționale relevante”), ca cerință minimă, la momentul primirii raportului inițial (sau, în mod alternativ, a raportului care a determinat comunicarea informațiilor) și atunci când acestea sunt informate că activitatea a revenit la normal (mai exact, prin ultimul raport intermediar).

6.2. Autoritățile competente trebuie să prezinte altor autorități naționale relevante informațiile necesare pentru a oferi o imagine clară a ceea ce s-a întâmplat și a consecințelor posibile. În acest sens, acestea trebuie să ofere, ca cerință minimă, informațiile date de către prestatorul serviciului de plată în următoarele câmpuri ale modelului (în raportul inițial sau în cel intermediar):

- data și ora depistării incidentului;
- data și ora declanșării incidentului;
- data și ora la care incidentul a fost stabilizat sau este prevăzut a fi stabilizat;
- o scurtă descriere a incidentului (inclusiv părțile nesensibile ale descrierii detaliate);
- o scurtă descriere a măsurilor luate sau prevăzute a fi luate pentru redresarea în urma incidentului;
- descrierea modului în care incidentul ar putea afecta alți PSP și/sau alte infrastructuri;
- descrierea acoperirii în mass-media (dacă există);
- cauza incidentului.

6.3. Autoritățile competente trebuie să deruleze un proces adecvat de anonimizare, după caz, și să omită orice informații care ar putea fi supuse restricțiilor privind confidențialitatea sau proprietatea intelectuală înainte de a comunica orice informații despre incident altor autorități naționale relevante. Cu toate acestea, autoritățile competente trebuie să furnizeze altor autorități naționale relevante numele și adresa prestatorului serviciului de plată care raportează atunci când autoritățile naționale în cauză pot garanta faptul că informațiile vor fi tratate în mod confidențial.

6.4. Autoritățile competente trebuie să păstreze în orice moment confidențialitatea și integritatea informațiilor stocate și schimbate cu alte autorități naționale relevante și, de asemenea, să se legitimeze în mod adecvat în fața altor autorități naționale relevante. În mod specific, autoritățile competente trebuie să trateze toate informațiile primite în cadrul prezentului ghid în conformitate cu obligațiile privind secretul profesional prevăzute în DSP 2, fără a aduce atingere dreptului Uniunii și cerințelor naționale aplicabile.

6. Orientări adresate autorităților competente referitor la criteriile privind modul de evaluare a detaliilor relevante din rapoartele referitoare la incident, care vor fi comunicate ABE și BCE, precum și la formatul și procedurile de comunicare a acestora

Orientarea 7: Informații care trebuie comunicate

7.1. Autoritățile competente trebuie să prezinte întotdeauna ABE și BCE toate rapoartele primite de la sau în numele prestatorilor de servicii de plată afectați de un incident operațional sau de securitate major (mai exact, rapoarte inițiale, intermediare și finale).

Orientarea 8: Comunicare

8.1. Autoritățile competente trebuie să păstreze în orice moment confidențialitatea și integritatea informațiilor stocate și schimbate cu ABE și BCE și, de asemenea, să se legitimeze în mod adecvat în fața ABE și BCE. În mod specific, autoritățile competente trebuie să trateze toate informațiile primite în cadrul prezentului ghid în conformitate cu obligațiile privind secretul profesional prevăzute în DSP 2, fără a aduce atingere dreptului Uniunii și cerințelor naționale aplicabile.

8.2. Pentru a evita întârzierile atunci când transmit informații legate de incidente către ABE/BCE și a ajuta la reducerea la minim a riscurilor întreruperilor operaționale, autoritățile competente trebuie să dețină mijloace adecvate de comunicare.

Anexa 1 – Modele de raportare pentru prestatorii de servicii de plată

CLASSIFICATION: RESTRICTED

Major Incident Report

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

Report date: DD/MM/YYYY — Time: HH:MM

Incident identification number, if applicable (for interim and final reports):

A - Initial report

A 1 - GENERAL DETAILS

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

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

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

B - Intermediate report

B 1 - GENERAL DETAILS

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

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

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

B 3 - INCIDENT DESCRIPTION

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

B 4 - INCIDENT IMPACT

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

B 5 - INCIDENT MITIGATION

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

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

Notes:

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

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

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

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

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

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

INSTRUCȚIUNI PRIVIND COMPLETAREA MODELELOR

Prestatorii de servicii de plată trebuie să completeze secțiunea relevantă din model în funcție de etapa de raportare în care se află: secțiunea A pentru raportul inițial, secțiunea B pentru rapoarte intermediare și secțiunea C pentru raportul final. Toate câmpurile sunt obligatorii, exceptând cazurile în care se specifică altfel în mod clar.

Titlu

Raport inițial: aceasta este prima notificare pe care PSP o transmite autorității competente din statul membru de origine.

