EBA/GL/2021/03

10 iunie 2021

Ghid revizuit

privind raportarea incidentelor majore în temeiul DSP2

1. Conformitate și obligații de raportare

Statutul prezentului ghid

1. Prezentul document conține orientări emise în temeiul articolul 16 din Regulamentul ABE[1]. În conformitate cu articolul 16 alineatul (3) din Regulamentul ABE, autoritățile competente și instituțiile financiare trebuie să depună toate eforturile pentru a respecta ghidul.

2. Ghidul prezintă punctul de vedere al ABE privind practicile adecvate în materie de supraveghere în cadrul Sistemului european de supraveghere financiară sau privind modul în care trebuie 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 ABE, trebuie să se conformeze și să îl integreze în practicile lor, după caz (de exemplu, prin modificarea cadrului legislativ sau a procedurilor de supraveghere), inclusiv în cazul în care orientările se adresează în primul rând instituțiilor.

Cerințe de raportare

3. În conformitate cu articolul 16 alineatul (3) din Regulamentul ABE, autoritățile competente trebuie să notifice ABE dacă se conformează sau intenționează să se conformeze prezentului ghid sau, în caz contrar, motivele neconformării până la data de (07.11.2021). 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, cu mențiunea „EBA/GL/2021/03”. Notificările trebuie trimise de persoane care au autoritatea de a raporta cu privire la conformare 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

Obiectul

5. Prezentul ghid derivă din mandatul acordat ABE la articolul 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 Regulamentul (UE) nr. 1093/2010, precum și de abrogare a Directivei 2007/64/CE (DSP2).

6. În special, prezentul ghid specifică criteriile de clasificare a 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 se prevede la articolul 96 alineatul (1) din DSP2, autorității competente din statul membru de origine.

7. În plus, prezentul ghid abordează modul în care aceste autorități competente trebuie să evalueze relevanța incidentului și detaliile rapoartelor privind incidentul pe care, în conformitate cu articolul 96 alineatul (2) din DSP2, trebuie să le comunice altor autorități naționale.

8. Mai mult, prezentul ghid se referă, de asemenea, la transmiterea către ABE și BCE a detaliilor relevante ale incidentelor raportate, în scopul promovării unei abordări comune și coerente.

Domeniul de aplicare

9. Prezentul ghid se aplică în ceea ce privește clasificarea și raportarea incidentelor majore operaționale sau de securitate în conformitate cu articolul 96 din DSP2.

10. Prezentul ghid se aplică tuturor incidentelor incluse în definiția „incidentelor operaționale sau de securitate majore”, care acoperă atât evenimente externe, cât și evenimente 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 își are originea în afara Uniunii (de exemplu, atunci când un incident își are originea în societatea-mamă sau într-o filială stabilită în afara Uniunii) și afectează serviciile de plată furnizate de un prestator de servicii de plată situat în Uniune fie direct (un serviciu de plată este efectuat de societatea din afara Uniunii afectată), fie indirect (capacitatea prestatorului de servicii de plată de a-și continua activitatea de plată este periclitată în alt mod ca urmare a incidentului).

12. Prezentul ghid se aplică, de asemenea, incidentelor majore care afectează funcțiile externalizate de prestatorii de servicii de plată către terți.

Destinatari

13. Primul set de orientări (secțiunea 4) se adresează prestatorilor de servicii de plată, astfel cum sunt definiți la articolul 4 alineatul (11) din DSP2 și astfel cum se menționează la articolul 4 alineatul (1) din Regulamentul (UE) nr. 1093/2010.

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

Definiții

15. Cu excepția cazului în care se prevede altfel, termenii utilizați și definiți în DSP2 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 prestatorul de servicii de plată care are sau ar putea avea un impact negativ asupra integrității, disponibilității, confidențialității și/sau autenticității serviciilor legate de plăți.
Integritate	Proprietatea de a garanta acuratețea și exhaustivitatea activelor (inclusiv a datelor).
Disponibilitate	Proprietatea serviciilor legate de plăți să fie pe deplin accesibile și utilizabile de către utilizatorii serviciilor de plată, în conformitate cu niveluri acceptabile predefinite de prestatorul de servicii de plată.
Confidențialitate	Proprietatea de a nu pune la dispoziție sau de a nu divulga informații persoanelor, entităților sau proceselor neautorizate.
Autenticitate	Proprietatea unei surse de a fi ceea ce se pretinde a fi.
Servicii legate de plăți	Orice activitate economică în sensul articolului 4 alineatul (3) din DSP 2 și toate sarcinile tehnice de suport necesare pentru furnizarea corectă a serviciilor de plată.

3. Implementare

Data punerii în aplicare

16. Prezentul ghid se aplică începând cu 1 ianuarie 2022.

Abrogare

17. Următorul ghid se abrogă începând cu 1 ianuarie 2022:

Ghid privind raportarea incidentelor majore în temeiul Directivei (UE) 2015/2366 (DSP2) (EBA/GL/2017/10)

4. Orientări adresate prestatorilor de servicii de plată cu privire la notificarea incidentelor operaționale sau de securitate majore către autoritatea competentă din statul lor membru de origine

Orientarea 1: Clasificarea ca incident major

1.1. Prestatorii de servicii de plată trebuie să clasifice drept incidente majore incidentele 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 la „nivelul de impact inferior”,

astfel cum se prevede 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 de bază ai acestora:

i. Tranzacții afectate

Prestatorii de servicii de plată trebuie să determine valoarea totală a tranzacțiilor afectate, precum și numărul de plăți compromise ca procent din nivelul regulat al operațiunilor de plată efectuate cu serviciile de plată afectate.

ii. Utilizatorii serviciilor de plată afectați

Prestatorii de servicii de plată trebuie să determine numărul de utilizatori ai serviciilor de plată afectați atât în termeni absoluți, cât și ca procent din numărul total de utilizatori ai serviciilor de plată.

iii. Încălcarea securității rețelelor sau a sistemelor informatice

Prestatorii de servicii de plată trebuie să stabilească dacă orice acțiune răuvoitoare a compromis securitatea rețelelor sau a sistemelor informatice legate de furnizarea de servicii de plată.

iv. Indisponibilitatea serviciului

Prestatorii de servicii de plată trebuie să stabilească perioada de timp în care serviciul ar putea să nu fie disponibil pentru utilizatorul serviciilor de plată sau în care ordinul de plată

— în sensul articolului 4 alineatul (13) din DSP2 — nu poate fi executat de prestatorul de servicii de plată.

v. Impactul economic

Prestatorii de servicii de plată trebuie să determine costurile monetare asociate incidentului în mod holistic și să țină seama atât de cifra absolută, cât și, după caz, de importanța relativă a acestor costuri în raport cu dimensiunea prestatorului de servicii de plată (și anume, cu capitalul de rangul 1 al prestatorului de servicii de plată).

vi. Nivel ridicat de escaladare internă

Prestatorii de servicii de plată trebuie să stabilească dacă acest incident a fost sau va fi probabil raportat agenților lor executivi.

vii. Alți prestatori de servicii de plată sau alte infrastructuri relevante potențial afectate

Prestatorii de servicii de plată trebuie să determine implicațiile sistemice pe care le-ar putea avea incidentul, și anume potențialul acestuia de a se extinde dincolo de prestatorul de servicii de plată afectat inițial către alți prestatori de servicii de plată, alte infrastructuri ale pieței financiare și/sau alte scheme de plată.

viii. 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, în general, în serviciul subiacent sau în piață în ansamblu.

1.3. Prestatorii de servicii de plată trebuie să calculeze valoarea indicatorilor în conformitate cu următoarea metodologie:

i. Tranzacțiile afectate:

Ca regulă generală, prestatorii de servicii de plată trebuie să înțeleagă drept „tranzacții afectate” toate tranzacțiile interne și transfrontaliere care au fost sau vor fi probabil afectate în mod direct sau indirect de incident și, în special, tranzacțiile care nu au putut fi inițiate sau procesate, cele pentru care conținutul mesajului de plată a fost modificat și cele care au fost comandate în mod fraudulos (fondurile au fost recuperate sau nu) sau în care executarea corespunzătoare este împiedicată sau împiedicată în orice alt mod de incident.

În cazul incidentelor operaționale care afectează capacitatea de a iniția și/sau prelucra tranzacții, prestatorii de servicii de plată trebuie să raporteze numai acele incidente cu o durată mai mare de o oră. Durata incidentului trebuie să fie măsurată din momentul în care are loc incidentul și până în momentul în care activitățile/operațiunile obișnuite au fost recuperate până la nivelul serviciului care a fost furnizat înainte de incident.

În plus, prestatorii de servicii de plată trebuie să înțeleagă nivelul regulat al operațiunilor de plată ca fiind media zilnică anuală a operațiunilor de plată naționale și transfrontaliere efectuate cu aceleași servicii de plată care au fost afectate de incident, luând anul precedent ca perioadă de referință pentru calcule. În cazul în care prestatorii de servicii de plată nu

consideră această cifră ca fiind reprezentativă (de exemplu, din cauza caracterului sezonier), aceștia trebuie să utilizeze în schimb un alt indicator mai reprezentativ și să transmită autorității competente justificarea care stă la baza acestei abordări în câmpul corespunzător din formular (a se vedea anexa).

ii. Utilizatorii serviciilor de plată afectați

Prestatorii de servicii de plată trebuie să înțeleagă drept „utilizatorii serviciilor de plată afectați" toți clienții (fie interni, fie din străinătate, consumatori sau întreprinderi) care au un contract cu prestatorul de servicii de plată afectat care le acordă acces la serviciul de plată afectat și care au suferit sau vor suferi probabil consecințele incidentului. Prestatorii de servicii de plată trebuie să efectueze estimări bazate pe activități anterioare pentru a determina numărul de utilizatori ai serviciilor de plată care ar fi putut utiliza serviciul de plată pe durata incidentului.

În cazul grupurilor, fiecare prestator de servicii de plată trebuie să își ia în considerare numai proprii utilizatori de servicii de plată. În cazul unui prestator de servicii de plată care oferă servicii operaționale altora, respectivul prestator de servicii de plată trebuie să ia în considerare numai proprii utilizatori de servicii de plată (dacă există), iar prestatorii de servicii de plată care primesc aceste servicii operaționale trebuie să evalueze incidentul în raport cu proprii utilizatori de servicii de plată.

