



# MONITORUL OFICIAL

## AL

# ROMÂNIEI

Anul 190 (XXXIV) — Nr. 252

PARTEA I  
LEGI, DECRETE, HOTĂRĂRI ȘI ALTE ACTE

Mărti, 15 martie 2022

### SUMAR

<u>Nr.</u>		<u>Pagina</u>
	ACTE ALE BĂNCII NAȚIONALE A ROMÂNIEI	
4.	— Regulament pentru modificarea Regulamentului Băncii Naționale a României nr. 2/2020 privind măsurile de securitate referitoare la riscurile operaționale și de securitate și cerințele de raportare aferente serviciilor de plată .....	2–16

# ACTE ALE BĂNCII NAȚIONALE A ROMÂNIEI

BANCA NAȚIONALĂ A ROMÂNIEI

## REGULAMENT

### pentru modificarea Regulamentului Băncii Naționale a României nr. 2/2020 privind măsurile de securitate referitoare la riscurile operaționale și de securitate și cerințele de raportare aferente serviciilor de plată

Având în vedere:

— prevederile art. 218, 219, 223 și art. 244 alin. (2) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative;

— Ghidul revizuit EBA/GL/2021/03 privind raportarea incidentelor majore în temeiul Directivei (UE) 2015/2.336 (DPS 2), în temeiul dispozițiilor art. 243 alin. (1) și ale art. 244 alin. (1) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, precum și ale art. 48 din Legea nr. 312/2004 privind Statutul Băncii Naționale a României,

**Banca Națională a României** emite prezentul regulament.

**Art. 1.** — Regulamentul Băncii Naționale a României nr. 2/2020 privind măsurile de securitate referitoare la riscurile operaționale și de securitate și cerințele de raportare aferente serviciilor de plată, publicat în Monitorul Oficial al României, Partea I, nr. 115 din 14 februarie 2020, cu modificările ulterioare, se modifică după cum urmează:

**1. La articolul 2 alineatul (2), litera g) se modifică și va avea următorul cuprins:**

„g) *confidențialitate* — proprietatea de a nu pune la dispoziție sau de a nu divulga informații persoanelor, entităților sau proceselor neautorizate;”.

**2. La articolul 2 alineatul (2), litera h) se modifică și va avea următorul cuprins:**

„h) *disponibilitate* — proprietatea serviciilor aferente plăților de a fi deplin accesibile și utilizabile de către utilizatorii serviciilor de plată, potrivit nivelurilor acceptabile predefinite anterior de prestatorul de servicii de plată;”.

**3. La articolul 2 alineatul (2), litera k) se modifică și va avea următorul cuprins:**

„k) *incident TIC operațional sau de securitate* — un singur eveniment sau o serie de evenimente corelate neplanificate de prestatorul de servicii de plată, care are/au sau ar putea avea un impact negativ asupra integrității, disponibilității, confidențialității și/sau autenticității serviciilor aferente plăților;”.

**4. La articolul 2 alineatul (2), litera l) se modifică și va avea următorul cuprins:**

„l) *integritate* — proprietatea de a asigura acuratețea și caracterul complet al activelor, inclusiv în ceea ce privește datele;”.

**5. Titlul III se modifică și va avea următorul cuprins:**

### „TITLUL III

#### Raportarea incidentelor operaționale și/sau de securitate majore

### CAPITOLUL I

#### Încadrarea incidentelor operaționale și/sau de securitate în categoria incidentelor majore

**Art. 66.** — Prestatorii de servicii de plată trebuie să evalueze dacă un incident operațional sau de securitate aferent serviciilor de plată prestate se încadrează în categoria incidentelor majore, în baza analizei asupra criteriilor și potrivit metodologiei menționate în anexa nr. 1.

**Art. 67.** — Prestatorii de servicii de plată trebuie să evalueze un incident prin a stabili, pentru fiecare criteriu în parte, dacă pragurile relevante din anexa nr. 2 sunt sau este probabil să fie atinse înainte de soluționarea incidentului.

**Art. 68.** — (1) Prestatorii de servicii de plată trebuie să încadreze în categoria incidentelor majore acele incidente operaționale sau de securitate pentru care:

a) unul sau mai multe criterii se încadrează în categoria «Nivel de impact ridicat»; sau

b) trei sau mai multe criterii se încadrează în categoria «Nivel de impact redus».

(2) Criteriile prevăzute la alin. (1) se încadrează în categoria «Nivel de impact redus», respectiv «Nivel de impact ridicat», prin atingerea pragurilor prevăzute în anexa nr. 2.

**Art. 69.** — Prestatorii de servicii de plată trebuie să recurgă la estimări, de exemplu, în etapa investigației inițiale a incidentului, dacă nu dețin date efective pentru a-și fundamenta evaluarea realizată potrivit art. 66—68, cum ar fi un prag stabilit sau pentru care este o probabilitate foarte mare de a fi atins înainte ca incidentul să fie soluționat.

**Art. 70.** — (1) Prestatorii de servicii de plată trebuie să efectueze evaluarea menționată la art. 66—68 pe bază continuă, pe întreaga durată a existenței incidentului, pentru a identifica orice posibilă schimbare a încadrării incidentului, respectiv prin încadrarea incidentului din incident minor în major sau prin încadrarea incidentului din major în minor.

(2) Orice schimbare a încadrării incidentului din categoria incident major în categoria incident minor trebuie transmisă Băncii Naționale a României fără întârzieri nejustificate, conform art. 91.

### CAPITOLUL II

#### Notificarea incidentelor operaționale și/sau de securitate majore

### SECȚIUNEA 1

#### Dispoziții generale

**Art. 71.** — (1) Prestatorii de servicii de plată, prevăzuți la art. 223 alin. (1) lit. a), b) și e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, trebuie să completeze și să transmită Băncii Naționale a României raportul privind incidentul major, potrivit formularelor și instrucțiunilor de completare prevăzute în anexa nr. 3.

(2) Prin excepție de la aplicarea prevederilor art. 1 alin. (2) lit. b), prestatorii de servicii de plată prevăzuți la art. 223 alin. (1)

lit. c) și d) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care desfășoară activitate de prestare de servicii de plată pe teritoriul României, trebuie să transmită Băncii Naționale a României o copie a notificării prevăzute la art. 219 alin. (4) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, prin intermediul rețelei de comunicații interbancare.

Art. 72. — (1) Prestatorii de servicii de plată trebuie să utilizeze formularele de raport prevăzute în anexa nr. 3 atunci când transmit rapoartele inițiale, intermediare și finale privind același incident, astfel cum sunt menționate în secțiunile a 2-a—a 4-a.

(2) Prestatorii de servicii de plată trebuie să completeze integral și progresiv rubricile din formularele de raport prevăzute la alin. (1), pe măsură ce sunt disponibile mai multe informații în cursul investigațiilor, și să indice informațiile modificate din rapoartele precedente, dacă este cazul.

Art. 73. — Prestatorii de servicii de plată trebuie să prezinte Băncii Naționale a României o copie a informării clienților săi, utilizatori ai serviciilor de plată, cu privire la incidentul operațional sau de securitate major și la toate măsurile pe care utilizatorii de servicii de plată le pot lua pentru a atenua efectele negative ale acestuia, conform prevederilor art. 219 alin. (2) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, de îndată ce această informare este disponibilă, dacă este cazul.

Art. 74. — (1) Prestatorii de servicii de plată trebuie să pună la dispoziția Băncii Naționale a României, la cererea acesteia, orice informații, date și documente suplimentare rapoartelor transmise.

(2) Orice informație adițională conținută în documentele furnizate Băncii Naționale a României, din propria inițiativă sau la cererea acesteia, trebuie să fie inclusă în rapoarte.

Art. 75. — Prestatorii de servicii de plată trebuie să răspundă oricăror solicitări de furnizare de informații suplimentare sau clarificări din partea Băncii Naționale a României cu privire la documentația care a fost deja transmisă.

Art. 76. — Prestatorii de servicii de plată trebuie să păstreze în permanență confidențialitatea și integritatea informațiilor schimbate cu Banca Națională a României și să se autentifice în mod corespunzător în raporturile cu aceasta.

#### SECȚIUNEA a 2-a

##### Raportul inițial

Art. 77. — Prestatorii de servicii de plată trebuie să transmită un raport inițial Băncii Naționale a României după ce un incident operațional și/sau de securitate a fost clasificat ca fiind major.

Art. 78. — Prestatorii de servicii de plată trebuie să indice codul unic de referință de identificare a incidentului comunicat de către Banca Națională a României, atunci când transmit o actualizare a raportului inițial și rapoartele intermediar și final, exceptând situația în care rapoartele intermediar și final sunt transmise împreună cu raportul inițial.

Art. 79. — Prestatorii de servicii de plată trebuie să transmită raportul inițial prevăzut la art. 77 în termen de 4 ore de la clasificarea incidentului ca incident operațional și/sau de securitate major, prin canalele de raportare comunicate de către Banca Națională a României sau de îndată ce aceste canale devin din nou disponibile/operationale, dacă se constată la momentul transmiterii raportării către Banca Națională a României indisponibilitatea canalelor de raportare.

Art. 80. — (1) Prestatorii de servicii de plată trebuie să clasifice incidentul ca incident operațional și/sau de securitate major conform prevederilor art. 68 și anexei nr. 2, în timp util de la detectarea incidentului, dar nu mai târziu de 24 de ore de la detectarea incidentului și fără întârzieri nejustificate din momentul în care prestatorul de servicii de plată are disponibile informațiile necesare procesului de clasificare a incidentului.

(2) Dacă este necesară extinderea termenului precizat la alin. (1) pentru clasificarea incidentului, prestatorii de servicii de plată trebuie să explice această necesitate în raportul inițial care va fi transmis Băncii Naționale a României.