Raport intermediar: acesta reprezintă o actualizare a raportului anterior (inițial sau intermediar) cu privire la același incident.

Ultimul raport intermediar: acesta informează autoritatea competentă din statul membru de origine cu privire la faptul că activitățile obișnuite au fost restabilite și că activitatea a revenit la normal, astfel că nu vor mai fi transmise rapoarte intermediare.

Raport final: acesta este ultimul raport pe care PSP îl va trimite cu privire la incident, întrucât (i) a fost deja efectuată o analiză a cauzelor fundamentale și estimările pot fi înlocuite cu cifre reale sau (ii) incidentul nu mai este considerat unul major.

Clasificarea incidentului drept unul minor: incidentul nu mai îndeplinește criteriile pentru a fi considerat major și nu este de așteptat să le îndeplinească înainte ca acesta să fie soluționat. PSP trebuie să explice motivele acestei declasări.

Data și ora raportului: data și ora exactă a transmiterii raportului autorității competente.

Numărul de identificare a incidentului, dacă este cazul (pentru raportul intermediar și cel final): numărul de referință emis de autoritatea competentă la momentul raportului inițial pentru a identifica în mod unic incidentul, dacă este cazul (mai exact, dacă o astfel de referință este oferită de autoritatea competentă).

A – Raport inițial

A 1 – Detalii generale

Tip de raport:

Individual: raportul se referă la un singur PSP.

Consolidat: raportul se referă la mai mulți PSP care utilizează opțiunea de raportare consolidată. Câmpurile de la secțiunea „PSP afectat” trebuie lăsate necompletate (cu excepția câmpului „Țara/țările afectată/afectate de incident”) și trebuie furnizată o listă a PSP incluși în raport prin completarea tabelului aferent (Raport consolidat - lista PSP).

PSP afectat: se referă la PSP căruia i se întâmplă incidentul.

Numele PSP: numele complet al PSP supus procedurii de raportare, așa cum apare în registrul național oficial al PSP aplicabil.

Numărul de identificare unic al PSP, dacă este relevant: numărul de identificare unic relevant utilizat în fiecare stat membru pentru identificarea PSP, care este oferit de PSP dacă nu se completează câmpul denumit „Numărul autorizației PSP”.

Numărul autorizației PSP: numărul de autorizare din statul membru de origine.

Șeful grupului: În cazul grupurilor de entități definite la articolul 4 alineatul (40) din Directiva (UE) 2015/2366 a Parlamentului European și a Consiliului din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010, și de abrogare a Directivei 2007/64/CE, vă rugăm să indicați numele entității conducătoare.

Țara de origine: Statul membru în care se află sediul social al PSP; sau, în cazul în care PSP nu are, în temeiul legislației naționale, niciun sediu social, statul membru în care se află sediul acestuia.

Țara/țările afectată/afectate de incident: țara sau țările în care s-a materializat impactul incidentului (de exemplu, sunt afectate mai multe sucursale ale unui PSP aflate în diferite țări). Este posibil ca aceasta să fie sau să nu fie aceeași cu statul membru de origine.

Persoana de contact principală: prenumele și numele de familie al persoanei responsabile de raportarea incidentului sau, dacă o persoană terță raportează în numele PSP afectat, prenumele și numele de familie al persoanei care conduce departamentul de gestionare a incidentelor/de risc sau o secție similară din cadrul PSP afectat.

E-mail: adresa de e-mail la care ar putea fi adresate orice solicitări de clarificări suplimentare, dacă este necesar. Poate fi un e-mail personal sau din partea societății.

Telefon: numărul de telefon care este apelat pentru orice solicitări de clarificări suplimentare, dacă este necesar. Poate fi un număr de telefon personal sau din partea societății.

Persoana de contact secundară: prenumele și numele de familie al unei persoane alternative care ar putea fi contactată de către autoritatea competentă pentru a solicita informații despre un incident atunci când persoana de contact principală nu este disponibilă. Dacă o parte terță raportează în numele PSP afectat, prenumele și numele de familie al unei persoane alternative din departamentul de gestionare a incidentelor/de risc sau dintr-o secție similară din cadrul PSP afectat.

E-mail: adresa de e-mail a persoanei de contact alternative la care ar putea fi adresate orice solicitări de clarificări suplimentare, dacă este necesar. Poate fi o adresă de e-mail personală sau din partea societății.

Telefon: numărul de telefon al persoanei de contact alternative care este apelat pentru orice solicitări de clarificări suplimentare, dacă este necesar. Poate fi un număr de telefon personal sau din partea societății.

Entitatea de raportare: această secțiune trebuie completată dacă o parte terță îndeplinește obligațiile de raportare în numele PSP afectat.