În cazul incidentelor operaționale care afectează capacitatea de a iniția și/sau prelucra tranzacții, prestatorii de servicii de plată trebuie să raporteze numai acele incidente care afectează utilizatorii serviciilor de plată cu o durată mai mare de o oră. Durata incidentului trebuie să fie măsurată din momentul în care are loc incidentul și până în momentul în care activitățile/operațiunile obișnuite au fost recuperate până la nivelul serviciului care a fost furnizat înainte de incident.

În plus, prestatorii de servicii de plată trebuie să ia ca număr total de utilizatori de servicii de plată cifra agregată a utilizatorilor de servicii de plată naționali și transfrontalieri care au obligații contractuale cu aceștia în momentul incidentului (sau, alternativ, cea mai recentă cifră disponibilă) și care au acces la serviciul de plată afectat, indiferent de dimensiunea lor sau de faptul că sunt considerați utilizatori activi sau pasivi ai serviciilor de plată.

iii. Încălcarea securității rețelelor sau a sistemelor informatice

Prestatorii de servicii de plată trebuie să stabilească dacă orice acțiune răuvoitoare a compromis disponibilitatea, autenticitatea, integritatea sau confidențialitatea rețelelor sau a sistemelor informatice (inclusiv a datelor) legate de prestarea de servicii de plată.

iv. Indisponibilitatea serviciului

Prestatorii de servicii de plată trebuie să ia în considerare perioada de timp în care orice sarcină, proces sau canal legat de furnizarea de servicii de plată este sau va fi probabil inaccesibil 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 contabilizeze perioada de indisponibilitate a serviciului din momentul în care începe timpul de inactivitate și trebuie

să ia în considerare atât intervalele de timp în care sunt deschise pentru afaceri, astfel cum este necesar pentru executarea serviciilor de plată, cât și orele de închidere și perioadele de întreținere, dacă este relevant și aplicabil. În cazul în care prestatorii de servicii de plată nu sunt în măsură să determine momentul în care a început întreruperea serviciului, aceștia trebuie, în mod excepțional, să contabilizeze perioada de indisponibilitate a serviciului din momentul detectării acesteia.

v. Impactul economic

Prestatorii de servicii de plată trebuie să ia în considerare atât costurile care pot fi legate direct de incident, cât și costurile indirect legate de incident. Printre altele, prestatorii de servicii de plată trebuie să ia în considerare fondurile sau activele expropriate, costurile de înlocuire a hardware-ului sau a software-ului, alte costuri de expertiză criminalistică sau de remediere, comisioanele pentru nerespectarea obligațiilor contractuale, sancțiunile, datoriile externe și pierderile de venituri. În ceea ce privește cheltuielile indirecte, prestatorii de servicii de plată trebuie să ia în considerare numai costurile care sunt deja cunoscute sau foarte susceptibile să se materializeze.

vi. *Nivel ridicat de escaladare internă*

Prestatorii de servicii de plată trebuie să analizeze dacă, ca urmare a impactului asupra serviciilor legate de plăți, organul de conducere, astfel cum este definit în Ghidul ABE privind gestionarea riscurilor TIC și de securitate, a fost sau va fi probabil informat, în conformitate cu orientarea 60 litera (d) din Ghidul ABE privind gestionarea riscurilor TIC și de securitate, cu privire la incident în afara oricărei proceduri de notificare periodică și în mod continuu pe întreaga durată a incidentului. În plus, prestatorii de servicii de plată trebuie să analizeze dacă, în urma impactului incidentului asupra serviciilor legate de plăți, a fost sau este probabil să fie declanșat un mod de criză.

vii. *Alți prestatori de servicii de plată sau alte infrastructuri relevante potențial afectate*

Prestatorii de servicii de plată trebuie să evalueze impactul incidentului asupra pieței financiare, înțeles ca infrastructurile pieței financiare și/sau schemele de plată care o sprijină, precum și restul prestatorilor de servicii de plată. În special, prestatorii de servicii de plată trebuie să evalueze dacă incidentul a fost sau va fi probabil reprodus la alți prestatori de servicii de plată, dacă a afectat sau este probabil să afecteze buna funcționare a infrastructurilor pieței financiare sau dacă a compromis sau ar putea compromite buna funcționare a sistemului financiar în ansamblu. Prestatorii de servicii de plată trebuie să aibă în vedere diverse dimensiuni, cum ar fi dacă software-ul/componenta afectat(ă) este brevetat(ă) sau general disponibil(ă), dacă rețeaua compromisă este internă sau externă sau dacă prestatorul de servicii de plată a încetat sau va înceta probabil să își îndeplinească obligațiile în cadrul infrastructurilor pieței financiare din care face parte.

viii. *Impactul asupra reputației*

Prestatorii de servicii de plată trebuie să ia în considerare nivelul de vizibilitate pe care, după cunoștințele lor, incidentul l-a dobândit sau îl va câștiga probabil pe piață. În special, prestatorii de servicii de plată trebuie să ia în considerare probabilitatea ca incidentul să

cauzeze prejudicii societății ca un bun indicator al potențialului acestuia de a le afecta reputația. Prestatorii de servicii de plată trebuie să ia în considerare dacă i) utilizatorii serviciilor de plată și/sau alți prestatori de servicii de plată s-au plâns de impactul negativ al incidentului, ii) incidentul a afectat un proces vizibil legat de serviciile de plată și, prin urmare, este probabil să primească sau a primit deja acoperire mediatică (având în vedere nu numai mass-media tradițională, cum ar fi ziarele, ci și blogurile, rețelele sociale etc.), iii) impunerea unor obligații contractuale au fost sau ar putea fi omise, ceea ce a dus la publicarea de acțiuni juridice împotriva prestatorului de servicii de plată, iv) nu au fost respectate cerințele de reglementare, ceea ce a dus la impunerea unor măsuri sau sancțiuni de supraveghere care au fost sau vor fi probabil făcute publice sau v) un tip similar de incident a avut loc anterior.

1.4. Prestatorii de servicii de plată trebuie să evalueze un incident stabilind, pentru fiecare criteriu în parte, dacă pragurile relevante din tabelul 1 sunt sau ar putea fi atinse înainte de soluționarea incidentului.

Tabelul 1: Praguri

Criterii	Nivel de impact mai scăzut	Nivel de impact mai ridicat
Tranzacții afectate	>10 % din nivelul obișnuit al tranzacțiilor prestatorului de servicii de plată (în ceea ce privește numărul de tranzacții) **și** durata incidentului > 1 oră* **sau** > 500,000 EUR **și** durata incidentului > 1 oră*	>25 % din nivelul obișnuit al tranzacțiilor prestatorului de servicii de plată (în ceea ce privește numărul de tranzacții) **sau** > 15.000.000 de euro
Utilizatorii serviciilor de plată afectați	> 5.000 **și** durata incidentului > 1 oră* **sau** >10 % din utilizatorii serviciilor de plată ai prestatorului de servicii de plată **și** durata incidentului > 1 oră*	> 50.000 **sau** >25 % din utilizatorii serviciilor de plată ai prestatorului de servicii de plată
Indisponibilitatea serviciului	>2 ore	Nu se aplică
Încălcarea securității rețelelor sau a sistemelor informatice	Da	Nu se aplică
Impactul economic	Nu se aplică	> Max (0,1 % capital de rangul 1** 200.000 de euro) **sau** > 5.000.000 de euro

Nivel ridicat de escaladare internă	Da	Da, și este probabil să se declanșeze un mod de criză (sau un mod echivalent)
Alți prestatori de servicii de plată sau alte infrastructuri relevante potențial afectate	Da	Nu se aplică
Impactul asupra reputației	Da	Nu se aplică

* Pragul privind durata incidentului pentru o perioadă mai mare de o oră se aplică numai incidentelor operaționale care afectează capacitatea prestatorului de servicii de plată de a iniția și/sau prelucra tranzacții.

**Capital de rangul 1, astfel cum este definit 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 firmele de investiții și de modificare a Regulamentul (UE) nr. 648/2012.

1.5. Prestatorii de servicii de plată trebuie să recurgă la estimări în cazul în care nu dispun de date reale pentru a-și susține aprecierea cu privire la măsura în care un anumit prag este sau ar putea fi atins înainte de soluționarea incidentului (de exemplu, acest lucru s-ar putea întâmpla în faza de investigare inițială).

1.6. Prestatorii de servicii de plată trebuie să efectueze această evaluare în mod continuu pe durata de viață a incidentului, astfel încât să identifice orice posibilă schimbare a statutului, fie în sens ascendent (de la non-major la major), fie descendent (de la major la non-major). Orice reclasificare a incidentului de la major la non-major trebuie comunicată autorității competente în conformitate cu cerința de la orientarea 2.21 și fără întârzieri nejustificate.

Orientarea 2: Procesul de notificare

2.1. Prestatorii de servicii de plată trebuie să colecteze toate informațiile relevante, să elaboreze un raport privind incidentul prin completarea modelului din anexă și să îl transmită autorității competente din statul membru de origine. Prestatorii de servicii de plată trebuie să completeze toate câmpurile formularului, urmând instrucțiunile furnizate în anexă.

2.2. Prestatorii de servicii de plată trebuie să utilizeze același model atunci când prezintă rapoartele inițiale, intermediare și finale referitoare la același incident. Prin urmare, prestatorii de servicii de plată trebuie să completeze un formular unic într-o manieră incrementală și să actualizeze, după caz, informațiile furnizate împreună cu rapoartele anterioare.

2.3. Prestatorii de servicii de plată trebuie să prezinte în continuare 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 se prevede la articolul 96 alineatul (1) al doilea paragraf din DSP2, de îndată ce acestea sunt disponibile.

2.4. Prestatorii de servicii de plată trebuie, la cererea autorității competente din statul membru de origine, să furnizeze orice documente suplimentare care completează informațiile

transmise cu modelul standardizat. Prestatorii de servicii de plată trebuie să dea curs oricăror cereri din partea autorității competente din statul membru de origine de a furniza informații suplimentare sau clarificări cu privire la documentația deja depusă.

2.5. Orice informații suplimentare conținute în documentele furnizate de prestatorii de servicii de plată autorității competente, fie la inițiativa prestatorului de servicii de plată, fie la cererea autorității competente în conformitate cu orientarea 2.4, trebuie reflectate de prestatorul de servicii de plată în modelul prevăzut în orientarea 2.1.