Art. 81. — (1) Prestatorii de servicii de plată trebuie să transmită, de asemenea, un raport inițial Băncii Naționale a României atunci când un incident cunoscut anterior ca fiind minor este reclasificat ca unul major, ca urmare a evaluării efectuate potrivit art. 70.

(2) În situația prevăzută la alin. (1), prestatorii de servicii de plată trebuie să transmită Băncii Naționale a României, prin canalele de raportare comunicate de către aceasta, raportul inițial, de îndată ce se identifică o schimbare de stare sau de îndată ce aceste canale devin din nou disponibile/operationale, dacă se constată la momentul transmiterii raportării către Banca Națională a României indisponibilitatea canalelor de raportare.

Art. 82. — (1) În rapoartele lor inițiale, prestatorii de servicii de plată trebuie să includă informațiile prevăzute în formularul «A — Raport inițial», cuprins în anexa nr. 3, prezentând unele caracteristici de bază ale incidentului și consecințele preconizate ale acestuia pe baza informațiilor disponibile imediat după încadrarea acestuia ca major, potrivit art. 70.

(2) Prestatorii de servicii de plată trebuie să recurgă la estimări atunci când nu sunt disponibile date efective, în acord cu dispozițiile art. 69.

#### SECȚIUNEA a 3-a

##### Raportul intermediar

Art. 83. — (1) Prestatorii de servicii de plată trebuie să transmită raportul intermediar potrivit formularului «B — Raport intermediar», cuprins în anexa nr. 3, când activitățile desfășurate în mod uzual au revenit la normal, cu informarea corespunzătoare a Băncii Naționale a României cu privire la această situație.

(2) Prestatorii de servicii de plată trebuie să considere că activitățile/operationile au revenit la normal atunci când acestea se desfășoară la nivelurile acceptabile predefinite anterior sau la nivelurile incluse în contractele încheiate cu furnizorii terți privind nivelul serviciilor cu referire cel puțin la timpii de prelucrare, capacitatea și cerințele de securitate și când măsurile de urgență nu mai sunt aplicabile.

Art. 84. — (1) Prestatorii de servicii de plată trebuie să transmită Băncii Naționale a României raportul intermediar potrivit formularului «B — Raport intermediar», cuprins în anexa nr. 3, care să conțină o descriere mai detaliată a incidentului și a consecințelor acestuia.

(2) Dacă activitățile desfășurate în mod uzual nu au fost restabilite, prestatorii de servicii de plată trebuie să transmită Băncii Naționale a României un raport intermediar în termen de 3 zile lucrătoare de la data transmiterii raportului inițial.

(3) Prestatorii de servicii de plată trebuie să actualizeze informațiile deja furnizate în formularele «A — Raport inițial» și «B — Raport intermediar», cuprinse în anexa nr. 3, atunci când au cunoștință despre schimbări semnificative de la data transmiterii raportului anterior, cum ar fi, de exemplu, faptul că incidentul a crescut sau a scăzut în intensitate, sunt identificate cauze noi sau sunt luate măsuri pentru soluționarea incidentului.

(4) În situația în care incidentul nu a fost soluționat în termen de 3 zile lucrătoare, prestatorii de servicii de plată vor actualiza informațiile potrivit alin. (3) și vor transmite Băncii Naționale a României un raport intermediar suplimentar.

(5) Prestatorii de servicii de plată trebuie să transmită un raport intermediar suplimentar la solicitarea Băncii Naționale a României.

Art. 85. — Când datele efective nu sunt disponibile, prestatorii de servicii de plată trebuie să recurgă la estimări, prin aplicarea în mod corespunzător a prevederilor art. 69.

Art. 86. — În cazul în care activitatea prestatorului de servicii de plată a revenit la normal în termenul de 4 ore de la momentul clasificării incidentului operațional și/sau de securitate ca major, prestatorii de servicii de plată trebuie să aibă în vedere transmiterea în mod simultan a raportului inițial și a raportului intermediar, prin completarea și transmiterea formularelor «A — Raport inițial» și «B — Raport intermediar», cuprinse în anexa nr. 3, înainte de termenul de 4 ore.

#### SECȚIUNEA a 4-a

##### Raportul final

Art. 87. — Prestatorii de servicii de plată trebuie să trimită un raport final potrivit formularului «C — Raport final», cuprins în anexa nr. 3, atunci când a fost efectuată analiza cauzelor principale, indiferent dacă au fost deja implementate măsurile de atenuare a incidentului sau dacă a fost identificată cauza principală finală, și atunci când există date disponibile pentru a înlocui orice estimări.

Art. 88. — (1) Prestatorii de servicii de plată trebuie să transmită raportul final Băncii Naționale a României în termen de maximum 20 de zile lucrătoare de la data la care aceștia pot demonstra că activitatea a revenit la normal.

(2) Prestatorii de servicii de plată care au nevoie de o prelungire a termenului prevăzut la alin. (1), inclusiv dacă nu sunt încă disponibile date efective cu privire la impact sau dacă nu a fost identificată cauza principală finală, trebuie să contacteze Banca Națională a României înainte de împlinirea termenului prevăzut la alin. (1) și să comunice o justificare adecvată a întârzierii, precum și o nouă dată estimată pentru transmiterea raportului final.

Art. 89. — În cazul în care prestatorii de servicii de plată pot să comunice toate informațiile necesare în raportul final potrivit formularului «C — Raport final», cuprins în anexa nr. 3, în decurs de 4 ore de la momentul clasificării incidentului ca major, aceștia trebuie să aibă în vedere furnizarea agregată a informațiilor referitoare la raportul inițial, raportul intermediar și raportul final prin completarea și transmiterea împreună/simultan a formularelor «A — Raport inițial», «B — Raport intermediar» și «C — Raport final», cuprinse în anexa nr. 3.

Art. 90. — Prestatorii de servicii de plată trebuie să includă în rapoartele finale informații complete cu privire la:

a) datele efective privind impactul în locul estimărilor utilizate și orice alte actualizări necesare ale informațiilor referitoare la raportul inițial și raportul intermediar, cuprinse în formularele «A — Raport inițial» și «B — Raport intermediar», prevăzute în anexa nr. 3; și

b) formularul «C — Raport final», cuprins în anexa nr. 3, care să includă cauza principală, dacă aceasta este deja cunoscută, precum și o prezentare succintă a măsurilor adoptate sau planificate a fi adoptate pentru a elimina problema și a preveni reparația acesteia în viitor.

Art. 91. — (1) Prestatorii de servicii de plată trebuie să transmită rapoartele finale și atunci când, ca urmare a evaluării pe bază continuă a incidentului, aceștia constată faptul că un incident major deja raportat nu mai îndeplinește criteriile pentru a fi considerat major și nu se preconizează că acesta le va îndeplini înainte de soluționarea incidentului.

(2) În situația prevăzută la alin. (1), prestatorii de servicii de plată trebuie să trimită rapoartele finale de îndată ce se constată această situație și, în orice caz, până la termenul transmiterii următorului raport.

(3) În situația prevăzută la alin. (1), prestatorii de servicii de plată trebuie să indice reîncadrarea incidentului drept minor, să transmită formularul «C — Raport final», cuprins în anexa nr. 3, și să explice motivele acestei încadrări.

#### CAPITOLUL III

##### Raportarea delegată și consolidată

Art. 92. — (1) În cazul prestatorilor de servicii de plată, prevăzuți la art. 223 alin. (1) lit. a), b) și e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care intenționează să delege îndeplinirea obligațiilor de raportare a incidentelor majore unei terțe părți, aceștia trebuie să informeze în prealabil Banca Națională a României și să asigure îndeplinirea următoarelor condiții:

a) contractul sau acordurile interne existente în cadrul unui grup, după caz, care stă/stau la baza raportării delegate dintre prestatorul de servicii de plată și terța parte definește/definesc în mod clar alocarea responsabilităților tuturor părților;

b) delegarea respectă cerințele privind externalizarea funcțiilor operaționale importante prevăzute la:

(i) art. 54 și 55 din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative și art. 46—50 din Legea nr. 210/2019 privind activitatea de emitere de monedă electronică în legătură cu instituțiile de plată și, respectiv, pentru instituțiile emittente de monedă electronică; sau

(ii) cap. V al titlului II din Regulamentul Băncii Naționale a României nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, cu modificările și completările ulterioare, pentru instituțiile de credit;

c) asigură în mod corespunzător confidențialitatea datelor sensibile, precum și calitatea, consecvența, integritatea și fiabilitatea informațiilor care vor fi transmise Băncii Naționale a României;

d) transmiterea, în prealabil, către Banca Națională a României a tuturor informațiilor în acord cu prevederile art. 97 și obținerea aprobării prevăzute la art. 98.

(2) În situația prevăzută la alin. (1) lit. a), contractul sau acordurile interne existente în cadrul unui grup, după caz, trebuie să prevadă în mod clar faptul că prestatorul de servicii de plată afectat rămâne pe deplin responsabil și răspunzător pentru îndeplinirea cerințelor prevăzute la art. 219 alin. (1), (2) și (4) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative și pentru conținutul informațiilor prezentate Băncii Naționale a României.

(3) În situația prevăzută la alin. (1) lit. b) pct. (i), prestatorii de servicii de plată vor trata obligația de raportare a incidentelor majore ca funcție operațională importantă.

(4) În situația prevăzută la alin. (1) lit. b) pct. (ii), prestatorii de servicii de plată vor trata obligația de raportare a incidentelor majore ca activitate semnificativă, în înțelesul Regulamentului Băncii Naționale a României nr. 5/2013 privind cerințe prudențiale pentru instituțiile de credit, cu modificările și completările ulterioare.