Denumirea entității de raportare: denumirea completă a entității care raportează incidentul, așa cum apare în registrul național oficial al companiilor aplicabil.

Număr de identificare unic, dacă este relevant: numărul de identificare unic relevant utilizat în țara în care se află partea terță pentru a identifica entitatea care raportează incidentul, care se introduce de către entitatea de raportare în cazul în care câmpul „Numărul autorizației” nu este completat.

Numărul autorizației, dacă este cazul: numărul de autorizare al părții terțe în țara în care se află aceasta, dacă este cazul.

Persoana de contact principală: prenumele și numele de familie al persoanei responsabile de raportarea incidentului.

E-mail: adresa de e-mail la care ar putea fi adresate orice solicitări de clarificări suplimentare, dacă este necesar. Poate fi un e-mail personal sau din partea societății.

Telefon: numărul de telefon care este apelat pentru orice solicitări de clarificări suplimentare, dacă este necesar. Poate fi un număr de telefon personal sau din partea societății.

Persoana de contact secundară: prenumele și numele de familie al unei persoane alternative din cadrul entității care raportează incidentul, care ar putea fi contactată de către autoritatea competentă atunci când persoana de contact principală nu este

disponibilă.

E-mail: adresa de e-mail a persoanei de contact alternative la care ar putea fi adresate orice solicitări de clarificări suplimentare, dacă este necesar. Poate fi o adresă de e-mail personală sau din partea societății.
Telefon: numărul de telefon al persoanei de contact alternative care este apelat pentru orice solicitări de clarificări suplimentare care pot fi abordate, dacă este necesar. Poate fi un număr de telefon personal sau din partea societății.

A 2 – Depistarea incidentului și clasificarea inițială

Data și ora depistării incidentului: data și ora la care incidentul a fost identificat pentru prima dată.
Incident depistat de către: indică dacă incidentul a fost depistat de către un utilizator al unui serviciu de plată, o altă parte din cadrul PSP (de exemplu, o funcție de audit internă) sau o parte externă (de exemplu, un prestator extern de servicii). În alte cazuri, vă rugăm să oferiți o explicație în câmpul aferent.
Descriere generală și pe scurt a incidentului: vă rugăm să explicați pe scurt cele mai relevante aspecte ale incidentului, cu acoperirea posibilelor cauze, a impactului imediat etc.
Care este momentul estimat pentru următoarea actualizare?: indică data și ora estimată pentru transmiterea următoarei actualizări (raportul intermediar sau cel final).

B – Raport intermediar

B 1 – Detalii generale

Descrierea mai detaliată a incidentului: vă rugăm să descrieți principalele caracteristici ale incidentului, care să acopere cel puțin punctele prezentate în chestionar (cu ce problemă specifică se confruntă PSP, cum s-a declanșat și s-a dezvoltat incidentul, o posibilă legătură cu un incident anterior, consecințe, mai ales pentru utilizatorii serviciilor de plată etc.).
Data și ora declanșării incidentului: data și ora la care a apărut incidentul, dacă sunt cunoscute.
Starea incidentului:

Diagnostic: caracteristicile incidentului tocmai au fost identificate.
Reparare: elementele atacate se află în curs de reconfigurare.
Redresare: elementele defectate se află în curs de stabilizare la ultima lor stare posibilă de redresare.
Stabilizare: se prestează din nou serviciul aferent plăților.

Data și ora la care incidentul a fost stabilizat sau este de așteptat a fi stabilizat: indică data și ora la care incidentul a fost sau este de așteptat a fi sub control și la care activitatea a fost sau este prevăzută a reveni la normal.

B 2 – Clasificarea incidentului/informații despre incident

Impact global: vă rugăm să indicați aspectele care au fost afectate de incident. Pot fi selectate mai multe casete.

Integritate: proprietatea de a asigura precizia și caracterul complet al activelor (inclusiv al datelor).
Disponibilitate: proprietatea serviciilor aferente plăților de a fi accesibile și utilizabile de către utilizatorii serviciilor de plată.
Confidențialitate: proprietatea de a nu pune la dispoziție sau de a nu prezenta informații persoanelor, entităților sau proceselor neautorizate.

Autenticitate: proprietatea unei surse de a fi ceea ce se pretinde a fi.

Continuitate: proprietatea proceselor, sarcinilor și activelor unei organizații, care sunt necesare pentru prestarea serviciilor aferente plăților, de a fi pe deplin accesibile și de a se desfășura, respectiv de a funcționa, la niveluri prestabilite acceptabile.