2.6. Prestatorii de servicii de plată trebuie să păstreze în permanență confidențialitatea și integritatea informațiilor partajate și autentificarea corespunzătoare a acestora față de autoritatea competentă din statul lor membru de origine.

Raportul inițial

2.7. Prestatorii de servicii de plată trebuie să prezinte un prim raport autorității competente din statul membru de origine după ce un incident operațional sau de securitate a fost clasificat ca fiind major. Autoritățile competente trebuie să confirme primirea raportului inițial fără întârzieri nejustificate și să atribuie un cod de referință unic care să identifice fără echivoc incidentul. Prestatorii de servicii de plată trebuie să indice acest cod de referință atunci când prezintă o actualizare fie a raportului inițial, fie a rapoartelor intermediare și finale referitoare la același incident, cu excepția cazului în care rapoartele intermediare și finale sunt prezentate împreună cu raportul inițial.

2.8. Prestatorii de servicii de plată trebuie să transmită raportul inițial autorității competente în termen de patru ore de la momentul în care incidentul operațional sau de securitate a fost clasificat ca fiind major. În cazul în care canalele de raportare ale autorității competente sunt cunoscute ca nefiind disponibile sau exploatate la momentul respectiv, prestatorii de servicii de plată trebuie să trimită raportul inițial de îndată ce canalele devin din nou disponibile/operaționale.

2.9. Prestatorii de servicii de plată trebuie să clasifice incidentul în conformitate cu orientările 1.1 și 1.4 în timp util după detectarea incidentului, dar nu mai târziu de 24 de ore de la detectarea incidentului și fără întârzieri nejustificate după ce informațiile necesare pentru clasificarea incidentului sunt puse la dispoziția prestatorului de servicii de plată. În cazul în care este nevoie de mai mult timp pentru a clasifica incidentul, prestatorii de servicii de plată trebuie să explice în raportul inițial prezentat autorității competente motivele.

2.10. Prestatorii de servicii de plată trebuie, de asemenea, să prezinte un raport inițial autorității competente din statul membru de origine atunci când un incident anterior, altul decât cel major, a fost reclasificat ca incident major. În acest caz particular, prestatorii de servicii de plată trebuie să trimită raportul inițial autorității competente imediat după identificarea schimbării statutului sau, în cazul în care canalele de raportare ale autorității competente nu

sunt cunoscute ca fiind disponibile sau exploatate la momentul respectiv, de îndată ce devin din nou disponibile/operaționale.

2.11. Prestatorii de servicii de plată trebuie să furnizeze informații la nivel central în rapoartele lor inițiale (și anume, secțiunea A din model), prezentând astfel unele caracteristici de bază ale incidentului și consecințele preconizate ale acestuia, pe baza informațiilor disponibile imediat după clasificarea incidentului ca fiind major. Prestatorii de servicii de plată trebuie să recurgă la estimări atunci când datele reale nu sunt disponibile.

Raportul intermediar

2.12. Prestatorii de servicii de plată trebuie să prezinte raportul intermediar atunci când activitățile curente au fost recuperate și activitățile sunt din nou normale, informând autoritatea competentă cu privire la această situație. Prestatorii de servicii de plată trebuie să considere că activitatea comercială este din nou normală atunci când activitatea/operațiunile sunt restabilite cu același nivel de servicii/condiții ca cele definite de prestatorul de servicii de plată sau stabilite extern printr-un acord privind nivelul serviciilor (timpi de procesare, capacitate, cerințe de securitate etc.) și atunci când nu mai există măsuri de contingență. Raportul intermediar trebuie să conțină o descriere mai detaliată a incidentului și a consecințelor acestuia (secțiunea B din model).

2.13. În cazul în care activitățile obișnuite nu au fost încă recuperate, prestatorii de servicii de plată trebuie să prezinte autorității competente un raport intermediar în termen de trei zile lucrătoare de la prezentarea raportului inițial.

2.14. Prestatorii de servicii de plată trebuie să actualizeze informațiile deja furnizate în secțiunile A și B din model atunci când iau cunoștință de modificări semnificative de la transmiterea raportului anterior (de exemplu, dacă incidentul a escaladat sau s-a diminuat, dacă au fost identificate noi cauze sau dacă s-au luat măsuri pentru a remedia problema). Aceasta include cazul în care incidentul nu a fost soluționat în termen de trei zile lucrătoare, ceea ce ar obliga prestatorii de servicii de plată să prezinte un raport intermediar suplimentar. În orice caz, prestatorii de servicii de plată trebuie să prezinte un raport intermediar suplimentar la cererea autorității competente din statul membru de origine.

2.15. Ca și în cazul rapoartelor inițiale, atunci când nu sunt disponibile date reale, prestatorii de servicii de plată trebuie să utilizeze estimări.

2.16. În cazul în care activitatea este din nou normală înainte de trecerea a patru ore de la clasificarea incidentului ca fiind major, prestatorii de servicii de plată trebuie să urmărească depunerea simultană atât a raportului inițial, cât și a celui intermediar (și anume completarea secțiunilor A și B din model) în termenul de patru ore.

Raportul final

2.17. Prestatorii de servicii de plată trebuie să prezinte un raport final atunci când a avut loc analiza cauzelor principale (indiferent dacă au fost deja puse în aplicare măsuri de atenuare sau dacă a fost identificată cauza principală finală) și atunci când există cifre reale disponibile pentru a înlocui orice estimări potențiale.

2.18. Prestatorii de servicii de plată trebuie să transmită raportul final autorității competente în termen de cel mult 20 zile lucrătoare de la data la care activitatea este considerată normală. Prestatorii de servicii de plată care au nevoie de o prelungire a acestui termen (de exemplu, atunci când nu există cifre reale privind impactul disponibil sau cauzele profunde nu au fost încă identificate) trebuie să contacteze autoritatea competentă înainte de trecerea timpului și să furnizeze o justificare adecvată a întârzierii, precum și o nouă dată estimată pentru raportul final.

2.19. În cazul în care prestatorii de servicii de plată pot furniza toate informațiile solicitate în raportul final (și anume, secțiunea C din model) în intervalul de patru ore, deoarece incidentul a fost clasificat ca fiind major, aceștia trebuie să vizeze furnizarea împreună a informațiilor referitoare la rapoartele inițiale, intermediare și finale.

2.20. Prestatorii de servicii de plată trebuie să urmărească să includă în rapoartele lor finale informații complete, mai exact: i) cifre reale privind impactul în locul estimărilor (precum și orice altă actualizare necesară în secțiunile A și B din model) și ii) secțiunea C a modelului, care include, dacă este deja cunoscută, cauza principală și un rezumat al măsurilor adoptate sau planificate a fi adoptate pentru a elimina problema și pentru a preveni repetarea acesteia în viitor.

2.21. Prestatorii de servicii de plată trebuie, de asemenea, să trimită un raport final atunci când, ca urmare a evaluării continue a incidentului, constată că un incident deja raportat nu mai îndeplinește criteriile pentru a fi considerat major și nu este de așteptat să le îndeplinească înainte de soluționarea incidentului. În acest caz, prestatorii de servicii de plată trebuie să trimită raportul final de îndată ce se constată această situație și, în orice caz, în termenul de depunere a următorului raport. În această situație specială, în loc să completeze secțiunea C din model, prestatorii de servicii de plată trebuie să bifeze caseta „incident reclasificat ca nefiind major” și să ofere o explicație a motivelor care justifică această reclasificare.

Orientarea 3: Raportare delegată și consolidată

3.1. În cazul în care autoritatea competentă permite acest lucru, prestatorii de servicii de plată care doresc să delege obligații de raportare în temeiul DSP2 unei părți terțe trebuie să informeze autoritatea competentă din statul membru de origine și să asigure îndeplinirea următoarelor condiții:

a. Contractul formal sau, după caz, mecanismele interne existente în cadrul unui grup care stau la baza raportării delegate dintre prestatorul de servicii de plată și terț definește fără ambiguitate repartizarea responsabilităților tuturor părților. În special, aceasta precizează în mod clar că, indiferent de posibila delegare a obligațiilor de raportare, prestatorul de servicii de plată afectat rămâne pe deplin responsabil și responsabil pentru îndeplinirea cerințelor prevăzute la articolul 96 din DSP2 și pentru conținutul informațiilor furnizate autorității competente din statul membru de origine.

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

   i. articolul 19 alineatul (6) din DSP 2 în ceea ce privește instituțiile de plată și instituțiile emitente de monedă electronică, aplicabil mutatis mutandis în conformitate cu articolul 3 din Directiva 2009/110/CE; sau

   ii. Ghidul ABE privind acordurile de externalizare (EBA/GL/2019/02) în legătură cu toți prestatorii de servicii de plată.

c. Informațiile sunt transmise autorității competente din statul membru de origine în prealabil și, în orice caz, în conformitate cu orice termene și proceduri stabilite de autoritatea competentă, după caz.

d. Confidențialitatea datelor sensibile și calitatea, coerența, integritatea și fiabilitatea informațiilor care trebuie furnizate autorității competente sunt asigurate în mod corespunzător.

3.2. Prestatorii de servicii de plată care doresc să permită părții terțe desemnate să îndeplinească obligațiile de raportare în mod consolidat (și anume, prin prezentarea unui singur raport referitor 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 furnizeze informațiile de contact incluse la rubrica „PSP afectat” în model și să se asigure că sunt îndeplinite următoarele condiții:

a. să includă această dispoziție în contractul care stă la baza raportării delegate;

b. să condiționeze raportarea consolidată de faptul că incidentul este cauzat de o perturbare a serviciilor furnizate de partea terță;

c. să limiteze raportarea consolidată la prestatorii de servicii de plată stabiliți în același stat membru;

d. să furnizeze o listă a tuturor prestatorilor de servicii de plată afectați de incident;

e. să se asigure că partea terță evaluează importanța incidentului pentru fiecare prestator de servicii de plată afectat și include în raportul consolidat numai prestatorii de servicii de plată pentru care incidentul este clasificat ca fiind major; în plus, să se asigure că, în cazul în care există îndoieli, un prestator de servicii de plată este inclus în raportul consolidat atât timp cât nu există dovezi care să confirme contrariul;

f. să se asigure că, atunci când există câmpuri ale modelului în care nu este posibil un răspuns comun (de exemplu, secțiunile B2, B4 sau C3 din formular), terțul fie i) le completează individual pentru fiecare prestator de servicii de plată afectat, specificând mai în detaliu identitatea fiecărui prestator de servicii de plată la care se referă informațiile, fie ii) utilizează valorile cumulate, astfel cum au fost observate sau estimate pentru prestatorii de servicii de plată;

g. terțul informează în permanență prestatorul de servicii de plată cu privire la toate informațiile relevante referitoare la incident și la toate interacțiunile pe care le poate avea cu autoritatea competentă, precum și cu privire la conținutul acestuia, dar numai în măsura posibilului, astfel încât să se evite orice încălcare 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 că acordul de externalizare nu îndeplinește cerințele menționate 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, respectând termenele și procedurile stabilite de acesta din urmă. Prestatorii de servicii de plată trebuie, de asemenea, să informeze 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 în mod semnificativ obligațiile de raportare fără a recurge la asistență externă ori de câte ori partea terță desemnată nu informează 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. Prestatorii de servicii de plată trebuie, de asemenea, să se asigure că un incident nu este raportat de două ori, individual de către prestatorul de servicii de plată respectiv și încă o dată de către terț.