Art. 93. — (1) Prestatorii de servicii de plată, prevăzuți la art. 223 alin. (1) lit. a), b) și e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care intenționează să delege unei terțe părți îndeplinirea obligațiilor de raportare în mod consolidat, prin transmiterea unui singur raport care face referire la mai mulți prestatori de servicii de plată afectați de același incident operațional sau de securitate major, trebuie să informeze Banca Națională a României, să includă informațiile de contact cu privire la prestatorii de servicii de plată afectați, cuprinse în formularul «A — Raport inițial» din anexa nr. 3, și să se asigure de îndeplinirea următoarelor condiții:

a) includerea dispozițiilor referitoare la raportarea consolidată în contractul care stă la baza raportării delegate;

b) raportarea consolidată condiționată de faptul că incidentul este cauzat de o întrerupere a serviciilor prestate de către terța parte;

c) limitarea raportării consolidate la prestatorii de servicii de plată stabiliți în același stat membru;

d) transmiterea listei tuturor prestatorilor de servicii de plată afectați de incident și asigurarea faptului că terța parte

evaluează semnificația incidentului pentru fiecare prestator de servicii de plată afectat și include în raportul consolidat doar prestatorii de servicii de plată pentru care incidentul a fost clasificat drept unul major. În cazul incertitudinii, asigură includerea unui prestator de servicii de plată în raportul consolidat atât timp cât nu există dovezi în sens contrar;

e) asigurarea faptului că, atunci când nu este posibil să se furnizeze un singur răspuns în unele câmpuri cuprinse în formularele prevăzute în anexa nr. 3, terța parte fie completează date individuale pentru fiecare prestator de servicii de plată afectat, specificând în plus identitatea fiecărui prestator de servicii de plată la care se referă informațiile, fie utilizează valori agregate, astfel cum au fost observate sau estimate pentru acei prestatori de servicii de plată;

f) trebuie să se asigure că terța parte informează în permanență prestatorii de servicii de plată, prevăzuți la art. 223 alin. (1) lit. a), b) și e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, cu privire la toate informațiile relevante legate de incident și la toate interacțiunile pe care terța parte le-ar putea avea cu Banca Națională a României, precum și cu privire la conținutul acestora, însă doar în măsura în care acest lucru este compatibil cu evitarea oricărei încălcări a confidențialității în ceea ce privește informațiile referitoare la alți prestatori de servicii de plată.

(2) Dispozițiile art. 92 alin. (1) lit. b) sunt aplicabile în mod corespunzător în ceea ce privește delegarea unei terțe părți pentru a îndeplini obligațiile de raportare în mod consolidat, în acord cu alin. (1).

Art. 94. — Prestatorii de servicii de plată, prevăzuți la art. 223 alin. (1) lit. a), b) și e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, nu trebuie să își delege îndeplinirea obligațiilor de raportare potrivit art. 92 sau 93, după caz, înainte de a obține aprobarea Băncii Naționale a României potrivit prevederilor art. 98 sau după ce au fost informați de către Banca Națională a României cu privire la faptul că acordul de externalizare nu îndeplinește cerințele prevăzute la art. 94 alin. (1) lit. b).

Art. 95. — (1) Prestatorii de servicii de plată, prevăzuți la art. 223 alin. (1) lit. a), b) și e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care intenționează să retragă delegarea îndeplinirii obligațiilor lor de raportare trebuie să informeze Banca Națională a României în termen de maximum 5 zile lucrătoare de la data luării acestei decizii.

(2) Prestatorii de servicii de plată prevăzuți la alin. (1) trebuie să informeze Banca Națională a României cu privire la orice evoluție semnificativă care afectează terța parte desemnată și capacitatea acesteia de a-și îndeplini obligațiile de raportare.

Art. 96. — (1) Prestatorii de servicii de plată trebuie să își îndeplinească obligațiile de raportare prevăzute în prezentul titlu, fără a recurge la asistența externă, ori de câte ori terța parte desemnată nu a informat Banca Națională a României cu privire la un incident operațional sau de securitate major în conformitate cu prevederile art. 219 alin. (1) și/sau (4) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative și cu cele ale prezentului titlu.

(2) Prestatorii de servicii de plată trebuie să se asigure că un incident operațional sau de securitate major nu este raportat de două ori, individual, de către prestatorul de servicii de plată în cauză și încă o dată de către terța parte către care prestatorul de servicii de plată a delegat îndeplinirea obligațiilor de raportare.

(3) Prestatorii de servicii de plată trebuie să se asigure că în cazul în care un incident este cauzat de o întrerupere a

serviciilor prestate de un furnizor terț de servicii tehnice sau de infrastructură, care afectează mai mulți prestatori de servicii de plată, raportarea delegată se referă la datele individuale aferente prestatorului de servicii de plată afectat, cu excepția cazului în care se raportează consolidat.

Art. 97. — (1) Prestatorii de servicii de plată, prevăzuți la art. 223 alin. (1) lit. a), b) și e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative, care intenționează, în acord cu prevederile art. 92 și 93, să își delege unei terțe părți obligațiile de raportare a incidentelor operaționale sau de securitate majore specifice propriilor servicii de plată prestate, la nivel individual sau consolidat, trebuie să transmită Băncii Naționale a României, fără întârzieri nejustificate, o cerere însoțită de următoarele documente și informații:

a) decizia internă cu privire la raportarea delegată sau consolidată a incidentelor majore specifice propriilor servicii de plată prestate, după caz, semnată la nivelul organului de conducere al prestatorilor de servicii de plată;

b) extrasul din contractul/acordul intern care stă la baza delegării îndeplinirii obligațiilor de raportare, care să probeze îndeplinirea condițiilor prevăzute la art. 92 alin. (1) lit. a) și c) și, respectiv, art. 93 alin. (1) lit. a)—f), după caz.

(2) În situația în care documentația transmisă de către prestatorii de servicii de plată nu îndeplinește cerințele menționate la alin. (1), Banca Națională a României comunică acestora, în termen de 30 de zile lucrătoare, documentele și informațiile necesare pentru conformarea la dispozițiile alin. (1).

(3) Banca Națională a României poate solicita orice alte informații, date, documente și declarații relevante în scopul evaluării cu privire la delegarea obligațiilor de raportare, în acord cu prevederile art. 92 și 93.

(4) Prestatorul de servicii de plată trebuie să transmită informațiile solicitate potrivit alin. (2) și/sau (3) în termen de maximum 45 de zile lucrătoare de la data comunicării solicitării.

(5) Pentru situații bine fundamentate de prestatorul de servicii de plată, la cererea acestuia, Banca Națională a României poate prelungi termenul de transmitere a documentelor și informațiilor prevăzut la alin. (4).

(6) Documentația este completă numai după ce prestatorii de servicii de plată au transmis toate documentele și informațiile potrivit alin. (1)—(3), în termenul prevăzut la alin. (4), respectiv alin. (5), dacă este cazul.

(7) Informațiile și documentele prezentate după expirarea termenelor prevăzute în prezentul articol nu sunt luate în considerare la evaluarea cererii prestatorului de servicii de plată de delegare a unei terțe părți a obligațiilor de raportare a incidentelor operaționale sau de securitate majore.

Art. 98. — Banca Națională a României evaluează și comunică prestatorului de servicii de plată decizia sa cu privire la posibilitatea prestatorului de servicii de plată de a delega către o terță parte obligațiile sale de raportare a incidentelor majore potrivit prezentului titlu, în termen de 30 de zile lucrătoare de la data la care documentația este considerată completă potrivit art. 97 alin. (6).”

**6. Anexa nr. 1 se modifică și se înlocuiește cu anexa nr. 1 care face parte integrantă din prezentul regulament.**

**7. Anexa nr. 2 se modifică și se înlocuiește cu anexa nr. 2 care face parte integrantă din prezentul regulament.**

**8. Anexa nr. 3 se modifică și se înlocuiește cu anexa nr. 3 care face parte integrantă din prezentul regulament.**

**Art. II. —** Prezentul regulament se publică în Monitorul Oficial al României, Partea I.

p. Președintele Consiliului de administrație al Băncii Naționale a României,  
**Florin Georgescu**

## Criteria relevante pentru calificarea incidentelor și indicatorii pe baza cărora acestea se cuantifică

### A. Operațiuni de plată afectate

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

Operațiuni afectate reprezintă toate operațiunile de plată naționale și transfrontaliere care au fost sau vor fi probabil afectate în mod direct sau indirect de incident și, în special, acele operațiuni de plată care nu au putut fi inițiate sau procesate, cele al căror conținut al mesajului de plată a fost modificat și cele care au fost dispuse în mod fraudulos, indiferent dacă fondurile aferente au fost recuperate sau nu sau executarea adecvată este prevenită sau împiedicată în orice fel de incident.

Pentru incidentele operaționale care afectează inițierea și/sau procesarea operațiunilor de plată prestatorii de servicii de plată trebuie să raporteze doar acele incidente operaționale cu o durată mai mare de o oră. Durata incidentului trebuie măsurată de la momentul apariției incidentului până la momentul la care activitățile/operațiunile afectate au fost restabilite la nivelul existent anterior apariției incidentului.

Prestatorii de servicii de plată trebuie să determine nivelul obișnuit al operațiunilor de plată ca media zilnică calculată la nivelul anului precedent a operațiunilor de plată naționale și transfrontaliere executate cu aceleași servicii de plată care au fost afectate de incident. Dacă prestatorii de servicii de plată nu consideră că această cifră este reprezentativă, de exemplu, din cauza caracterului sezonier, aceștia trebuie să utilizeze un alt indicator mai reprezentativ și să prezinte Băncii Naționale a României justificarea aferentă pentru această abordare și să indice această abordare în câmpul „Operațiuni de plată afectate/Comentarii” din secțiunea B2 a formularului „B — Raport intermediar” cuprins în anexa nr. 3 la regulament.

Dacă nu este posibil a se stabili numărul și valoarea operațiunilor afectate, prestatorii de servicii de plată trebuie să utilizeze estimări și să indice această abordare în câmpul „Estimare” din secțiunea B2 a formularului „B — Raport intermediar” cuprins în anexa nr. 3 la regulament.