Operațiuni afectate: PSP trebuie să precizeze pragurile care sunt sau vor fi probabil atinse de către incident, dacă există, precum și cifrele aferente: numărul operațiunilor afectate, procentul operațiunilor afectate în raport cu numărul operațiunilor de plată executate cu aceleași servicii de plată care au fost afectate de incident, precum și valoarea totală a operațiunilor. PSP trebuie să prezinte valori specifice pentru aceste variabile, care pot fi cifre efective sau estimări. Entitățile care raportează în numele mai multor PSP (mai exact, raportarea consolidată) pot prezenta în schimb intervale de valori reprezentând valori minime și maxime observate sau estimate în cadrul grupului de PSP incluși în raport, separate printr-o cratimă. Ca și regulă generală, PSP trebuie să înțeleagă ca fiind „operațiuni afectate" toate operațiunile interne și transfrontaliere care au fost sau vor fi probabil afectate în mod direct sau indirect de incident și, în mod specific, acele operațiuni care nu au putut fi inițiate sau procesate, cele al căror conținut al mesajului de plată a fost modificat și cele care au fost dispuse în mod fraudulos (indiferent dacă fondurile au fost recuperate sau nu). Mai mult, PSP trebuie să înțeleagă faptul că nivelul obișnuit al operațiunilor de plată este media anuală zilnică a operațiunilor interne și transfrontaliere executate cu aceleași servicii de plată care au fost afectate de incident, anul anterior fiind perioada de referință pentru calcule. Dacă PSP nu consideră că această cifră este reprezentativă (de exemplu, din cauza caracterului sezonier), aceștia trebuie să utilizeze, în schimb, un alt indicator mai reprezentativ și să prezinte autorității naționale justificarea aferentă acestei abordări în câmpul „Observații".

Utilizatori ai serviciilor de plată afectați: PSP trebuie să precizeze pragurile care sunt sau vor fi probabil atinse de către incident, dacă există, și cifrele aferente: numărul total al utilizatorilor serviciilor de plată care au fost afectați și procentul utilizatorilor serviciilor de plată afectați din numărul total al utilizatorilor serviciilor de plată. PSP trebuie să prezinte valori concrete pentru aceste variabile, care pot fi cifre efective sau estimări. Entitățile care raportează în numele mai multor PSP (mai exact, raportarea consolidată) pot prezenta în schimb intervale de valori reprezentând valori minime și maxime observate sau estimate în cadrul grupului de PSP incluși în raport, separate printr-o cratimă. PSP trebuie să înțeleagă ca fiind „utilizatori ai serviciilor de plată afectate" toți clienții (de la nivel intern sau din străinătate, consumatori sau întreprinderi) care au un contract cu prestatorul serviciului de plată afectat, care le acordă acestora accesul la serviciul de plată afectat, și care au suportat sau vor suporta probabil consecințele incidentului. PSP trebuie să recurgă la estimări bazate pe activitatea anterioară pentru a stabili numărul utilizatorilor serviciilor de plată care este posibil să fi folosit serviciul de plată pe durata incidentului. În cazul grupurilor, fiecare PSP trebuie să aibă în vedere doar utilizatorii serviciilor de plată proprii. În cazul unui PSP care oferă servicii operaționale altor persoane, acesta trebuie să aibă în vedere doar utilizatorii de servicii de plată proprii (dacă există), iar PSP care beneficiază de respectivele servicii operaționale trebuie să evalueze, de asemenea, incidentul în legătură cu utilizatorii serviciilor de plată proprii. Mai mult, PSP trebuie să considere ca fiind numărul total al utilizatorilor serviciilor de plată valoarea agregată a utilizatorilor serviciilor de plată interni și transfrontalieri care le sunt acestora obligați prin contract la momentul incidentului (sau, alternativ, cea mai recentă valoare disponibilă) și care au acces la serviciul de plată afectat, indiferent de dimensiunea acestora sau dacă aceștia sunt considerați utilizatori activi sau pasivi ai serviciilor de plată.

Timpul de indisponibilitate a serviciului: PSP trebuie să precizeze dacă pragul este sau va fi probabil atins de către incident, precum și cifra aferentă: timpul total de indisponibilitate a

serviciului. PSP trebuie să prezinte valori concrete pentru această variabilă, care poate fi exprimată în cifre efective sau estimări. Entitățile care raportează în numele mai multor PSP (mai exact, raportarea consolidată) pot prezenta în schimb un interval de valori reprezentând valori minime și maxime observate sau estimate în cadrul grupului de PSP incluși în raport, separate printr-o cratimă. PSP trebuie să aibă în vedere perioada de timp în care orice sarcină, proces sau canal asociat prestării serviciilor de plată este sau va fi probabil indisponibil și, astfel, împiedică (i) inițierea și/sau executarea unui serviciu de plată și/sau (ii) accesul la un cont de plăți. PSP trebuie să calculeze timpul de indisponibilitate a serviciului de la momentul inițial al indisponibilității și trebuie să ia în considerare atât intervalele de timp în care aceștia funcționează conform cerințelor de executare a serviciilor de plată, cât și orele în care nu funcționează, precum și perioadele de întreținere, dacă este cazul și dacă există. Dacă prestatorii de servicii de plată nu pot să stabilească momentul inițial al indisponibilității serviciului, aceștia trebuie să calculeze în mod excepțional timpul de indisponibilitate a serviciului de la momentul în care s-a depistat indisponibilitatea.