3.6. Prestatorii de servicii de plată trebuie să se asigure că, în situația în care un incident este cauzat de o perturbare a serviciilor furnizate de un prestator de servicii tehnice (sau de o infrastructură) care afectează mai mulți prestatori de servicii de plată, raportarea delegată

se referă la datele individuale ale prestatorului de servicii de plată (cu excepția raportării consolidate).

Orientarea 4: Politica operațională și de securitate

4.1. Prestatorii de servicii de plată trebuie să se asigure că politica lor operațională și de securitate generală definește în mod clar toate responsabilitățile de raportare a incidentelor în temeiul DSP2, precum și procesele puse în aplicare pentru a îndeplini cerințele definite în prezentul ghid.

5. Orientări adresate autorităților competente cu privire la criteriile de evaluare a relevanței incidentului și la detaliile rapoartelor privind incidentul care urmează să fie comunicate 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 propriilor opinii ale experților și utilizând următoarele criterii ca indicatori principali ai importanței incidentului respectiv:

a. Cauzele incidentului țin de competența de reglementare a celeilalte autorități naționale (adică de domeniul lor de competență).
b. Consecințele incidentului au un impact asupra obiectivelor unei alte autorități naționale (de exemplu, protejarea stabilității financiare).
c. Incidentul afectează sau ar putea afecta utilizatorii serviciilor de plată la scară largă.
d. Este probabil ca incidentul să primească sau să fi beneficiat de o largă acoperire mediatică.

5.2. Autoritățile competente din statul membru de origine trebuie să efectueze această evaluare în mod continuu pe durata de viață a incidentului, astfel încât să identifice orice posibilă modificare care ar putea face ca un incident care nu a fost considerat anterior ca atare să fie relevant.

Orientarea 6: Informații care trebuie partajate

6.1. Fără a aduce atingere oricărei alte cerințe legale de a face schimb de informații legate de incidente cu alte autorități naționale, autoritățile competente trebuie să furnizeze informații cu privire la incidentele operaționale sau de securitate majore autorităților naționale relevante identificate în urma aplicării orientării 5.1, cel puțin la momentul primirii raportului inițial (sau, alternativ, a raportului care a determinat schimbul de informații) și atunci când sunt notificate că întreprinderea este din nou normală (și anume, raportul intermediar).

6.2. Autoritățile competente trebuie să transmită autorităților naționale relevante informațiile necesare pentru a oferi o imagine clară a ceea ce s-a întâmplat și a consecințelor potențiale.

În acest scop, acestea trebuie să furnizeze cel puțin informațiile furnizate de prestatorul de servicii de plată în următoarele câmpuri ale modelului (fie în raportul inițial, fie în raportul intermediar):

- Data și ora clasificării incidentului ca fiind major.
- Data și ora detectării incidentului.
- Data și ora declanșării incidentului.
- Data și ora la care incidentul a fost restabilit sau se preconizează că va fi restabilit.
- Scurtă descriere a incidentului (inclusiv părți nesensibile ale descrierii detaliate).
- Scurtă descriere a măsurilor luate sau planificate pentru a se redresa în urma incidentului.
- Descrierea modului în care incidentul ar putea afecta alți prestatori de servicii de plată și/sau alte infrastructuri.
- Descrierea (dacă există) a acoperirii mediatice.
- Cauza incidentului.

6.3. Autoritățile competente trebuie să efectueze anonimizarea corespunzătoare, după caz, și să excludă orice informații care ar putea face obiectul unor restricții privind confidențialitatea sau proprietatea intelectuală înainte de a face schimb de informații legate de incidente cu autoritățile naționale relevante. Cu toate acestea, autoritățile competente trebuie să furnizeze autorităților naționale relevante numele și adresa prestatorului de servicii de plată care raportează atunci când autoritățile naționale respective pot garanta că informațiile vor fi tratate în mod confidențial.

6.4. Autoritățile competente trebuie să păstreze în permanență confidențialitatea și integritatea informațiilor stocate și partajate, precum și autentificarea corespunzătoare a acestora cu autoritățile naționale relevante. În special, autoritățile competente trebuie să trateze toate informațiile primite în temeiul prezentului ghid în conformitate cu obligațiile privind secretul profesional prevăzute în DSP2, fără a aduce atingere legislației aplicabile a Uniunii și cerințelor naționale.

6. Orientări adresate autorităților competente cu privire la criteriile de evaluare a detaliilor relevante ale rapoartelor privind incidentele care urmează să fie comunicate ABE și BCE, precum și cu privire la formatul și procedurile de comunicare a acestora

Orientarea 7: Informații care trebuie partajate

7.1. Autoritățile competente trebuie să furnizeze întotdeauna ABE și BCE toate rapoartele primite de la prestatorii de servicii de plată afectați de un incident operațional sau de securitate major (sau în numele acestora), utilizând un fișier standardizat pus la dispoziție pe site-ul ABE.

Orientarea 8: Comunicare

8.1. Autoritățile competente trebuie să păstreze în permanență confidențialitatea și integritatea informațiilor stocate și partajate, precum și autentificarea corespunzătoare a acestora cu ABE și BCE. În special, autoritățile competente trebuie să trateze toate informațiile primite în temeiul prezentului ghid în conformitate cu obligațiile privind secretul profesional prevăzute în DSP2, fără a aduce atingere legislației aplicabile a Uniunii și cerințelor naționale.

8.2. Pentru a evita întârzierile în transmiterea informațiilor conexe către ABE/BCE și pentru a contribui la reducerea la minimum a riscurilor de perturbări operaționale, autoritățile competente trebuie să sprijine mijloacele adecvate de comunicare.

Anexă — Model de raportare pentru prestatorii de servicii de plată

Raport inițial

Raport inițial	în termen de 4 ore de la clasificarea incidentului ca fiind major		Resetarea selecțiilor verticale
Data raportului *(ZZ/LL/AAAA)*		Ora *(HH:MM)*	
Cod de referință incident			

A – Raport inițial					
A 1 – DETALII GENERALE					
Tip de raport					
Tip de raport					
Prestator de servicii de plată (PSP) afectat					
Denumirea PSP					
Numărul național de identificare al PSP					
Conducătorul grupului, dacă este cazul					
Țara/țările afectate de incident	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ LI ☐ GR ☐ RU ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NU ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Persoana de contact principală		E-mail		Telefon	
Persoana de contact secundară		E-mail		Telefon	
Entitatea de raportare (completați această secțiune dacă entitatea de raportare nu este PSP afectat, în cazul raportării delegate)					
Denumirea entității raportoare					
Număr național de identificare					
Persoana de contact principală		E-mail		Telefon	
Persoana de contact secundară		E-mail		Telefon	
A 2 - DETECTAREA ȘI CLASIFICAREA INCIDENTELOR					
Data și ora detectării incidentului *(ZZ/LL/AAAA, HH:MM)*					
Data și ora clasificării incidentului: *(ZZ/LL/AAAA, HH:MM)*					
Incidentul a fost depistat de către		Pentru „Altele", vă rugăm specificați:			
Tip de incident					
Criterii care declanșează raportul privind incidentul major	☐ Tranzacții afectate	☐ Utilizatorii serviciilor de plată afectați	☐ Indisponibilitatea serviciului	☐ Încălcarea securității rețelelor sau a sistemelor informatice	☐ Impactul economic	☐ Nivel ridicat de escaladare internă	☐ Alți PSP sau alte infrastructuri relevante care ar putea fi afectate	☐ Impactul asupra reputației
O scurtă descriere generală a incidentului								
Impactul în alte state membre ale UE, dacă este cazul								
Raportarea către alte autorități		Dacă da, vă rugăm specificați:						
Motivele transmiterii cu întârziere a raportului inițial								

Raport intermediar

Raport privind un incident major

Raport intermediar	maximum 3 zile lucrătoare de la prezentarea raportului inițial	Resetarea selecțiilor verticale

Data raportului *(ZZ/LL/AAAA)* | Ora *(HH:MM)*

Cod de referință incident

B - Raport intermediar

B 1 - DETALII GENERALE

O descriere mai detaliată a incidentului:		
Care este problema specifică?		
Cum a început incidentul?		
Cum s-a desfășurat?		
Care sunt consecințele (în special pentru utilizatorii serviciilor de plată)?		
Incidentul a fost comunicat utilizatorilor serviciilor de plată?		Dacă da, vă rugăm specificați:
A fost legat de un incident(incidente) anterior(anterioare)?		Dacă da, vă rugăm specificați:
Au fost afectați sau implicați alți prestatori de servicii/alte părți terțe?		Dacă da, vă rugăm specificați:
A început gestionarea crizei (internă și/sau externă)?		Dacă da, vă rugăm specificați:
Data și ora declanșării incidentului (dacă au fost deja identificate) *(ZZ/LL/AAAA, HH:MM)*		
Data și ora la care incidentul a fost restabilit sau se preconizează că va fi restabilit *(ZZ/LL/AAAA, HH:MM)*		
Segmente funcționale afectate	☐ Autentificare/autorizare ☐ Decontare directă ☐ Comunicare ☐ Decontare indirectă ☐ Compensare ☐ Altele	Pentru „Altele", vă rugăm specificați:
Modificări aduse rapoartelor anterioare		

B 2 - CLASIFICAREA INCIDENTELOR/INFORMAȚII PRIVIND INCIDENTUL

Tranzacțiile afectate [2]	Nivel de impact Numărul tranzacțiilor afectate Ca % din numărul obișnuit de operațiuni Valoarea operațiunilor afectate în EUR Durata incidentului (se aplică numai incidentelor operaționale) Observații:	
Utilizatori ai serviciilor de plată afectați [3]	Nivel de impact Numărul utilizatorilor serviciilor de plată afectați Ca % din totalul utilizatorilor serviciilor de plată	
Încălcarea securității rețelelor sau a sistemelor informatice		Descrierea modului în care rețeaua sau sistemele informatice au fost afectate
Indisponibilitatea serviciului	Perioada totală de indisponibilitate a serviciului:	Zile: Ore: Proces-verbal:
Impactul economic	Nivel de impact Cheltuieli directe în EUR Cheltuieli indirecte în EUR	
Nivel ridicat de escaladare internă		Descrieți nivelul de escaladare internă a incidentului, indicând dacă acesta a declanșat sau este susceptibil de a declanșa o stare de criză (sau o stare echivalentă) și, în acest caz, vă rugăm să descrieți
Alți PSP sau alte infrastructuri relevante care ar putea fi afectate		Descrieți modul în care acest incident ar putea afecta alți PSP și/sau alte infrastructuri
Impactul asupra reputației		Descrieți modul în care incidentul ar putea afecta reputația PSP (de exemplu, acoperirea în mass-media, o posibilă încălcare a legii sau a normelor de reglementare...)