### B. Utilizatori ai serviciilor de plată afectați

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

Utilizatori ai serviciilor de plată afectați reprezintă toți clienții de la nivel național sau din străinătate, consumatori sau persoane juridice, care au un contract cu prestatorul serviciului de plată afectat, care le acordă acestora accesul la serviciul de plată afectat, și care au suportat sau vor suporta probabil consecințele incidentului. Dacă nu este posibil a se stabili numărul utilizatorilor serviciilor de plată care este posibil să fi folosit serviciul de plată pe durata incidentului, prestatorii de servicii de plată trebuie să utilizeze estimări bazate pe activitatea anterioară și să indice această abordare în câmpul „Estimare” din secțiunea B2 a formularului „B — Raport intermediar” cuprins în anexa nr. 3 la regulament.

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

Pentru incidentele operaționale care afectează inițierea și/sau procesarea operațiunilor de plată, prestatorii de servicii de plată trebuie să raporteze doar acele incidente operaționale care afectează utilizatorii serviciilor de plată cu o durată mai mare de o oră. Durata incidentului trebuie măsurată de la momentul apariției incidentului până la momentul la care

activitățile/operațiunile afectate au fost restabilite la nivelul existent anterior apariției incidentului.

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

### C. 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.

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.

### D. Perioadă de nefuncționare a serviciului

Prestatorii de servicii de plată trebuie să stabilească perioada de timp în care serviciul va fi probabil nefuncțional pentru utilizatorul serviciilor de plată sau în care ordinul de plată nu poate fi executat de către prestatorul de servicii de plată.

Prestatorii de servicii de plată trebuie să aibă în vedere perioada de timp în care orice activitate, proces sau canal asociat prestării serviciilor de plată este sau va fi probabil indisponibilă/indisponibil și, astfel, împiedică (i) inițierea și/sau executarea unui serviciu de plată și/sau (ii) accesul la un cont de plăți.

Prestatorii de servicii de plată trebuie să calculeze perioada de nefuncționare a serviciului de la momentul inițial al indisponibilității și trebuie să ia în considerare atât intervalele de timp cuprinse într-o zi lucrătoare în care aceștia desfășoară activitate ce le permite executarea unui serviciu de plată, cât și orele din afara programului de activitate și perioadele de întreținere, dacă este cazul și dacă sunt aplicabile. Dacă prestatorii de servicii de plată nu pot să stabilească momentul inițial al nefuncționării serviciilor, aceștia trebuie să calculeze în mod excepțional perioada de nefuncționare a serviciului de la momentul în care s-a detectat nefuncționarea.

### E. Impact economic

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

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

### F. Nivel ridicat de escaladare internă

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

Prestatorii de servicii de plată trebuie să aibă în vedere dacă, în urma impactului incidentului asupra serviciilor aferente plăților, conducerea relevantă, stabilită conform prevederilor art. 47<sup>9</sup> alin. (2) lit. d) din regulament, a fost sau va fi probabil informată cu privire la incident în afara oricărei proceduri de notificare periodice și în permanență pe durata existenței incidentului. Suplimentar, prestatorii de servicii de plată trebuie să aibă în

vedere dacă, în urma impactului incidentului asupra serviciilor aferente plăților, a fost sau este susceptibil de a fi declanșat modulul de gestionare a situației de criză.

#### G. Alți prestatori de servicii de plată sau infrastructuri relevante potențial afectați/afectate

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

Prestatorii de servicii de plată trebuie să evalueze impactul incidentului asupra pieței financiare, care trebuie înțeleasă ca fiind infrastructurile pieței financiare și/sau schemele de plată care susțin serviciile lor de plată și alți prestatori de servicii de plată. În mod specific, prestatorii de servicii de plată trebuie să evalueze dacă incidentul s-a propagat sau probabil se va propaga în mod similar la alți prestatori de servicii de plată, dacă acesta a afectat sau va afecta probabil funcționarea infrastructurilor pieței financiare și dacă a compromis sau va compromite probabil funcționarea robustă a sistemului financiar în ansamblu. Prestatorii de servicii de plată trebuie să aibă în vedere diferite aspecte, precum dacă o componentă/un echipament software afectată/afectat este supusă/supus unor drepturi de proprietate sau este disponibilă/disponibil în general, dacă rețeaua compromisă este internă sau externă și dacă prestatorul de servicii de plată a încetat sau va înceta probabil să își îndeplinească obligațiile rezultate din participarea sa la infrastructurile pieței financiare.

#### H. Impact reputațional

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

Prestatorii de servicii de plată trebuie să aibă în vedere nivelul de vizibilitate pe care, după cunoștința lor, incidentul l-a atins sau îl va atinge probabil pe piață. În mod specific, prestatorii de servicii de plată trebuie să considere probabilitatea ca incidentul să provoace daune societății ca fiind un indicator bun al potențialului acestuia de a afecta reputația lor.

Prestatorii de servicii de plată trebuie să țină cont dacă: (i) utilizatorii serviciilor de plată și alți prestatori de servicii de plată au sesizat efectele adverse ale incidentului; (ii) incidentul a afectat un proces vizibil aferent unui serviciu de plată și, prin urmare, este susceptibil de a dobândi sau a dobândit deja acoperire mediatică (având în vedere nu doar media tradițională, precum ziarele, ci și bloguri, rețele de socializare etc.); (iii) au fost sau vor fi probabil nerespectate obligațiile contractuale, care au condus la publicarea unor măsuri legale împotriva prestatorului/prestatorilor de servicii de plată; (iv) au fost sau vor fi probabil nerespectate cerințele prevăzute în cadrul de reglementare, care au condus la impunerea unor măsuri specifice supravegherii sau sancțiuni împotriva prestatorului/prestatorilor de servicii de plată, care au fost sau vor fi probabil publicate; sau (v) a apărut același tip de incident în trecut.

ANEXA Nr. 2

(Anexa nr. 2 la Regulamentul nr. 2/2020)

#### Praguri ale criteriilor luate în considerare la calificarea unui incident în categoria incidentelor majore

Criterii	Nivel de impact redus	Nivel de impact ridicat
Operațiuni de plată afectate	> 10% din nivelul obișnuit al operațiunilor de plată procesate de prestatorul de servicii de plată (sub aspectul numărului de operațiuni) și durata incidentului > o oră*) sau > 500.000 EUR și durata incidentului > o oră*)	> 25% din nivelul obișnuit al operațiunilor de plată procesate de prestatorul de servicii de plată (sub aspectul numărului de operațiuni)  sau > 15.000.000 EUR
Utilizatori ai serviciilor de plată afectați	> 5.000 și durata incidentului > o oră*) sau > 10% dintre utilizatorii serviciilor de plată ai prestatorului de servicii de plată și durata incidentului > o oră*)	> 50.000  sau > 25% dintre utilizatorii serviciilor de plată ai prestatorului de servicii de plată
Perioadă de nefuncționare a serviciului	> 2 ore	Nu este cazul.
Încălcarea securității rețelelor sau a sistemelor informatice	Da	Nu este cazul.
Impact economic	Nu este cazul.	> Max. (0,1% fonduri proprii de nivelul 1**), 200.000 EUR) sau > 5.000.000 EUR
Nivel ridicat de escaladare internă	Da	Da, și declanșarea modulului de gestionare a situației de criză (sau echivalent) este cea mai probabilă.
Alți prestatori de servicii de plată sau infrastructuri relevante potențial afectați/afectate	Da	Nu este cazul.
Impact reputațional	Da	Nu este cazul.

\*) Pragul privind durata incidentului pe o perioadă mai mare de o oră se aplică numai la incidente operaționale care afectează capacitatea prestatorului de servicii de plată de a iniția și/sau procesa operațiuni de plată.

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

## Formularele de raportare a incidentelor majore\*)

Raport Incident Major	
Raport inițial	In termen de 4 ore de la clasificarea incidentului ca major
Data raportului (ZZLL/AAAA)	Ora (HH:MM)
Codul de identificare a incidentului	
Resetează selecțiile	
<b>A - Raport inițial</b>	
<b>A 1 - DETALII GENERALE</b>	
Tip raport	
Prestatorul de servicii de plată afectat (PSP)	
Denumirea prestatorului de servicii de plată	
Numărul unic de identificare al prestatorului de servicii de plată la nivel național	
Conducerea/Entitatea mamă la nivelul grupului	
Tara /Țările afectate/afectate de incident	
Persoana de contact principală	
Persoana de contact secundară	
Entitatea raportoare (această secțiune trebuie completată dacă o parte terță îndeplinește obligațiile de raportare în numele PSP afectat, dacă este cazul)	
Denumirea entității raportoare	
Numărul unic de identificare al entității raportoare la nivel național	
Persoana de contact principală	
Persoana de contact secundară	
<b>A 2 - DETECTAREA ȘI CLASIFICAREA INCIDENTULUI</b>	
Data și ora detectării incidentului (ZZLL/AAAA HH:MM)	
Data și ora clasificării incidentului (ZZLL/AAAA HH:MM)	
Incidentul a fost detectat de	
Tipul incidentului	
Criterii care declanșează elaborarea raportului privind incidentul major	
O scurtă și generală descriere a incidentului	
Impactul asupra altor state ale UE, dacă este cazul	
Raportarea incidentului către alte autorități	
Motivul trimiterii întârziate a raportului inițial	

În cazul în care raportarea se face pe bază consolidată, vă rugăm să completați următorul tabel:

RAPORT CONSOLIDAT - LISTA PSP	
Denumire PSP	Numărul unic de identificare al prestatorului de servicii de plată la nivel național

Raport Incident Major	
Raport intermediar	maximum 3 zile lucrătoare de la remiterea raportului inițial
Data raportului (ZZLL/AAAA)	Ora (HH:MM)
Codul de identificare a incidentului	
Resetează selecțiile	