Impactul economic: PSP trebuie să precizeze dacă pragul este sau va fi probabil atins de către incident, precum și cifrele aferente: costurile directe și indirecte. PSP trebuie să prezinte valori concrete pentru aceste variabile, care pot fi cifre efective sau estimări. Entitățile care raportează în numele mai multor PSP (mai exact, raportarea consolidată) pot prezenta în schimb un interval de valori reprezentând valori minime și maxime observate sau estimate în cadrul grupului de PSP incluși în raport, separate printr-o cratimă. PSP trebuie să aibă în vedere atât costurile care pot fi legate în mod direct de incident, cât și cele care sunt legate în mod indirect de incident. Printre altele, PSP trebuie să țină cont de fondurile sau activele expropriate, costurile de înlocuire a echipamentelor hardware sau software, alte costuri realizate în scopuri judiciare sau costuri de remediere, taxe aplicate ca urmare a neconformității cu obligațiile contractuale, sancțiuni, datorii externe și venituri pierdute. În ceea ce privește costurile indirecte, PSP trebuie să le aibă în vedere doar pe cele care sunt deja cunoscute sau foarte probabil de a se concretiza.

> **Costuri directe:** suma de bani (în euro) asociată costului direct al incidentului, inclusiv fonduri necesare pentru remedierea incidentului (de exemplu, fonduri sau active expropriate, costuri de înlocuire a echipamentelor hardware și software, tarife datorate nerespectării obligațiilor contractuale).
>
> **Costuri indirecte:** suma de bani (în euro) asociată costului indirect al incidentului (de exemplu, costuri asociate reparațiilor/compensațiilor pentru clienți, venituri pierdute ca urmare a oportunităților de afaceri ratate, posibile cheltuieli judiciare).

Nivelul ridicat de escaladare internă: PSP trebuie să aibă în vedere dacă, în urma impactului incidentului asupra serviciilor aferente plăților, responsabilul pentru sistemele informatice (sau o persoană cu o funcție similară) a fost sau va fi probabil informat cu privire la incident în afara oricărei proceduri de notificare periodice și în permanență pe durata existenței incidentului. În cazul raportării delegate, escaladarea ar avea loc în cadrul părții terțe. În plus, PSP trebuie să aibă în vedere dacă, în urma impactului incidentului asupra serviciilor aferente plăților, a fost sau este susceptibilă de a fi declanșată o stare de criză.

Alți PSP sau infrastructuri relevante care ar putea fi afectate: prestatorii de servicii de plată trebuie să evalueze impactul incidentului asupra pieței financiare, care este înțeleasă ca fiind infrastructurile pieței financiare și/sau schemele de plată cu cardul care îi susțin pe aceștia și pe ceilalți PSP. În mod specific, PSP trebuie să evalueze dacă incidentul a apărut sau va apărea probabil în mod similar la alți PSP, dacă acesta a afectat sau va afecta probabil funcționarea fără probleme a infrastructurilor pieței financiare și dacă a compromis sau va compromite probabil soliditatea sistemului financiar în ansamblu. PSP trebuie să aibă în vedere diferite aspecte, precum dacă o componentă/un echipament software afectată/afectat este supusă/supus unor

drepturi de proprietate sau este disponibilă/disponibil în general, dacă rețeaua compromisă este internă sau externă și dacă PSP a încetat sau va înceta probabil să își îndeplinească obligațiile în infrastructurile pieței financiare al cărei membru este acesta.

Impactul asupra reputației: PSP trebuie să aibă în vedere nivelul de vizibilitate pe care, după cunoștința lor, incidentul l-a atins sau îl va atinge probabil pe piață. În mod specific, PSP trebuie să aibă în vedere probabilitatea ca incidentul să provoace daune societății ca fiind un indicator bun al potențialului acestuia de a afecta reputația lor. PSP trebuie să țină cont dacă (i) incidentul a afectat un proces vizibil și, prin urmare, este susceptibil de a dobândi sau a dobândit deja acoperire mediatică (având în vedere nu doar mass-media tradițională, precum ziarele, ci și blog-uri, rețele de socializare etc.), (ii) obligațiile de reglementare au fost sau sunt susceptibile de a fi omise, (iii) au fost sau vor fi susceptibile de a fi încălcate sancțiuni sau (iv) a apărut același tip de incident în trecut.

B 3 – Descrierea incidentului

Tipul incidentului: precizați dacă, după cunoștința voastră, este un incident operațional sau de securitate.