B 3 - DESCRIEREA INCIDENTULUI

Tip de incident		
Cauza incidentului	☐ În curs de investigare ☐ Acțiune răuvoitoare ☐ Eroare de proces ☐ Eroare de sistem ☐ Eroare umană ☐ Evenimente externe ☐ Altele	Pentru „Altele", vă rugăm specificați:
Incidentul v-a afectat în mod direct sau indirect, prin intermediul unui prestator de servicii?		Dacă v-a afectat indirect, vă rugăm să precizați numele prestatorului serviciului:

B 4 – IMPACTUL INCIDENTULUI

Impact global	☐ Integritate ☐ Disponibilitate	☐ Confidențialitate ☐ Autenticitate	
Canale comerciale afectate	☐ Sucursale ☐ Servicii bancare electronice ☐ Comerț electronic	☐ Servicii bancare prin telefon ☐ Servicii bancare pe mobil ☐ Bancomate	☐ Punct de desfacere ☐ Altele
	Pentru „Altele", vă rugăm specificați:		
Servicii de plată afectate	☐ Plasare de numerar într-un cont de plăți ☐ Retragere de numerar dintr-un cont de plăți ☐ Operațiuni necesare pentru operarea unui cont de plăți ☐ Dobândirea de instrumente de plată	☐ Transferuri de credit ☐ Debitare directă ☐ Plăți cu card ☐ Emiterea de instrumente de plată	☐ Remitere de bani ☐ Servicii de inițiere ☐ Servicii de informare cu privire la conturi

B 5 - ATENUAREA INCIDENTULUI

Ce acțiuni/măsuri au fost luate până acum sau sunt prevăzute pentru a redresa situația după incident?		
Planul de continuitate a activității și/sau planul de recuperare în caz de dezastru au fost activate?		
Dacă da, când? *(ZZ/LL/AAAA, HH:MM)*		
Dacă da, vă rugăm să oferiți o descriere		

Raport final

Raport privind un incident major

Vă rugăm selectați tipul raportului:	În termen de 20 zile lucrătoare de la prezentarea raportului intermediar
Vă rugăm descrieți: (aplicabil pentru incidente reclasificate ca nefiind majore)	

Resetarea selecțiilor verticale

Data raportului *(ZZ/LL/AAAA)*	Ora *(HH:MM)*
Cod de referință incident	

C – Raport final

Dacă nu a fost transmis niciun raport intermediar, vă rugăm să completați și secțiunea B

C 1 - DETALII GENERALE

Actualizarea informațiilor din raportul inițial și din raportul(rapoartele) intermediar(e)	
Modificări aduse rapoartelor anterioare	
Orice alte informații pertinente	
Sunt în vigoare toate controalele inițiale? Dacă nu, specificați controalele și perioada suplimentară necesară pentru restabilirea lor	

C 2 – ANALIZA CAUZEI FUNDAMENTALE ȘI ACȚIUNI DE URMĂRIRE

Care a fost cauza fundamentală (dacă este deja cunoscută)?	☐ Acțiune răuvoitoare ☐ Eroare de proces ☐ Eroare de sistem ☐ Eroare umană ☐ Eveniment extern ☐ Altele
Vă rugăm, specificați:	☐ Cod rău intenționat ☐ Culegerea de informații ☐ Intruziuni ☐ Atac distribuit/refuzat de serviciu (D/DoS) ☐ Acțiuni interne deliberate ☐ Deteriorare fizică externă deliberată ☐ Securitatea conținutului informațiilor ☐ Acțiuni frauduloase ☐ Altele ☐ Monitorizare și control deficitare ☐ Probleme de comunicare ☐ Operațiuni ☐ Gestionarea inadecvată a modificărilor ☐ Insuficiența procedurilor și a documentației interne ☐ Aspecte legate de recuperare ☐ Altele ☐ Defecțiune la ☐ Defecțiune la ☐ Probleme cu ☐ Defecțiune la software/aplicație ☐ Daune fizice ☐ Altele ☐ Neintenționate ☐ Lipsă de acțiune ☐ Resurse insuficiente ☐ Altele ☐ Defecțiune la un furnizor/prestator de servicii tehnice ☐ Forță majoră ☐ Altele Pentru „Altele", vă rugăm specificați:
Alte informații relevante privind cauza principală	
Acțiuni corective/măsuri de remediere principale luate sau prevăzute pentru prevenirea reapariției incidentului în viitor, dacă sunt deja cunoscute	

C 3 - INFORMAȚII SUPLIMENTARE

Incidentul a fost comunicat altor PSP în scop informativ?	În caz afirmativ, vă rugăm să furnizați detalii:
Au fost inițiate acțiuni în justiție împotriva PSP?	În caz afirmativ, vă rugăm să furnizați detalii:
Evaluarea eficacității acțiunii întreprinse	Vă rugăm să furnizați detalii:

INSTRUCȚIUNI PENTRU COMPLETAREA MODELULUI

Prestatorii de servicii de plată (PSP-uri) 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. PSP trebuie să utilizeze același model atunci când prezintă rapoartele inițiale, intermediare și finale referitoare la același incident. Toate câmpurile sunt obligatorii, cu excepția cazului în care se specifică altfel în mod clar.

Titlu

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

Raport intermediar: conține o descriere mai detaliată a incidentului și a consecințelor acestuia. Este o actualizare a raportului inițial (și, după caz, a unui raport intermediar anterior) cu privire la același incident.

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

Incident reclasificat ca nefiind major: incidentul nu mai îndeplinește criteriile pentru a fi considerat major și nu este de așteptat să le îndeplinească înainte de a fi soluționat. PSP trebuie să explice motivele acestei reclasificări.

Data și ora raportului: data și ora exacte de transmitere a raportului către autoritatea competentă.

Codul de referință al incidentului (aplicabil pentru rapoartele intermediare și finale, precum și pentru actualizările raportului inițial): codul de referință emis de autoritatea competentă la momentul raportului inițial pentru a identifica fără echivoc incidentul. Fiecare autoritate competentă trebuie să includă ca prefix codul ISO de[2] 2 cifre al statului membru respectiv.

A - Raport inițial

A 1 - Detalii generale

Tipul raportului:

Individual: raportul se referă la un singur PSP.

Consolidat: raportul se referă la mai mulți PSP din același stat membru care sunt afectați de același incident major operațional sau de securitate, care utilizează raportarea consolidată. Câmpurile de la rubrica „PSP afectați” trebuie lăsate necompletate (cu excepția rubricii „Țara/țările afectate de incident”), iar o listă a PSP incluși în raport trebuie furnizată prin completarea tabelului corespunzător (raport consolidat — Lista PSP).

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

Nume PSP: denumirea completă a PSP care face obiectul procedurii de raportare, astfel cum apare în registrul național oficial al PSP aplicabil.

Numărul național de identificare al PSP: numărul național unic de identificare utilizat de autoritatea competentă a statului membru de origine în registrul său național pentru identificarea fără echivoc a PSP.

Șef de grup: în cazul grupurilor de entități, astfel cum sunt definite la articolul 4 alineatul (40) din DSP2, vă rugăm să indicați denumirea entității principale.

Țara/țările afectată/afectate de incident: țara sau țările în care s-a materializat impactul incidentului (de exemplu, sunt afectate mai multe ramuri ale unui PSP situat în țări diferite), indiferent de gravitatea incidentului în cealaltă țară/celelalte țări. Acesta poate fi sau nu același cu statul membru de origine.

[2] A se vedea codurile de țară alfa-2 din ISO-3166 la adresa https://www.iso.org/iso-3166-country-codes.html

Persoana de contact principală: numele și prenumele persoanei responsabile cu raportarea incidentului sau, în cazul în care un al treilea prestator de servicii raportează în numele PSP afectat, numele și prenumele persoanei responsabile cu gestionarea incidentelor/departamentul de gestionare a riscurilor sau cu o zonă 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 vorba fie de o adresă de e-mail personală, fie de o adresă de e-mail a întreprinderii.

Telefon: numărul de telefon prin care ar putea fi soluționate eventualele solicitări de clarificări suplimentare, dacă este necesar. Poate fi vorba fie de un număr de telefon personal, fie de un număr de telefon al întreprinderii.

Persoana de contact secundară: numele și prenumele unei persoane alternative care ar putea fi contactată de autoritatea competentă pentru a solicita informații cu privire la un incident atunci când persoana principală de contact nu este disponibilă. În cazul unui al treilea prestator de servicii care raportează în numele PSP afectat, numele și prenumele unei persoane alternative din departamentul de gestionare a incidentelor/de risc sau din zona 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 vorba fie de o adresă de e-mail personală, fie de o adresă de e-mail a întreprinderii.

Telefon: numărul de telefon al persoanei de contact alternative, prin intermediul căruia ar putea fi adresate eventualele solicitări de clarificări suplimentare, dacă este necesar. Poate fi vorba fie de un număr de telefon personal, fie de un număr de telefon al întreprinderii.