B - Raport intermediar	
<b>B 1 - DETALII GENERALE</b>	
Descriere mai detaliată a incidentului:	
Care este deficiența/aspectul/problema specifică?	
Cum a început incidentul?	
Cum a evoluat incidentul?	
Care sunt consecințele (în special pentru utilizatorii serviciilor de plată)?	
Incidentul a fost comunicat utilizatorilor serviciilor de plată?	
A fost considerat incidentul în legătură cu unul sau mai multe incidente anterioare?	
Au fost afectați sau implicați alți furnizori de servicii sau terți?	
S-au aplicat măsuri de gestionare a crizei (intern și/sau extern)?	
Data și ora începerii incidentului (dacă a fost deja identificat) (ZZLL/AAAA HH:MM)	
Data și ora la care incidentul a fost restabilit (soluționat) sau este de așteptat să fie restabilit (soluționat) (ZZLL/AAAA HH:MM)	
Arii funcționale afectate	
Modificări aduse rapoartelor anterioare	

B 2 - CLASIFICAREA INCIDENTULUI ȘI INFORMAȚII PRIVIND INCIDENTUL	
Operațiuni de plată afectate	Nivelul impactului
	Numărul de operațiuni de plată afectate
Utilizatori ai serviciilor de plată afectați	Procentul operațiunilor de plată executate în raport cu numărul operațiunilor de plată executate cu aceleași servicii de plată care au fost afectate de incident
	Valoarea operațiunilor de plată afectate în EUR
Încălcarea a securității rețelelor sau a sistemelor informatice	Durata incidentului (aplicabilă numai incidentelor operaționale)
	Comentarii:
Perioadă de nefuncționare a serviciului	Nivelul impactului
	Numărul de utilizatori de servicii de plată afectați
Impact economic	Ca procent din totalul utilizatorilor serviciilor de plată
	Descrieți modul în care rețelele sau sistemele informatice au fost afectate
Nivel ridicat de escaladare internă	Durata totală de nefuncționare a serviciului
	Costuri directe exprimate în EUR
Alți PSP sau infrastructuri relevante potențial afectați/afectate	Costuri indirecte exprimate în EUR
	Descrieți nivelul escaladării interne a incidentului, indicând dacă a declanșat sau este posibil să declanșeze un mod de criză (sau echivalent) și dacă "Da", vă rugăm să descrieți
Impact reputațional	Descrieți modul în care acest incident ar putea afecta alți PSP și/sau infrastructuri
	Descrieți modul în care acest incident ar putea afecta reputația PSP (de exemplu, acoperire mediatică, publicarea/mpunerea unor măsuri împotriva prestatorului etc.)

\*) Modelele formularelor sunt reproduse în facsimil.



B 3 - DESCRIEREA INCIDENTULUI	
Tipul incidentului	
Cauza incidentului	<input type="checkbox"/> În curs de investigație <input type="checkbox"/> Acțiune răuvoitoare <input type="checkbox"/> Eșecul procesului <input type="checkbox"/> Eșecul sistemului <input type="checkbox"/> Eroare umană <input type="checkbox"/> Evenimente externe <input type="checkbox"/> Altele
Incidentul v-a afectat direct sau indirect prin intermediul unui furnizor de servicii?	Dacă "Altele", vă rugăm specificați: Dacă "Indirect", vă rugăm să specificați furnizorul/furnizorii de servicii.
B 4 - IMPACTUL INCIDENTULUI	
Impact general	<input type="checkbox"/> Integritate <input type="checkbox"/> Disponibilitate <input type="checkbox"/> Confidențialitate <input type="checkbox"/> Autenticitate
Canale comerciale afectate	<input type="checkbox"/> Sucursale <input type="checkbox"/> Servicii bancare electronice <input type="checkbox"/> Comerț electronic <input type="checkbox"/> Servicii bancare prin telefon <input type="checkbox"/> Servicii bancare prin telefon mobil <input type="checkbox"/> ATM-uri <input type="checkbox"/> Punct de vânzare <input type="checkbox"/> Altele
Serviciile de plată afectate	<input type="checkbox"/> Depunere de numerar într-un cont de plată <input type="checkbox"/> Retragere de numerar dintr-un cont de plată <input type="checkbox"/> Operațiuni necesare funcționării unui cont de plată <input type="checkbox"/> Acceptare de instrumente de plată <input type="checkbox"/> Operațiuni de transfer-credit <input type="checkbox"/> Debitări directe <input type="checkbox"/> Operațiuni de plată inițiate cu card de plată <input type="checkbox"/> Emisie de instrumente de plată <input type="checkbox"/> Remitere de bani <input type="checkbox"/> Servicii de inițiere a plății <input type="checkbox"/> Servicii de informare cu privire la conturi
B 5 - DIMINUAREA INCIDENTULUI	
Ce acțiuni/măsuri au fost luate până acum sau sunt planificate pentru a recupera situația după incident?	
Planurile de asigurare a continuității activității și/sau de recuperare în caz de dezastru au fost activate?	
Dacă "Da", atunci când? (ZZLL/AAAA HHMM)	
Dacă "Da", vă rugăm descrieți.	

Raport Incident Major	
Vă rugăm selectați tipul raportului:	In termen de 20 de zile lucrătoare de la data la care activitatea a revenit la normal
Vă rugăm să descrieți: (aplicabil pentru incidente reclasificate ca minore)	<input type="text"/>
	<input type="button" value="Resetează selecțiile"/>
Data raportului (ZZLL/AAAA)	Ora (HH MM)
Codul de referință al incidentului	<input type="text"/>

C - Raport final						
Dacă nu a fost transmis un raport intermediar, vă rugăm completați și secțiunea B						
C 1 - DETALII GENERALE						
Actualizarea informațiilor din raportul inițial și raportul intermediar sau rapoartele intermediare						
Modificări aduse rapoartelor anterioare						
Orice alte informații relevante						
Măsurile de control inițiale sunt în vigoare?						
Dacă "Nu", specificați ce controale și perioadă adițională cerută pentru restaurare						
C 2 - ANALIZA CAUZEI PRINCIPALE ȘI ACȚIUNI DE URMĂRIRE						
Care a fost cauza principală (dacă este deja cunoscută)?	<input type="checkbox"/> Acțiune răuvoitoare <input type="checkbox"/> Eșecul procesului <input type="checkbox"/> Eșecul sistemului <input type="checkbox"/> Eroare umană <input type="checkbox"/> Eveniment extern <input type="checkbox"/> Altele					
Trebuie indicată cauza principală a incidentului prin selectarea opțiunii sau opțiunilor relevante.	<table border="0"> <tr> <td> <input checked="" type="checkbox"/> Software rău intenționat  <input checked="" type="checkbox"/> Colectare de informații  <input checked="" type="checkbox"/> Intruțiuni  <input checked="" type="checkbox"/> Atac distribuit de indisponibilizare a serviciului (DDoS)  <input checked="" type="checkbox"/> Acțiuni interne deliberare  <input checked="" type="checkbox"/> Daunele fizice cauzate de acțiuni externe deliberate  <input checked="" type="checkbox"/> Securitatea conținutului informațiilor  <input checked="" type="checkbox"/> Acțiuni frauduloase  <input checked="" type="checkbox"/> Altele                     </td> <td> <input checked="" type="checkbox"/> Monitorizare și control deficitar  <input checked="" type="checkbox"/> Aspecte de comunicare  <input checked="" type="checkbox"/> Operațiuni necorespunzătoare  <input checked="" type="checkbox"/> Gestionarea inadecvată a schimbării  <input checked="" type="checkbox"/> Neadecvare a procedurilor și a documentației interne  <input checked="" type="checkbox"/> Aspecte legate de recuperare  <input checked="" type="checkbox"/> Altele                     </td> <td> <input checked="" type="checkbox"/> Eșecul echipamentului  <input checked="" type="checkbox"/> Eșecul rețelei  <input checked="" type="checkbox"/> Deficiențele bazei de date  <input checked="" type="checkbox"/> Eșecul aplicației/software  <input checked="" type="checkbox"/> Daună fizică  <input checked="" type="checkbox"/> Altele                     </td> <td> <input checked="" type="checkbox"/> Neintenționată  <input checked="" type="checkbox"/> Lipsă de acțiune  <input checked="" type="checkbox"/> Resurse insuficiente  <input checked="" type="checkbox"/> Altele                     </td> <td> <input checked="" type="checkbox"/> Eșec la nivelul unui furnizor/prestator de servicii tehnice  <input checked="" type="checkbox"/> Forță majoră  <input checked="" type="checkbox"/> Altele                     </td> </tr> </table>	<input checked="" type="checkbox"/> Software rău intenționat <input checked="" type="checkbox"/> Colectare de informații <input checked="" type="checkbox"/> Intruțiuni <input checked="" type="checkbox"/> Atac distribuit de indisponibilizare a serviciului (DDoS) <input checked="" type="checkbox"/> Acțiuni interne deliberare <input checked="" type="checkbox"/> Daunele fizice cauzate de acțiuni externe deliberate <input checked="" type="checkbox"/> Securitatea conținutului informațiilor <input checked="" type="checkbox"/> Acțiuni frauduloase <input checked="" type="checkbox"/> Altele	<input checked="" type="checkbox"/> Monitorizare și control deficitar <input checked="" type="checkbox"/> Aspecte de comunicare <input checked="" type="checkbox"/> Operațiuni necorespunzătoare <input checked="" type="checkbox"/> Gestionarea inadecvată a schimbării <input checked="" type="checkbox"/> Neadecvare a procedurilor și a documentației interne <input checked="" type="checkbox"/> Aspecte legate de recuperare <input checked="" type="checkbox"/> Altele	<input checked="" type="checkbox"/> Eșecul echipamentului <input checked="" type="checkbox"/> Eșecul rețelei <input checked="" type="checkbox"/> Deficiențele bazei de date <input checked="" type="checkbox"/> Eșecul aplicației/software <input checked="" type="checkbox"/> Daună fizică <input checked="" type="checkbox"/> Altele	<input checked="" type="checkbox"/> Neintenționată <input checked="" type="checkbox"/> Lipsă de acțiune <input checked="" type="checkbox"/> Resurse insuficiente <input checked="" type="checkbox"/> Altele	<input checked="" type="checkbox"/> Eșec la nivelul unui furnizor/prestator de servicii tehnice <input checked="" type="checkbox"/> Forță majoră <input checked="" type="checkbox"/> Altele
<input checked="" type="checkbox"/> Software rău intenționat <input checked="" type="checkbox"/> Colectare de informații <input checked="" type="checkbox"/> Intruțiuni <input checked="" type="checkbox"/> Atac distribuit de indisponibilizare a serviciului (DDoS) <input checked="" type="checkbox"/> Acțiuni interne deliberare <input checked="" type="checkbox"/> Daunele fizice cauzate de acțiuni externe deliberate <input checked="" type="checkbox"/> Securitatea conținutului informațiilor <input checked="" type="checkbox"/> Acțiuni frauduloase <input checked="" type="checkbox"/> Altele	<input checked="" type="checkbox"/> Monitorizare și control deficitar <input checked="" type="checkbox"/> Aspecte de comunicare <input checked="" type="checkbox"/> Operațiuni necorespunzătoare <input checked="" type="checkbox"/> Gestionarea inadecvată a schimbării <input checked="" type="checkbox"/> Neadecvare a procedurilor și a documentației interne <input checked="" type="checkbox"/> Aspecte legate de recuperare <input checked="" type="checkbox"/> Altele	<input checked="" type="checkbox"/> Eșecul echipamentului <input checked="" type="checkbox"/> Eșecul rețelei <input checked="" type="checkbox"/> Deficiențele bazei de date <input checked="" type="checkbox"/> Eșecul aplicației/software <input checked="" type="checkbox"/> Daună fizică <input checked="" type="checkbox"/> Altele	<input checked="" type="checkbox"/> Neintenționată <input checked="" type="checkbox"/> Lipsă de acțiune <input checked="" type="checkbox"/> Resurse insuficiente <input checked="" type="checkbox"/> Altele	<input checked="" type="checkbox"/> Eșec la nivelul unui furnizor/prestator de servicii tehnice <input checked="" type="checkbox"/> Forță majoră <input checked="" type="checkbox"/> Altele		
Alte informații relevante privind cauza principală	Dacă "Altele", vă rugăm specificați.					
Principalele acțiuni/măsuri corective luate sau planificate pentru prevenirea reapariției incidentului în viitor, dacă se cunosc deja						