Operațional: Incident care apare ca urmare a unor procese inadecvate sau defectuoase, din cauza unor persoane și sisteme ori cazuri de forță majoră care afectează integritatea, disponibilitatea, confidențialitatea, autenticitatea și/sau continuitatea serviciilor aferente plăților.

Securitate: accesul, utilizarea, publicarea, întreruperea, modificarea sau distrugerea neautorizată a activelor PSP care afectează integritatea, disponibilitatea, confidențialitatea, autenticitatea și/sau continuitatea serviciilor aferente plăților. Acest lucru se poate întâmpla atunci când, printre altele, PSP se confruntă cu atacuri cibernetice, o proiectare sau implementare defectuoasă a politicilor de securitate sau o securitate fizică necorespunzătoare.

Cauza incidentului: precizați cauza incidentului sau, dacă aceasta nu se cunoaște încă, cea mai probabilă cauză. Pot fi selectate mai multe casete.

În curs de investigare: cauza nu a fost încă stabilită.

Atac extern: sursa cauzei provine din exterior și vizează în mod intenționat PSP (de exemplu, atacuri prin malware).

Atac intern: sursa cauzei provine din interior și vizează în mod intenționat PSP (de exemplu, fraudă internă).

Tip de atac:

Atacuri distribuite cu blocarea accesului (D/DoS): o încercare de a indisponibiliza un serviciu online prin încărcarea acestuia cu trafic din mai multe surse.

Infectarea sistemelor interne: o activitate dăunătoare care atacă sistemele informatice, încercând să fure spațiu de pe hard disk sau timp de pe CPU, să acceseze informații cu caracter personal, să corupă date, să trimită mesaje nesolicitate la adresele de contact etc.

Intruziune țintită: un act neautorizat de spionare, supraveghere și furt de informații în spațiul cibernetic.

Altele: orice alt tip de atac pe care PSP l-ar fi putut suferi în mod direct sau prin intermediul unui prestator de servicii. În mod specific, dacă a existat un atac care a vizat procesul de autorizare și autentificare, trebuie selectată această casetă. Trebuie adăugate detalii în câmpul aferent textului liber.

Evenimente externe: cauza este asociată unor evenimente care se află, în general, în afara controlului organizației (de exemplu, calamități naturale, probleme juridice,

probleme economice și dependențe de servicii).

Eroare umană: incidentul a fost cauzat ca urmare a erorii neintenționate a unei persoane, fie în cadrul procedurii de plată (de exemplu, încărcarea fișierului lot de plăți greșit în sistemul de plăți) sau oarecum în legătură cu aceasta (de exemplu, se întrerupe accidental curentul și activitatea de plată este pusă în așteptare).

Eroare de procesare: cauza incidentului a fost o proiectare sau o executare deficitară a procesului de plată, a comenzilor procesului și/sau a proceselor suport (de exemplu, procesul de schimbare/migrare, testare, configurare, capacitate, monitorizare).

Defectarea sistemului: cauza incidentului este asociată caracterului inadecvat al proiectării, executării, componentelor, specificațiilor, integrării sau complexității sistemelor care susțin activitatea de plată.

Altele: cauza incidentului nu este niciuna dintre cele de mai sus. Trebuie furnizate detalii suplimentare în câmpul aferent textului liber.

Incidentul v-a afectat în mod direct sau indirect prin intermediul unui prestator de servicii?: un incident poate viza un PSP în mod direct sau în mod indirect, prin intermediul unei terțe părți. În cazul unui impact indirect, vă rugăm să precizați numele prestatorului (prestatorilor) de servicii.

B 4 – Impactul incidentului

Clădire (clădiri) afectată (afectate), dacă este cazul: dacă o clădire este afectată fizic, vă rugăm să precizați adresa acesteia.

Canale comerciale afectate: precizați canalul sau canalele de interacțiune cu utilizatorii serviciilor de plată, care au fost afectate de incident. Pot fi selectate mai multe casete.

Sucursale: sediul comercial (altul decât sediul social) care face parte dintr-un PSP, nu are personalitate juridică și execută în mod direct unele sau toate operațiunile inerente activității unui PSP. Toate sediile comerciale înființate în același stat membru de către un PSP al cărui sediu social se află într-un alt stat membru trebuie considerate ca fiind o singură sucursală.

Servicii bancare electronice: utilizarea de calculatoare pentru desfășurarea tranzacțiilor financiare pe internet.

Servicii bancare prin telefon: utilizarea de telefoane pentru desfășurarea tranzacțiilor financiare.

Servicii bancare pe mobil: utilizarea unei anumite aplicații bancare pe un smartphone sau un dispozitiv similar pentru desfășurarea tranzacțiilor financiare.