Entitatea raportoare: această secțiune trebuie completată în cazul în care o parte terță îndeplinește obligațiile de raportare în numele PSP afectat, dacă este cazul.

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

Numărul național unic de identificare: numărul național unic de identificare utilizat în țara în care se află partea terță pentru a identifica fără echivoc entitatea care raportează incidentul. În cazul în care partea terță raportoare este un PSP, numărul național de identificare trebuie să fie numărul național unic de identificare al PSP utilizat de autoritatea competentă a statului membru de origine în registrul său național.

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 vorba fie de o adresă de e-mail personală, fie de o adresă de e-mail a întreprinderii.

Telefon: numărul de telefon prin care ar putea fi soluționate eventualele solicitări de clarificări suplimentare, dacă este necesar. Poate fi vorba fie de un număr de telefon personal, fie de un număr de telefon al întreprinderii.

Persoană de contact secundară: numele și prenumele unei persoane alternative din cadrul entității care raportează incidentul care ar putea fi contactată de 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 vorba fie de o adresă de e-mail personală, fie de o adresă de e-mail a întreprinderii.

Telefon: numărul de telefon al persoanei de contact alternative, prin intermediul căruia ar putea fi adresate eventualele solicitări de clarificări suplimentare, dacă este necesar. Poate fi vorba fie de un număr de telefon personal, fie de un număr de telefon al întreprinderii.

A 2 - Detectarea și clasificarea incidentelor

Data și ora detectării incidentului: data și ora la care incidentul a fost identificat pentru prima dată.

Data și ora clasificării incidentului: data și ora la care incidentul de securitate sau operațional a fost clasificat ca fiind major.

Incident depistat de către: indicați dacă incidentul a fost detectat de un utilizator al serviciilor de plată, în cadrul PSP (de exemplu, funcția de audit intern) sau de o altă parte externă (de exemplu, prestatorul de servicii). Dacă nu ați făcut acest lucru, vă rugăm să furnizați o explicație în câmpul corespunzător.

Tipul incidentului: indicați dacă, din informațiile pe care le dețineți și dacă informațiile sunt disponibile, este vorba despre un incident operațional sau despre un incident de securitate.

> **Operațional:** incident generat de procese, persoane și sisteme inadecvate sau defecte sau evenimente de forță majoră care afectează integritatea, disponibilitatea, confidențialitatea și/sau autenticitatea serviciilor legate de plată.
>
> **Securitate:** accesul, utilizarea, divulgarea, perturbarea, modificarea sau distrugerea neautorizată a activelor PSP care afectează integritatea, disponibilitatea, confidențialitatea și/sau autenticitatea serviciilor legate de plată. Acest lucru se poate întâmpla, printre altele, atunci când PSP se confruntă cu o încălcare a securității rețelelor sau a sistemelor informatice.

Criterii care declanșează raportul privind incidentul major: vă rugăm să indicați care dintre criterii a declanșat raportul privind incidentul major. Pot fi selectate mai multe opțiuni între criterii: tranzacțiile afectate, utilizatorii serviciilor de plată afectați, indisponibilitatea serviciilor, încălcarea securității rețelelor sau a sistemelor informatice, impactul economic, nivelul ridicat de escaladare internă, alți prestatori de servicii de plată sau alte infrastructurile relevante care ar putea fi afectate și/sau impactul asupra reputației.

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.

Impactul în alte state membre ale UE, dacă este cazul: vă rugăm să explicați pe scurt impactul pe care l-a avut incidentul într-un alt stat membru al UE (de exemplu, asupra utilizatorilor serviciilor de plată, a prestatorilor de servicii de plată și/sau a infrastructurilor de plată). Dacă este fezabil, în termenele de raportare aplicabile, vă rugăm să furnizați o traducere în limba engleză.

Raportarea către alte autorități:: vă rugăm să indicați dacă incidentul a fost/va fi raportat altor autorități în temeiul unor cadre separate de raportare a incidentelor, dacă acestea sunt cunoscute la momentul raportării. Dacă da, vă rugăm să precizați autoritățile respective.

Motivele transmiterii cu întârziere a raportului inițial: vă rugăm să explicați motivele pentru care ați solicitat mai mult de 24 ore pentru a clasifica incidentul.

B Raport intermediar

B 1 – Detalii generale

O descriere mai detaliată a incidentului: vă rugăm să descrieți principalele caracteristici ale incidentului, care să acopere cel puțin informațiile privind problema specifică și contextul aferent, descrierea modului în care a început și a evoluat incidentul, precum și consecințele acestuia, în special pentru utilizatorii serviciilor de plată etc. Vă rugăm să furnizați, de asemenea, informații cu privire la comunicarea cu utilizatorii serviciilor de plată, dacă este cazul.

A fost legat de un incident (incidente) anterior (anterioare)?: vă rugăm să indicați dacă incidentul are sau nu legătură cu incidente anterioare, dacă aceste informații sunt disponibile. Dacă incidentul a fost legat de incidente anterioare, vă rugăm să precizați care sunt acestea.

Au fost afectați sau implicați alți prestatori de servicii/ alte părți terțe?: vă rugăm să indicați dacă incidentul a afectat sau nu alți prestatori de servicii/alte părți terțe, dacă aceste informații sunt disponibile. Dacă incidentul a afectat sau a implicat alți prestatori de servicii/alte părți terțe, vă rugăm să le enumerați și să furnizați mai multe informații.

A început gestionarea crizei (internă și/sau externă)?: vă rugăm să indicați dacă a început sau nu gestionarea crizei (internă și/sau externă). Dacă gestionarea crizei a început, vă rugăm să furnizați mai multe informații.

Data și ora declanșării incidentului: data și ora la care a apărut incidentul, dacă sunt cunoscute.

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.

Zonele funcționale afectate: indicați etapa sau etapele procesului de plată care au fost afectate de incident, cum ar fi autentificarea/autorizarea, comunicarea, compensarea, decontarea directă, decontarea indirectă și altele.

Autentificare/autorizare: proceduri care permit PSP să verifice identitatea unui utilizator al serviciilor de plată sau valabilitatea utilizării unui anumit instrument de plată, inclusiv utilizarea elementelor de securitate personalizate ale utilizatorului și a utilizatorului serviciilor de plată (sau a unei părți terțe care acționează în numele utilizatorului respectiv) care își dă consimțământul pentru transferul de fonduri.

Comunicare: fluxul de informații în scopul identificării, autentificării, notificării și informării între prestatorii de servicii de plată care oferă servicii de administrare cont și prestatorii de servicii de inițiere a plății, prestatorii de servicii de informare cu privire la conturi, plătitorii, beneficiarii plăților și alți 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: finalizarea unei tranzacții sau a unei prelucrări în scopul îndeplinirii obligațiilor participanților prin transferul de fonduri, atunci când această acțiune este efectuată de un alt PSP în numele PSP afectat.

Altele: domeniul funcțional afectat nu este niciunul dintre cele de mai sus. Detalii suplimentare trebuie furnizate în câmpul pentru text liber.

Modificări aduse rapoartelor anterioare: vă rugăm să indicați modificările aduse informațiilor furnizate în rapoartele anterioare referitoare la același incident (de exemplu, raportul inițial sau, după caz, un raport intermediar).

B 2 – Clasificarea incidentelor/Informații privind incidentul

Tranzacțiile 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 furnizeze valori concrete pentru aceste variabile, care pot fi fie cifre reale, fie estimări. Ca regulă generală, prestatorii de servicii de plată trebuie să înțeleagă drept „tranzacții afectate” toate tranzacțiile interne și transfrontaliere care au fost sau vor fi probabil afectate direct sau indirect de incident și, în special, tranzacțiile care nu au putut fi inițiate sau procesate, cele pentru care conținutul mesajului de plată a fost modificat și cele care au fost comandate în mod fraudulos (fondurile au fost recuperate sau nu). În plus, PSP trebuie să înțeleagă nivelul regulat al tranzacțiilor de plată ca fiind media zilnică anuală a operațiunilor de plată naționale și transfrontaliere efectuate cu aceleași servicii de plată care au fost afectate de incident, luând anul precedent ca perioadă de referință pentru calcule. În cazul în care PSP nu consideră această cifră ca fiind reprezentativă (de exemplu, din cauza caracterului sezonier), aceștia trebuie să utilizeze în schimb un alt indicator mai reprezentativ și să transmită autorității competente justificarea care stă la

baza acestei abordări în câmpul „Observații”. În cazurile în care tranzacțiile de plată în alte monede decât euro sunt afectate de incident, atunci când se calculează pragurile și se raportează valoarea tranzacțiilor afectate, PSP afectați trebuie să convertească valoarea tranzacțiilor în altă monedă decât euro prin utilizarea cursului de schimb zilnic de referință al BCE pentru ziua precedentă depunerii raportului privind incidentul.

Utilizatorii 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 furnizeze valori concrete pentru aceste variabile, care pot fi fie cifre reale, fie estimări. Prestatorii de servicii de plată trebuie să înțeleagă drept „utilizatorii serviciilor de plată afectați” toți clienții (fie interni, fie din străinătate, consumatori sau întreprinderi) care au un contract cu prestatorul de servicii de plată afectat care le acordă acces la serviciul de plată afectat și care au suferit sau vor suferi probabil consecințele incidentului. Prestatorii de servicii de plată trebuie să revină la estimări bazate pe activitatea anterioară pentru a determina numărul de utilizatori ai serviciilor de plată care ar fi putut utiliza serviciul de plată pe durata incidentului. În cazul grupurilor, fiecare prestator de servicii de plată trebuie să își ia în considerare doar proprii utilizatori de servicii de plată. În cazul unui prestator de servicii de plată care oferă servicii operaționale altor persoane, respectivul prestator de servicii de plată trebuie să ia în considerare doar proprii utilizatori de servicii de plată (dacă există), iar prestatorii de servici de plată care primesc aceste servicii operaționale trebuie, de asemenea, să evalueze incidentul în raport cu proprii utilizatori de servicii de plată. În plus, PSP trebuie să ia ca număr total de utilizatori de servicii de plată cifra agregată a utilizatorilor de servicii de plată naționali și transfrontalieri care au obligații contractuale cu aceștia în momentul incidentului (sau, alternativ, cea mai recentă cifră disponibilă) și care au acces la serviciul de plată afectat, indiferent de dimensiunea acestora sau de faptul că sunt considerați utilizatori activi sau pasivi ai serviciilor de plată.