C 3 - INFORMAȚII SUPLIMENTARE	
Incidentul a fost comunicat altor prestatori de servicii de plată în scopul informării?	Dacă "Da", vă rugăm furnizați detalii.
A fost luată vreo măsură cu caracter legal împotriva prestatorului de servicii de plată?	Dacă "Da", vă rugăm furnizați detalii.
Evaluarea eficacității măsurilor aplicate	Dacă "Da", vă rugăm furnizați detalii.

## Metodologie și instrucțiuni de completare a formularelor de raportare a incidentelor majore

Prestatorii de servicii de plată trebuie să completeze secțiunea relevantă din formularele de raport cuprinse în prezenta anexă 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. Prestatorii de servicii de plată trebuie să utilizeze același formular atunci când transmit informațiile referitoare la raportul inițial, raportul intermediar și raportul final prin completarea și transmiterea formularelor „A — Raport inițial”, „B — Raport intermediar” și „C — Raport final”. Toate câmpurile sunt obligatorii, exceptând cazurile în care se specifică altfel în mod clar.

### Titlu

Raport inițial: aceasta este prima notificare pe care prestatorul de servicii de plată (PSP) o transmite Băncii Naționale a României (BNR).

Raport intermediar: acesta conține o descriere detaliată a incidentului și a efectelor acestuia și reprezintă o actualizare a raportului inițial și intermediar, dacă este cazul, cu privire la același incident.

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

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

Data și ora raportului: data și ora exactă a transmiterii raportului către BNR

Codul de identificare a incidentului (aplicabil pentru raportul intermediar și cel final, precum și pentru actualizări ale raportului inițial): cod de referință emis de BNR la primirea raportului inițial pentru a identifica în mod unic incidentul

### A — Raport inițial

#### A 1 — Detalii generale

##### Tip de raport:

Individual: trebuie indicat dacă raportul se referă la un singur prestator de servicii de plată afectat (PSP), după caz.

Consolidat: trebuie indicat dacă raportul se referă la mai mulți PSP afectați de același incident major operațional și/sau de securitate, care utilizează opțiunea de raportare consolidată, după caz. Câmpurile de la secțiunea „Prestatorul de servicii de plată afectat” trebuie lăsate necompletate (cu excepția câmpului „Țara/Țările afectată/afectate de incident”) și trebuie furnizată o listă a PSP incluși în raport prin completarea tabelului aferent (Raport consolidat — lista PSP).

Prestatorul de servicii de plată afectat (PSP): se referă la PSP căruia i se întâmplă incidentul.

Denumirea prestatorului de servicii de plată: trebuie indicat numele complet al PSP care face obiectul procedurii de raportare, așa cum apare în registrul național oficial al PSP aplicabil, administrat de BNR.

Numărul unic de identificare al prestatorului de servicii de plată la nivel național: trebuie indicat numărul de identificare unic relevant, utilizat pentru identificarea PSP, astfel:

a) numărul din registrul administrat de BNR pentru instituțiile de plată prevăzute la art. 223 alin. (1) lit. a) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative;

b) numărul din registrul administrat de BNR pentru instituțiile emitente de monedă electronică prevăzute la art. 223 alin. (1) lit. a) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative;

c) numărul din registrul administrat de BNR pentru furnizorii specializați în servicii de informare cu privire la conturi, persoane juridice române și persoane fizice cu sediul profesional în România, prevăzute la art. 223 alin. (1) lit. b) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative;

d) numărul de înmatriculare din registrul instituțiilor de credit, administrat de BNR pentru entitățile care sunt instituții de credit, persoane juridice române sau sucursale ale instituțiilor de credit din state terțe autorizate de Banca Națională a României, prevăzute la art. 223 alin. (1) lit. a) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative;

e) codul unic de identificare fiscală sau un element echivalent pentru entitățile care sunt furnizori de servicii poștale giro care prestează servicii de plată potrivit cadrului legislativ național aplicabil, prevăzute la art. 223 alin. (1) lit. e) din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative.

Conducerea/Entitatea-mamă la nivelul grupului: în cazul grupurilor de entități definite la art. 5 alin. (1) pct. 29 din Legea nr. 209/2019 privind serviciile de plată și pentru modificarea unor acte normative trebuie indicat numele entității conducătoare.

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

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

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

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

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

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

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

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

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

Numărul unic de identificare al entității raportoare la nivel național: trebuie indicat numărul de identificare unic relevant utilizat în țara în care se află partea terță pentru a identifica entitatea care raportează incidentul.

Persoana de contact principală: trebuie indicate prenumele și numele de familie ale persoanei responsabile de raportarea incidentului.

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

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

Persoana de contact secundară: trebuie indicate prenumele și numele de familie ale unei persoane alternative din cadrul entității care raportează incidentul, care ar putea fi contactată de către Banca Națională României atunci când persoana de contact principală nu este disponibilă.

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

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

#### A 2 — Detectarea și încadrarea incidentului

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

Data și ora încadrării incidentului: trebuie indicate data și ora la care incidentul operațional sau de securitate a fost clasificat ca major.

Incidentul a fost detectat de către: trebuie indicat dacă incidentul a fost detectat de către un utilizator al unui serviciu de plată, o structură organizatorică din cadrul PSP (de exemplu, o funcție de audit internă) sau o parte externă (de exemplu, un furnizor extern de servicii). În alte cazuri vă rugăm să oferiți o explicație în câmpul aferent.

Tipul incidentului: trebuie indicat dacă, din informațiile și datele deținute, este un incident operațional și/sau de securitate.

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

Securitate: reprezintă un incident cauzat de accesul, utilizarea, divulgarea, perturbarea, modificarea sau distrugerea neautorizată a activelor PSP care afectează integritatea, disponibilitatea, confidențialitatea și/sau autenticitatea serviciilor

aferente plăților. Acest lucru se poate întâmpla atunci când, printre altele, PSP se confruntă o încălcare a securității rețelelor sau a sistemelor informatice.

Criterii care declanșează elaborarea raportului privind incidentul major: trebuie indicat criteriul sau indicate criteriile care au generat raportarea incidentului ca major. Se pot selecta una sau mai multe opțiuni din următoarele criterii: operațiuni de plată afectate, utilizatori ai serviciilor de plată afectați, perioadă de nefuncționare a serviciului, încălcare a securității rețelelor sau a sistemelor informatice, impact economic, nivel ridicat de escaladare internă, alți prestatori de servicii de plată sau alte infrastructuri relevante potențial afectați/afectate și impact reputațional.

O descriere scurtă și generală a incidentului: trebuie explicate pe scurt cele mai relevante aspecte ale incidentului, cu indicarea posibilelor cauze, a impactului imediat etc.

Impactul asupra altor state ale UE, dacă este cazul: trebuie indicat în cazul în care se consideră că incidentul are impact în alt stat membru sau în alte state membre și se încadrează în termenele-limită de raportare aplicabile. Trebuie furnizată și traducerea în limba engleză.

Raportarea incidentului către alte autorități: trebuie indicat dacă incidentul a fost/va fi raportat către alte autorități în baza altor cerințe legale de raportare, dacă acestea sunt cunoscute la momentul raportării. Trebuie indicată fiecare autoritate națională către care s-a efectuat/va fi efectuată raportarea.