Bancomate: dispozitive electromecanice care permit utilizatorilor serviciilor de plată să retragă numerar din conturile lor și/sau să acceseze alte servicii.

Punct de desfacere: spațiu fizic al comerciantului la care este inițiată operațiunea de plată.

Altele: canalul comercial afectat nu este niciunul dintre cele de mai sus. Trebuie furnizate detalii suplimentare în câmpul aferent textului liber.

Servicii de plată afectate: precizați acele servicii de plată care nu funcționează corect ca urmare a incidentului. Pot fi selectate mai multe casete.

Plasare de numerar într-un cont de plăți: depunerea de numerar la un PSP pentru a credita un cont de plăți.

Retragere de numerar dintr-un cont de plăți: solicitarea primită de către un PSP din partea utilizatorului serviciului său de plăți pentru a furniza numerar și a-și debita contul de plăți cu suma aferentă.

Operațiuni impuse pentru operarea unui cont de plăți: acele acțiuni care trebuie să fie realizate într-un cont de plăți pentru a activa, a dezactiva și/sau a menține contul respectiv (de exemplu, deschidere, blocare).

Dobândirea de instrumente de plată: un serviciu de plată care constă în faptul că un PSP stabilește în baza unui contract cu un beneficiar al plății să accepte și să proceseze operațiuni de plată, rezultând într-un transfer al fondurilor către beneficiarul plății.

Transferuri de credit: un serviciu de plată pentru creditarea a unui cont de plăți al unui beneficiar al plății cu o operațiune de plată sau o serie de operațiuni de plată din contul de plăți al unui plătitor de către PSP care deține contul de plăți al plătitorului pe baza unei instrucțiuni date de către plătitor.

Debitări directe: un serviciu de plată pentru debitarea contului de plăți al unui plătitor, în cazul în care o operațiune de plată este inițiată de beneficiarul plății pe baza consimțământului dat de către plătitor beneficiarului plății, prestatorului de servicii de plată al plătitorului sau propriului prestator de servicii de plată al beneficiarului plății.

Plăți cu cardul: un serviciu de plată bazat pe infrastructura și regulile economice ale unei scheme de plată cu cardul pentru a desfășura o tranzacție de plată prin intermediul oricărui card, oricăror mijloace de telecomunicații, dispozitive digitale sau informatice, ori software dacă rezultatul acestuia este o operațiune cu cardul de debit sau cu cardul de credit. Operațiunile de plată cu cardul exclud operațiunile bazate pe alte tipuri de servicii de plată.

Emiterea instrumentelor de plată: un serviciu de plată care constă în faptul că un PSP stabilește cu un plătitor în baza unui contract ca acesta să îi furnizeze un instrument de plată pentru a iniția și a procesa operațiunile de plată ale plătitorului.

Remitere de bani: un serviciu de plată prin care se primesc fonduri de la un plătitor fără a se crea conturi de plăți în numele plătitorului sau al beneficiarului plății în scopul unic de a transfera o sumă corespunzătoare unui beneficiar al plății sau unui alt PSP care acționează în numele beneficiarului plății și/sau prin care se primesc astfel de fonduri în numele și la dispoziția beneficiarului plății.

Servicii de inițiere a plății: servicii de plată pentru inițierea unui ordin de plată la solicitarea utilizatorului serviciului de plăți în legătură cu un cont de plăți deținut în cadrul unui alt PSP.

Servicii de informare privind conturi: servicii de plată online pentru a oferi informații consolidate cu privire la unul sau mai multe conturi de plăți deținute de către utilizatorul serviciului de plăți la un alt PSP sau la mai mulți PSP.

Altele: serviciul de plată afectat nu este niciunul dintre cele de mai sus. Trebuie furnizate detalii suplimentare în câmpul aferent textului liber.

Segmente funcționale afectate: precizați etapa sau etapele din cadrul procesului de plată care au fost afectate de incident. Pot fi selectate mai multe casete.

Autentificare/autorizare: procedurile care permit PSP să verifice identitatea unui utilizator al serviciului de plată sau valabilitatea utilizării unui anumit instrument de plată, inclusiv a utilizării elementelor de securitate personalizate ale utilizatorului, și a exprimării acordului utilizatorului serviciului de plată (sau al unui terț care acționează în numele utilizatorului respectiv) față de transferarea fondurilor sau a valorilor mobiliare.

Comunicare: fluxul de informații în scopul identificării, autentificării, notificării și informării în rândul PSP care deservesc contul și al prestatorilor de servicii de inițiere a plății, al prestatorilor de servicii de informare cu privire la conturi, al plătitorilor, al beneficiarilor plății și al altor PSP.