Încălcarea securității rețelelor sau a sistemelor informatice: Prestatorii de servicii de plată trebuie să stabilească dacă orice acțiune răuvoitoare a compromis disponibilitatea, autenticitatea, integritatea sau confidențialitatea rețelelor sau a sistemelor informatice (inclusiv a datelor) legate de furnizarea de servicii de plată.

Indisponibilitatea serviciului: PSP trebuie să indice dacă pragul este sau va fi probabil atins de incident și cifra aferentă: perioada totală de indisponibilitate a serviciului. PSP trebuie să furnizeze valori concrete pentru această variabilă, care pot fi fie cifre reale, fie estimări. PSP trebuie să ia în considerare perioada de timp pentru care orice sarcină, proces sau canal legat de furnizarea de servicii de plată este sau va fi probabil inaccesibil, împiedicând astfel i) inițierea și/sau executarea unui serviciu de plată și/sau ii) accesul la un cont de plăți. PSP trebuie să contabilizeze perioada de indisponibilitate a serviciului din momentul în care începe timpul de inactivitate și trebuie să ia în considerare atât intervalele de timp în care sunt deschise pentru activități, astfel cum este necesar pentru executarea serviciilor de plată, cât și orele de închidere și perioadele de întreținere, după caz. În cazul în care prestatorii de servicii de plată nu sunt în măsură să determine momentul în care a început întreruperea serviciului, aceștia trebuie, în mod excepțional, să contabilizeze perioada de indisponibilitate a serviciului din momentul detectării acesteia.

Impactul economic: PSP trebuie să indice dacă pragul este sau va fi probabil atins de incident și cifrele aferente: cheltuieli directe și cheltuieli indirecte. PSP trebuie să furnizeze valori concrete pentru aceste variabile, care pot fi fie cifre reale, fie estimări. PSP trebuie să ia în considerare atât costurile care pot fi legate direct de incident, cât și costurile indirect legate de incident. Printre altele, PSP trebuie să ia în considerare fondurile sau activele expropriate, costurile de înlocuire a hardware-ului sau a software-ului, alte costuri de expertiză criminalistică sau de remediere, comisioanele pentru nerespectarea obligațiilor contractuale, sancțiunile, datoriile externe și pierderile de venituri. În ceea ce privește cheltuielile indirecte, PSP trebuie să ia în considerare numai acele costuri care sunt deja cunoscute sau foarte susceptibile să se materializeze. În cazurile în care costurile sunt exprimate în alte monede decât

euro, atunci când se calculează pragul și se raportează valoarea impactului economic, PSP trebuie să convertească valoarea costurilor într-o monedă din afara zonei euro în euro utilizând cursul de schimb zilnic de referință al BCE pentru ziua precedentă depunerii raportului privind incidentul.

Cheltuieli directe: costuri (EUR) cauzate în mod direct de incident, inclusiv costurile pentru corectarea incidentului (de exemplu, fonduri sau active expropriate, costuri de înlocuire a hardware-ului și software-ului, taxe datorate nerespectării obligațiilor contractuale).

Cheltuieli indirecte: costuri (EUR) cauzate în mod indirect de incident (de exemplu, costuri de despăgubire/compensare pentru clienți, potențiale costuri juridice).

Nivel ridicat de escaladare internă: PSP trebuie să analizeze dacă, în urma impactului asupra serviciilor legate de plăți, organul de conducere, astfel cum este definit în Ghidul ABE privind gestionarea riscurilor TIC și de securitate, a fost sau va fi probabil informat, în conformitate cu orientarea 60 litera (d) din Ghidul ABE privind gestionarea riscurilor TIC și de securitate, cu privire la incident în afara oricărei proceduri de notificare periodică și în mod continuu pe întreaga durată a incidentului. În plus, prestatorii de servicii de plată trebuie să analizeze dacă, în urma impactului incidentului asupra serviciilor legate de plăți, a fost sau este probabil să fie declanșat un mod de criză.

Alți PSP sau alte infrastructuri relevante potențial afectate: PSP trebuie să evalueze impactul incidentului asupra pieței financiare, înțeles ca infrastructuri ale pieței financiare și/sau scheme de plată care o susțin, precum și restul PSP. În special, PSP trebuie să evalueze dacă incidentul a fost sau va fi probabil reprodus la alți PSP, dacă a afectat sau este probabil să afecteze buna funcționare a infrastructurilor pieței financiare sau dacă a compromis sau ar putea compromite soliditatea sistemului financiar în ansamblu. PSP trebuie să aibă în vedere diferite dimensiuni, cum ar fi dacă software-ul/componenta afectat(ă) este brevetat(ă) sau general disponibil(ă), dacă rețeaua compromisă este internă sau externă sau dacă PSP a încetat sau ar putea înceta să își îndeplinească obligațiile în cadrul infrastructurilor pieței financiare din care face parte.

Impactul asupra reputației: PSP trebuie să ia în considerare nivelul de vizibilitate pe care, după cunoștințele lor, incidentul l-a dobândit sau îl va câștiga probabil pe piață. În special, PSP trebuie să ia în considerare probabilitatea ca incidentul să cauzeze prejudicii societății ca un bun indicator al potențialului acestuia de a le afecta reputația. Prestatorii de servicii de plată trebuie să ia în considerare dacă i) utilizatorii serviciilor de plată și/sau alți prestatori de servicii de plată s-au plâns de impactul negativ al incidentului, ii) incidentul a afectat un proces vizibil legat de serviciile de plată și, prin urmare, este probabil să primească sau a primit deja acoperire mediatică (având în vedere nu numai mass-media tradițională, cum ar fi ziarele, ci și blogurile, rețelele sociale etc.); cu toate acestea, acoperirea mediatică în acest context înseamnă nu numai câteva comentarii negative din partea urmăritorilor, ci ar trebui să existe o raportare valabilă sau un număr semnificativ de comentarii/alerte negative), iii) obligațiile contractuale au fost sau ar putea fi omise, ceea ce a dus la publicarea de acțiuni juridice împotriva prestatorului de servicii de plată, iv) nu au fost respectate cerințele de reglementare, ceea ce a dus la impunerea unor măsuri sau sancțiuni de supraveghere care au fost sau vor fi probabil făcute publice sau v) un tip similar de incident a avut loc anterior.

B 3 – Descrierea incidentului

Tip de incident: operațional sau de securitate. Explicații suplimentare sunt furnizate în câmpul corespunzător din raportul inițial.

Cauza incidentului: indicați cauza incidentului și, dacă acesta nu este cunoscut încă, cel mai probabil. Pot fi selectate mai multe opțiuni.

În curs de investigare: vă rugăm să bifați căsuța atunci când cauza este necunoscută în prezent.

Acțiune răuvoitoare: acțiuni care vizează în mod intenționat PSP. Acestea includ codul rău intenționat, colectarea de informații, intruziunile, atacurile distribuite/refuzarea serviciului (D/DoS), acțiunile interne deliberate, daunele fizice externe deliberate, securitatea conținutului

informațiilor, acțiunile frauduloase și altele. Pentru mai multe detalii, vă rugăm să consultați secțiunea C2 din prezentul model.

Eroare de proces: cauza incidentului a fost o concepție sau o execuție defectuoasă a procesului de plată, a controalelor procesului și/sau a proceselor de sprijin (de exemplu, procesul de schimbare/migrare, testare, configurare, capacitate, monitorizare).

Eroare de sistem: cauza incidentului este asociată cu o proiectare, execuție, componente, specificații, integrarea sau complexitatea necorespunzătoare a sistemelor, rețelelor, infrastructurilor și bazelor de date care sprijină activitatea de plată.

Erori umane: incidentul a fost cauzat de eroarea neintenționată a unei persoane, fie ca parte a procedurii de plată (de exemplu, încărcarea fișierului unui lot de plăți greșit în sistemul de plăți), fie în legătură cu aceasta (de exemplu, puterea este întreruptă în mod accidental, iar activitatea de plată este suspendată).

Evenimente externe: cauza este asociată cu evenimente aflate în general în afara controlului direct al organizației (de exemplu, dezastre naturale, o defecțiune la un prestator de servicii tehnice).

Altele: cauza incidentului nu este niciuna dintre cele de mai sus. Detalii suplimentare trebuie furnizate în câmpul pentru text liber.

Incidentul v-a afectat în mod direct sau indirect, prin intermediul unui prestator de servicii?: vă rugăm să indicați dacă incidentul a vizat în mod direct PSP sau dacă acesta îl afectează indirect prin intermediul unei terțe părți, dacă aceste informații sunt disponibile. În cazul unui impact indirect, vă rugăm să precizați numele prestatorului (prestatorilor) de servicii.

B 4 – Impactul incidentului

Impact general: vă rugăm să indicați ce dimensiuni au fost afectate de incidentul operațional sau de securitate. Pot fi selectate mai multe opțiuni.

Integritate: proprietatea de a asigura acuratețea și caracterul complet al activelor (inclusiv al datelor).

Disponibilitate: proprietatea serviciilor legate de plăți să fie pe deplin accesibilă și utilizabilă de către utilizatorii serviciilor de plată, în conformitate cu niveluri predefinite acceptabile.

Confidențialitate: proprietatea de a nu pune la dispoziție sau de a nu prezenta informații persoanelor, entităților sau proceselor neautorizate.

Autenticitate: proprietatea unei surse fiind ceea ce pretinde că este.

Canalele comerciale afectate: indicați canalul sau canalele de interacțiune cu utilizatorii serviciilor de plată care au fost afectați de incident. Se pot bifa 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 locurile de desfășurare a activității înființate în același stat membru de un prestator de servicii de plată cu sediul central 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.

ATM-uri: un dispozitiv electromecanic care permite 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.

Comerț electronic: operațiunea de plată este inițiată la un punct virtual de vânzare (de exemplu, pentru plățile inițiate prin internet utilizând transferuri de credit, carduri de plată, transfer de monedă electronică între conturi de monedă electronică).

Altele: canalul comercial afectat nu este niciunul dintre cele de mai sus. Detalii suplimentare trebuie furnizate în câmpul pentru text liber.

Servicii de plată afectate: precizați acele servicii de plată care nu funcționează corect ca urmare a incidentului. Se pot bifa mai multe casete.