Motivul trimerii întârziate a raportului inițial: trebuie indicată motivația pentru care prestatorul de servicii de plată necesită extinderea termenului de raportare de 24 de ore de la momentul clasificării incidentului ca major.

### B — Raport intermediar

#### B 1 — Detalii generale

Descrierea mai detaliată a incidentului: trebuie furnizată o descriere detaliată a principalelor caracteristici ale incidentului, care să includă cel puțin următoarele: aspectele specifice și contextul aferent, apariția și evoluția incidentului, impactul, în special asupra utilizatorilor serviciilor de plată (*USP*), și, după caz, comunicarea avută cu *USP*.

A fost considerat incidentul în legătură cu unul sau mai multe incidente anterioare?: trebuie indicat dacă incidentul este sau nu corelat cu incidente anterioare, în cazul în care aceste informații sunt disponibile. Dacă incidentul a fost corelat cu incidente anterioare, trebuie indicat/indicate care dintre acestea.

Au fost afectați sau implicați alți furnizori de servicii sau terți?: trebuie indicat dacă incidentul a afectat sau nu alți furnizori de servicii/terțe părți, în cazul în care aceste informații sunt disponibile. Dacă incidentul a afectat sau a implicat alți furnizori de servicii/terțe părți, trebuie indicate părțile afectate, prin enumerare, și trebuie furnizate mai multe informații.

S-au aplicat măsuri de gestionare a crizei (intern și/sau extern)?: trebuie indicat dacă a început sau nu gestionarea crizei la nivel intern și/sau extern. Dacă gestionarea crizei a început, trebuie furnizate mai multe informații.

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

Data și ora la care incidentul a fost restabilit (soluționat) sau este de așteptat să fie restabilit (soluționat): trebuie indicate data

și ora când incidentul a fost sau se așteaptă să fie restabilit și activitățile au revenit sau se așteaptă să revină la normal.

**Arii funcționale afectate:** trebuie indicată fiecare etapă din cadrul procesului de plată care a fost afectată de incident. Se pot selecta una sau mai multe opțiuni din următoarele: autentificare/ autorizare, comunicare, compensare, decontare directă, decontare indirectă, altele.

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

**Comunicare:** reprezintă fluxul de informații în scopul identificării, autentificării, notificării și comunicării dintre PSP care oferă servicii de administrare cont și prestatorii de servicii de inițiere a plății, prestatorii de servicii de informare cu privire la conturi, plătitori, beneficiarii plății și alți PSP.

**Compensare:** reprezintă 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:** reprezintă încheierea unei operațiuni de plată 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:** reprezintă încheierea unei operațiuni de plată sau a procesării cu scopul de a îndeplini obligațiile participanților prin transferarea de fonduri atunci când această acțiune este desfășurată de către un alt PSP în numele PSP afectat.

**Altele:** reprezintă altă arie funcțională afectată, diferită cele de mai sus. Trebuie furnizate detalii suplimentare în câmpul aferent textului liber.

**Modificări aduse rapoartelor anterioare:** trebuie indicate modificările față de informațiile furnizate în rapoartele precedente cu privire la același incident (de exemplu, raportul inițial și, dacă este cazul, raportul intermediar).

**B 2 — Clasificarea incidentului și informații privind incidentul**

**Operațiuni de plată afectate:** trebuie precizate pragurile care sunt sau vor fi probabil atinse de către incident, dacă există, precum și valorile aferente: numărul operațiunilor de plată afectate, procentul operațiunilor de plată afectate în raport cu numărul operațiunilor de plată executate cu aceleași servicii de plată care au fost afectate de incident, precum și valoarea totală a operațiunilor. PSP trebuie să prezinte valori specifice pentru aceste variabile, care pot fi valori efective sau estimări. Ca regulă generală, PSP trebuie să înțeleagă ca fiind „operațiuni de plată afectate” toate operațiunile interne și transfrontaliere care au fost sau vor fi probabil afectate în mod direct sau indirect de incident și, în mod specific, acele operațiuni care nu au putut fi inițiate sau procesate, cele al căror conținut al mesajului de plată a fost modificat și cele care au fost inițiate în mod fraudulos (indiferent dacă fondurile au fost recuperate sau nu). Mai mult, PSP trebuie să înțeleagă faptul că nivelul obișnuit al operațiunilor de plată este media anuală zilnică a operațiunilor interne și transfrontaliere executate cu aceleași servicii de plată care au fost afectate de incident, considerând anul anterior ca fiind perioada de referință pentru calcule. Dacă PSP nu consideră că această valoare este reprezentativă (de exemplu,

din cauza caracterului sezonier), aceștia trebuie să utilizeze în schimb un alt indicator mai reprezentativ și să prezinte autorității naționale justificarea aferentă acestei abordări în câmpul „Comentarii”. În cazurile în care operațiunile de plată, denumite în alte monede decât euro, sunt afectate de incident, la calcularea pragurilor și raportarea valorii operațiunilor de plată, PSP trebuie să convertească valoarea acestor operațiuni în euro prin utilizarea cursului de schimb de referință zilnic al Băncii Centrale Europene publicat pentru ziua anterioară transmiterii raportului.

**Utilizatori ai serviciilor de plată afectați:** trebuie precizate pragurile care sunt sau vor fi probabil atinse de către incident, dacă există, și valorile aferente: numărul total al utilizatorilor serviciilor de plată care au fost afectați și procentul utilizatorilor serviciilor de plată afectați din numărul total al utilizatorilor serviciilor de plată. PSP trebuie să prezinte valori concrete pentru aceste variabile, care pot fi valori efective sau estimări. PSP trebuie să înțeleagă ca fiind „utilizatori ai serviciilor de plată afectate” toți clienții (de la nivel intern sau din străinătate, consumatori sau întreprinderi) care au un contract cu prestatorul serviciului de plată afectat, care le acordă acestora accesul la serviciul de plată afectat și care au suportat sau vor suporta probabil consecințele incidentului. PSP trebuie să recurgă la estimări bazate pe activitatea anterioară pentru a stabili numărul utilizatorilor serviciilor de plată care este posibil să fi folosit serviciul de plată pe durata incidentului. În cazul grupurilor, fiecare PSP trebuie să aibă în vedere doar utilizatorii serviciilor de plată proprii. În cazul unui PSP care oferă servicii operaționale altor persoane, acesta trebuie să aibă în vedere doar utilizatorii de servicii de plată proprii (dacă există), iar PSP care beneficiază de respectivele servicii operaționale trebuie să evalueze, de asemenea, incidentul în legătură cu utilizatorii serviciilor de plată proprii. Mai mult, PSP trebuie să considere ca fiind numărul total al utilizatorilor serviciilor de plată valoarea agregată a utilizatorilor serviciilor de plată interni și din străinătate față de care este obligat prin contract la momentul incidentului (sau, alternativ, cea mai recentă valoare disponibilă) și care au acces la serviciul de plată afectat, indiferent de dimensiunea acestora sau dacă aceștia sunt considerați utilizatori activi sau pasivi ai serviciilor de plată.

**Încălcarea securității rețelelor sau a sistemelor informatice:** trebuie stabilit 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.

**Perioadă de nefuncționare a serviciului:** trebuie precizate dacă pragul este sau va fi probabil atins de către incident, precum și valoarea aferentă: timpul total de indisponibilitate a serviciului. PSP trebuie să prezinte valori concrete pentru această variabilă, care pot fi exprimate în valori efective sau estimări. PSP trebuie să aibă în vedere perioada de timp în care orice activitate, proces sau canal asociat prestării serviciilor de plată este sau va fi probabil indisponibil și, astfel, împiedică: (i) inițierea și/sau executarea unui serviciu de plată; și/sau (ii) accesul la un cont de plăți. PSP trebuie să calculeze durata de nefuncționare a serviciului de la momentul inițial al indisponibilității și trebuie să ia în considerare atât intervalele de timp în care aceștia funcționează conform cerințelor de executare a serviciilor de plată, cât și orele în care nu funcționează, precum și perioadele de întreținere, dacă este cazul și dacă există. Dacă prestatorii de servicii de plată nu pot

să stabilească momentul inițial al indisponibilității serviciului, aceștia trebuie să calculeze în mod excepțional durata de nefuncționare a serviciului de la momentul în care s-a detectat indisponibilitatea.

**Impact economic:** trebuie precizate dacă pragul este sau va fi probabil atins de către incident, precum și valorile aferente: costurile directe și indirecte exprimate în euro. PSP trebuie să prezinte valori concrete pentru aceste variabile, care pot fi valori efective sau estimări. PSP trebuie să aibă în vedere atât costurile care pot fi legate în mod direct de incident, cât și cele care sunt legate în mod indirect de incident. Printre altele, PSP trebuie să țină cont de fondurile sau activele expropriate, costurile de înlocuire a echipamentelor hardware sau software, alte costuri specifice expertizei criminalistice sau costuri de remediere, taxe aplicate ca urmare a neconformității cu obligațiile contractuale, sancțiuni, datorii externe și venituri pierdute. În ceea ce privește costurile indirecte, PSP trebuie să le aibă în vedere doar pe cele care sunt deja cunoscute sau foarte probabil de a se concretiza. 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 în euro prin utilizarea cursului de schimb de referință zilnic al Băncii Centrale Europene publicat pentru ziua anterioară transiterii raportului.

**Costuri directe:** suma de bani (în euro) asociată costului direct al incidentului, inclusiv fonduri necesare pentru remedierea incidentului (de exemplu, fonduri sau active expropriate, costuri de înlocuire a echipamentelor hardware și software, tarife datorate nerespectării obligațiilor contractuale).

**Costuri indirecte:** suma de bani (în euro) asociată costului indirect al incidentului (de exemplu, costuri asociate reparațiilor/compensațiilor pentru clienți, venituri pierdute ca urmare a oportunităților de afaceri ratate, posibile cheltuieli judiciare).