Compensare: un proces de transmitere, reconciliere și, în unele cazuri, confirmare a ordinelor de transfer înainte de decontare, eventual cu includerea compensării ordinelor și cu stabilirea pozițiilor finale pentru decontare.
Decontare directă: încheierea unei tranzacții sau a procesării cu scopul de a îndeplini obligațiile participanților prin transferarea de fonduri atunci când această acțiune este desfășurată de către însuși PSP afectat.
Decontare indirectă: încheierea unei tranzacții sau a procesării cu scopul de a îndeplini obligațiile participanților prin transferarea de fonduri atunci când această acțiune este desfășurată de către un alt PSP în numele PSP afectat.
Altele: domeniul funcțional afectat nu este niciunul dintre cele de mai sus. Trebuie furnizate detalii suplimentare în câmpul aferent textului liber.

Sisteme și componente afectate: precizați care parte sau părți din infrastructura tehnologică a PSP a/au fost afectată/afectate de incident. Pot fi selectate mai multe casete.

Aplicație/software: programe, sisteme de operare etc. care susțin furnizarea de servicii de plată de către PSP.
Bază de date: structură de date care stochează informații cu caracter personal și despre plăți necesare pentru executarea operațiunilor de plată.
Hardware: echipament tehnologic fizic care derulează procesele și/sau stochează datele necesare PSP pentru a-și desfășura activitatea legată de plăți.
Rețea/infrastructură: rețele de telecomunicații, publice sau private, care permit schimbul de date și informații în cursul procesului de plată (de exemplu, internetul).
Altele: sistemul și componenta afectate nu sunt dintre cele de mai sus. Trebuie furnizate detalii suplimentare în câmpul aferent textului liber.

Personal afectat: precizați dacă incidentul a avut efecte asupra personalului PSP și, în acest caz, oferiți detalii în câmpul aferent textului liber.

B 5 – Atenuarea incidentului

Ce acțiuni/măsuri au fost luate până acum sau sunt prevăzute pentru a redresa situația după incident?: vă rugăm să oferiți detalii despre acțiuni care au fost luate sau prevăzute a fi luate pentru abordarea temporară a incidentului.
Planurile de asigurare a continuității activității și/sau de recuperare în urma dezastrelor au fost activate?: vă rugăm să precizați dacă acestea au fost activate și, în acest caz, să oferiți cele mai relevante detalii despre ceea ce s-a întâmplat (mai exact, când au fost activate și în ce au constat aceste planuri).
PSP a anulat sau a slăbit unele măsuri de control din cauza incidentului?: vă rugăm să precizați dacă PSP a trebuit să anuleze unele măsuri de control (de exemplu, încetarea aplicării principiului celor patru ochi) pentru abordarea incidentului și, în acest caz, să ofere detalii despre motivele aferente, cu justificarea slăbirii sau anulării măsurilor de control în cauză.

C – Raportul final

C 1 – Detalii generale

Actualizarea informațiilor din raportul intermediar (rezumat): vă rugăm să oferiți informații suplimentare cu privire la acțiunile luate pentru recuperarea de pe urma incidentului și evitarea reapariției acestuia, analiza cauzei fundamentale, lecțiile învățate etc.

Data și ora încheierii incidentului: precizați data și ora la care incidentul a fost considerat încheiat.

Măsurile de control inițiale au fost reluate?: dacă PSP a trebuit să anuleze sau să slăbească unele măsuri de control din cauza incidentului, precizați dacă astfel de măsuri de control au fost

reluate și oferiți orice informații suplimentare în câmpul aferent textului liber.

C 2 – Analiza cauzei fundamentale și acțiuni de urmărire

Care a fost cauza fundamentală, dacă este deja cunoscută?: vă rugăm să explicați care este cauza fundamentală a incidentului sau, dacă aceasta nu este cunoscută încă, concluziile preliminare trase ca urmare a analizei cauzei fundamentale. PSP pot anexa un fișier cu informații detaliate, dacă se consideră necesar.

Acțiuni corective/măsuri de remediere principale luate sau prevăzute pentru prevenirea reapariției incidentului în viitor, dacă se cunoaște deja: vă rugăm să descrieți acțiunile principale care au fost luate sau sunt prevăzute a fi luate pentru a preveni reapariția incidentului în viitor.

C 3 – Informații suplimentare

Incidentul a fost comunicat altor PSP în scop informativ?: vă rugăm să oferiți o scurtă prezentare a PSP care au fost contactați, pe cale oficială sau neoficială, pentru a-i pune la curent cu privire la incident, prezentând detalii despre PSP care au fost informați, informațiile care au fost comunicate și motivele care au stat la baza comunicării acestor informații.

Au fost inițiate acțiuni în justiție împotriva PSP?: vă rugăm să precizați dacă la data completării raportului final, PSP a făcut obiectul vreunei acțiuni în justiție (de exemplu, a fost adus în instanță sau și-a pierdut licența) ca urmare a producerii incidentului.