Plasare în numerar într-un cont de plăți: predarea de numerar către un PSP pentru a-l credita într-un cont de plăți.

Retragere de numerar dintr-un cont de plăți: cererea primită de un prestator de servicii de plată de la utilizatorul serviciilor sale de plată de a furniza numerar și de a debita contul său de plăți cu suma corespunzătoare.

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 într-un prestator de servicii de plată care încheie un contract cu un beneficiar al plății pentru a accepta și a prelucra operațiuni de plată, ceea ce are ca rezultat un transfer de fonduri 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, PSP-ului plătitorului sau propriului PSP al beneficiarului plății.

Plăți cu cardul: un serviciu de plată bazat pe infrastructura și normele comerciale ale unui sistem de plată cu cardul de a efectua o operațiune de plată prin intermediul oricărui card, dispozitiv de telecomunicații, digital sau informatic sau program informatic, în cazul în care acest lucru are ca rezultat o operațiune cu card de debit sau de credit. Nu constituie tranzacții de plată cu cardul operațiunile bazate pe alte tipuri de servicii de plată.

Emiterea de instrumente de plată: un serviciu de plată care constă într-un prestator de servicii de plată care încheie un contract cu un plătitor pentru a-i pune la dispoziție un instrument de plată pentru a iniția și a prelucra operațiunile de plată ale plătitorului.

Remitere de bani: un serviciu de plată în cadrul căruia fondurile sunt primite de la un plătitor, fără crearea unui cont de plăți în numele plătitorului sau al beneficiarului plății, cu unicul scop de a transfera o sumă corespunzătoare unui beneficiar al plății sau unui alt PSP care acționează în numele beneficiarului plății și/sau în cazul în care aceste fonduri sunt primite în numele beneficiarului plății și sunt puse la dispoziția acestuia.

Servicii de inițiere a plății: un serviciu de plată de inițiere a unui ordin de plată la cererea utilizatorului serviciilor de plată cu privire la un cont de plăți deținut la un alt PSP.

Servicii de informare cu privire la conturi: un serviciu de plată online care furnizează informații consolidate cu privire la unul sau mai multe conturi de plăți deținute de utilizatorul serviciilor de plată fie la un alt prestator de servicii de plată, fie la mai mulți PSP.

B 5 – Atenuarea incidentelor

Ce acțiuni/măsuri au fost luate până în prezent sau sunt planificate să se recupereze în urma incidentului?: vă rugăm să furnizați detalii cu privire la acțiunile care au fost întreprinse sau care urmează să fie întreprinse pentru a aborda temporar incidentul.

Planul de continuitate a activității și/sau planul de recuperare în caz de dezastru au fost activate?: vă rugăm să indicați dacă acest lucru s-a întâmplat și, în caz afirmativ, să furnizați cele mai relevante detalii cu privire la ceea ce s-a întâmplat (și anume, când au fost activate și în ce a constat).

C – Raport final

C 1 – Detalii generale

Actualizarea informațiilor din raportul inițial și din raportul(rapoartele) intermediar(e) (rezumat): vă rugăm să furnizați informații suplimentare privind incidentul, inclusiv modificările specifice aduse informațiilor furnizate în raportul intermediar. Vă rugăm să includeți, de asemenea, orice alte informații relevante.

Sunt în vigoare toate controalele inițiale?: vă rugăm să indicați dacă PSP a trebuit sau nu să anuleze sau să slăbească anumite controale în orice moment al incidentului. În caz afirmativ, vă rugăm să indicați dacă toate controalele sunt reinstituite și, în caz contrar, să explicați în câmpul pentru text liber ce controale nu sunt reinstituite și perioada suplimentară necesară pentru restaurarea lor.

C 2 – Analiza cauzelor principale și acțiuni ulterioare

Care a fost cauza fundamentală, dacă este deja cunoscută?: vă rugăm să indicați care este cauza principală a incidentului sau, dacă acesta nu este cunoscut încă, cea mai probabilă cauză a incidentului. Pot fi selectate mai multe opțiuni. (Vă rugăm să rețineți că ar trebui să se facă distincție între cauza principală și impactul incidentului.)

Acțiune răuvoitoare: acțiuni externe sau interne care vizează în mod intenționat PSP. Acestea sunt împărțite în următoarele categorii:

Cod rău intenționat: De exemplu, un virus, viermi, Trojan, spyware.

Culegerea de informații de exemplu, scanare, umflare, inginerie socială.

Intruziuni: de exemplu, compromiterea unui cont privilegiat, compromiterea unui cont neprivilegiat, compromiterea aplicației, bot.

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

Acțiuni interne deliberate: ex. sabotajul, furtul.

Deteriorare fizică externă deliberată: de exemplu, sabotajul, atacul fizic al sediilor/centrelor de date.

Securitatea conținutului informațiilor: Acces neautorizat la informații, modificarea neautorizată a informațiilor).

Acțiuni frauduloase: utilizarea neautorizată a resurselor, drepturile de autor, masquerada, phishingul.

Altele (vă rugăm specificați): cauza incidentului nu este nici una dintre cele de mai sus. Detalii suplimentare trebuie furnizate în câmpul pentru text liber.

Eroare de proces: cauza incidentului a fost o concepție sau o execuție defectuoasă a procesului de plată, a controalelor procesului și/sau a proceselor de sprijin (de exemplu, procesul de schimbare/migrare, testare, configurare, capacitate, monitorizare). Acestea sunt împărțite în următoarele categorii:

Monitorizare și control deficitare: de exemplu, în ceea ce privește operațiunile în curs, datele de expirare a certificatului, datele de expirare a licenței, datele de expirare ale plasturilor, valorile maxime definite ale contorului, nivelurile de completare a bazei de date, gestionarea drepturilor utilizatorilor, principiul controlului dual.

Probleme de comunicare: de exemplu, între participanții la piață sau în cadrul organizației.

Operații necorespunzătoare: de exemplu, nu există niciun schimb de certificate, cache este plin.

Gestionarea inadecvată a modificărilor: de exemplu, erori de configurare neidentificate, instalare, inclusiv actualizări, probleme de întreținere, erori neașteptate.

Insuficiența procedurilor și a documentației interne: de exemplu, lipsa de transparență în ceea ce privește funcționalitățile, procesele și apariția unei funcționări defectuoase, absența documentației.

Aspecte legate de recuperare: de exemplu, gestionarea situațiilor de urgență, redundanță inadecvată.

Altele (vă rugăm specificați): cauza incidentului nu este nici una dintre cele de mai sus. Detalii suplimentare trebuie furnizate în câmpul pentru text liber.

Eroare de sistem: cauza incidentului este asociată cu o proiectare, execuție, componente, specificații, integrarea sau complexitatea necorespunzătoare a sistemelor, rețelelor, infrastructurilor și bazelor de date care sprijină activitatea de plată. Acestea sunt împărțite în următoarele categorii:

Defecțiune la hardware: defectarea echipamentelor tehnologice fizice care desfășoară procesele și/sau stochează datele necesare prestatorilor de servicii de plată pentru a-și desfășura activitatea legată de plată (de exemplu, defectarea unităților de hard disk, a centrelor de date, a altor infrastructuri).

Defecțiune la rețea: funcționarea necorespunzătoare a rețelelor de telecomunicații, publice sau private, care permit schimbul de date și informații (de exemplu, prin internet) în timpul procesului de plată.

Probleme cu baza de date: structura datelor care stochează informațiile cu caracter personal și informațiile legate de plăți necesare pentru executarea operațiunilor de plată.

Defecțiune la software/aplicație: defecțiuni ale programelor, ale sistemelor de operare etc. care sprijină furnizarea de servicii de plată de către PSP (de exemplu, defecțiuni, funcții necunoscute).

Daune fizice: de exemplu, daune neintenționate cauzate de condiții inadecvate, lucrări de construcții.

Altele (a se preciza): cauza incidentului nu este nici una dintre cele de mai sus. Detalii suplimentare trebuie furnizate în câmpul pentru text liber.

Eroare umană: incidentul a fost cauzat de eroarea neintenționată a unei persoane, fie ca parte a procedurii de plată (de exemplu, încărcarea fișierului unui lot de plăți greșit în sistemul de plăți), fie în legătură cu aceasta (de exemplu, puterea este întreruptă în mod accidental, iar activitatea de plată este suspendată). Acestea sunt împărțite în următoarele categorii:

Neintenționate: de exemplu, greșeli, erori, omisiuni, lipsa de experiență și de cunoștințe.

Lipsă de acțiune: de exemplu, din cauza lipsei de competențe, cunoștințe, experiență, sensibilizare.

Resurse insuficiente: de exemplu, lipsa resurselor umane, disponibilitatea personalului.

Altele (a se preciza): cauza incidentului nu este nici una dintre cele de mai sus. Detalii suplimentare trebuie furnizate în câmpul pentru text liber.

Eveniment extern:: cauza este asociată cu evenimente aflate, în general, în afara controlului organizației. Acestea sunt împărțite în următoarele categorii:

Defecțiune la un furnizor/prestator de servicii tehnice: De exemplu, întreruperi ale alimentării cu energie electrică, întreruperi ale internetului, aspecte juridice, probleme de afaceri, dependențe de servicii.

Forță majoră: de exemplu, întreruperea alimentării cu energie electrică, incendii, cauze naturale precum cutremurele, inundațiile, precipitațiile abundente, vânturile puternice.

Altele (a se preciza): cauza incidentului nu este nici una dintre cele de mai sus. Detalii suplimentare trebuie furnizate în câmpul pentru text liber.

Altele: cauza incidentului nu este niciuna dintre cele de mai sus. Detalii suplimentare trebuie furnizate în câmpul pentru text liber.

Alte informații relevante privind cauza principală: vă rugăm să furnizați orice detalii suplimentare privind cauza principală, inclusiv concluziile preliminare desprinse din analiza cauzelor principale.

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 furnizați o imagine de ansamblu cu privire la PSP care au fost contactați, fie formal, fie informal, pentru a-i informa cu privire la incident, furnizând detalii cu privire la PSP care au fost informați, informațiile care au fost partajate și motivele care stau la baza schimbului de 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, și-a pierdut licența) ca urmare a producerii incidentului.

Evaluarea eficacității acțiunii întreprinse: vă rugăm să includeți, dacă este cazul, o autoevaluare a eficacității acțiunilor întreprinse pe durata incidentului, inclusiv a lecțiilor învățate în urma incidentului.