**Nivel ridicat de escaladare internă:** trebuie să se aibă în vedere dacă, în urma impactului incidentului asupra serviciilor aferente plăților, conducerea relevantă, stabilită conform prevederilor art. 47<sup>9</sup> alin. (2) lit. d) din regulament, a fost sau va fi probabil informată cu privire la incident în afara oricărei proceduri de notificare periodice și în permanență pe durata existenței incidentului. În plus, PSP trebuie să aibă în vedere dacă, în urma impactului incidentului asupra serviciilor aferente plăților, a fost sau este susceptibil de a fi declanșat modulul de gestionare a situației de criză.

**Alți PSP sau infrastructuri relevante potențial afectați/afectate:** trebuie evaluat impactul incidentului asupra pieței financiare, care este înțeleasă ca fiind infrastructurile pieței financiare și/sau schemele de plată care o susțin, precum și restul PSP. În mod specific, PSP trebuie să evalueze dacă incidentul s-a propagat sau probabil se va propaga în mod similar la alți PSP, dacă acesta a afectat sau va afecta probabil funcționarea fără probleme a infrastructurilor pieței financiare și dacă a compromis sau va compromite probabil soliditatea sistemului financiar în ansamblu. PSP trebuie să aibă în vedere diferite aspecte, precum dacă o componentă/un echipament software afectată/afectat este supusă/supus unor drepturi de proprietate sau este disponibilă/disponibil în general, dacă rețeaua compromisă este internă sau externă și dacă PSP a încetat sau va înceta probabil să își îndeplinească obligațiile rezultate din participarea sa la infrastructurile pieței financiare.

**Impact reputațional:** trebuie să se aibă în vedere nivelul de vizibilitate pe care, după cunoștința PSP, incidentul l-a atins sau îl va atinge probabil pe piață. În mod specific, PSP trebuie să aibă în vedere probabilitatea ca incidentul să provoace daune societății ca fiind un indicator bun al potențialului acestuia de a afecta reputația lor. PSP trebuie să țină cont dacă: (i) utilizatorii serviciilor de plată și alți prestatori de servicii de plată au sesizat efectele adverse ale incidentului; (ii) incidentul a afectat un proces vizibil aferent unui serviciu de plată și, prin urmare, este susceptibil de a dobândi sau a dobândit deja acoperire mediatică (având în vedere nu doar media tradițională, precum ziarele, ci și bloguri, rețele de socializare etc. Acoperirea mediatică în acest context nu înseamnă doar câteva comentarii negative din partea urmăritorilor, ci ar trebui să existe o raportare valabilă sau un număr semnificativ de comentarii/alerte negative); (iii) au fost sau vor fi probabil nerespectate obligațiile contractuale, care au condus la publicarea unor măsuri legale împotriva prestatorului/prestatorilor de servicii de plată; (iv) au fost sau vor fi probabil nerespectate cerințele prevăzute în cadrul de reglementare, care au condus la impunerea unor măsuri specifice supravegherii sau sancțiuni împotriva prestatorului/prestatorilor de servicii de plată, care au fost sau vor fi probabil publicate; sau (v) a apărut același tip de incident în trecut.

### B 3 — Descrierea incidentului

**Tipul incidentului:** trebuie precizată natura operațională sau de securitate a incidentului. Explicații suplimentare trebuie furnizate în câmpul corespunzător din raportul inițial.

**Cauza incidentului:** trebuie precizată cauza incidentului sau, dacă aceasta nu se cunoaște încă, cea mai probabilă cauză. Se pot selecta una sau mai multe opțiuni.

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

**Acțiune răuvoitoare:** acțiuni care vizează în mod intenționat PSP. Acestea includ utilizarea de software rău intenționat, colectarea de informații, intruziunile, atacurile distribuite/refuzarea serviciului (D/DoS), acțiunile interne deliberate, daunele fizice cauzate de acțiuni externe deliberate, securitatea conținutului informațiilor, acțiunile frauduloase și altele. Pentru mai multe detalii, vă rugăm să consultați secțiunea C 2.

**Eșecul procesului:** cauza incidentului a fost o proiectare 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).

**Eșecul sistemului:** cauza incidentului este asociată cu o proiectare, execuție, componente, specificații, integrare sau complexitate necorespunzătoare a sistemelor, rețelelor, infrastructurilor și bazelor de date care sprijină activitatea de prestare a serviciilor de plată.

**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).

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

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

Incidentul v-a afectat direct sau indirect prin intermediul unui furnizor de servicii?: trebuie indicat 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 trebuie precizată denumirea furnizorului/furnizorilor de servicii.

#### B 4 — Impactul incidentului

Impact general: trebuie indicate dimensiunile care au fost afectate de incidentul operațional sau de securitate. Se pot selecta una sau mai multe opțiuni.

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

Disponibilitate: proprietatea serviciilor aferente plăților de a fi deplin accesibile și utilizabile de către utilizatorii serviciilor de plată, potrivit nivelurilor acceptabile predefinite anterior 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: reprezintă proprietatea unei surse de a fi ceea ce se pretinde a fi.

Canale comerciale afectate: trebuie precizate canalul sau canalele de interacțiune cu utilizatorii serviciilor de plată, care au fost afectate de incident. Se pot selecta una sau mai multe opțiuni.

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

Servicii bancare electronice (E-banking): utilizarea de computere pentru desfășurarea operațiunilor financiare prin internet.

Servicii bancare prin telefon (Telephone banking): utilizarea de telefoane pentru desfășurarea operațiunilor financiare.

Servicii bancare prin telefon mobil (Mobile banking): utilizarea unei anumite aplicații bancare pe un telefon inteligent sau un dispozitiv similar pentru desfășurarea operațiunilor financiare.

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

Punct de vânzare: spațiu fizic al comerciantului în care este inițiată operațiunea de plată.

Comerț electronic: operațiunea de plată este inițiată la un punct virtual de vânzare (de exemplu, pentru operațiunile de plată 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. Trebuie furnizate detalii suplimentare în câmpul aferent textului liber.

Servicii de plată afectate: trebuie precizate serviciile de plată care nu funcționează în parametri normali ca urmare a incidentului. Se pot selecta una sau mai multe opțiuni.

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

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

Operațiuni necesare funcționării 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).

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

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

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

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

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

Remitere de bani: un serviciu de plată prin care fondurile sunt primite de la plătitor, fără crearea unui cont de plăți pe numele plătitorului sau al beneficiarului plății pentru realizarea respectivei operațiuni de plată, cu scopul unic de a transfera o sumă echivalentă beneficiarului plății sau unui alt prestator de servicii de plată care acționează în numele și pe seama beneficiarului plății, inclusiv în situația în care fondurile sunt primite în numele și pe seama beneficiarului plății și sunt puse la dispoziția acestuia.

Servicii de inițiere a plății: servicii de plată pentru inițierea unui ordin de plată la cererea utilizatorului serviciilor de plată cu privire la un cont de plăți deținut la un alt prestator de servicii de plată.

Servicii de informare cu privire la conturi: servicii de plată online prin care se furnizează informații consolidate în legătură cu unul sau mai multe conturi de plăți deținute de utilizatorul serviciilor de plată la alt prestator de servicii de plată sau la mai mulți prestatori de servicii de plată.

#### B 5 — Diminuarea incidentului

Ce acțiuni/măsurile au fost luate până în prezent sau sunt planificate pentru a restabili situația după incident?: trebuie furnizate detalii privind acțiunile care au fost luate sau prevăzute a fi luate pentru gestionarea temporară a incidentului.

Planurile de asigurare a continuității activității și/sau de recuperare în caz de dezastre au fost activate?: trebuie precizate dacă acestea au fost activate și, în acest caz, trebuie furnizate cele mai relevante detalii despre ceea ce s-a întâmplat, cum ar fi, când au fost activate și în ce au constat aceste planuri.

**C — Raportul final****C 1 — Detalii generale**

Actualizarea informațiilor din raportul inițial și raportul intermediar sau rapoartele intermediare (rezumat): trebuie precizate informații suplimentare cu privire la incident, inclusiv modificările specifice aduse informațiilor furnizate în raportul intermediar. Trebuie indicate, de asemenea, orice alte informații relevante.

Măsurile de control inițiale sunt în vigoare?: trebuie indicat dacă a trebuit sau nu să fie anulate sau reduse unele măsuri de control în orice moment pe durata manifestării incidentului. În caz afirmativ, trebuie indicate toate măsurile de control care au fost reinstituite și, în caz contrar, trebuie indicate în câmpul aferent textului liber care din măsurile de control nu sunt reinstituite și perioada suplimentară necesară pentru reinstituirea lor.

**C 2 — Analiza cauzei principale și acțiuni de urmărire**

Care a fost cauza principală (dacă este deja cunoscută)? trebuie indicată care este cauza principală a incidentului sau, dacă aceasta nu este cunoscută încă, care este cea mai probabilă cauză a incidentului. Pot fi selectate mai multe opțiuni, dar trebuie să se facă distincție între cauza principală și impactul incidentului:

Acțiune răuvoitoare: orice acțiune externă sau internă care vizează în mod intenționat PSP. Trebuie să selecteze una sau mai multe opțiuni din următoarele categorii:

Software rău intenționat: de exemplu, un virus informatic, un vierme informatic, Trojan, spyware

Colectare de informații: de exemplu, scanare, *sniffing*, inginerie socială

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

Atac distribuit de indisponibilizare a serviciului (D/DoS): o încercare de a indisponibiliza un serviciu online prin încărcarea acestuia cu trafic (număr mare de solicitări) din mai multe surse

Acțiuni interne deliberate: de exemplu, sabotaj, furt

Daunele fizice cauzate de acțiuni externe deliberate: de exemplu, sabotaj, atac fizic al sediilor/centrelor de date

Securitatea conținutului informațiilor: acces neautorizat la informații, modificarea neautorizată a informațiilor

Acțiuni frauduloase: utilizare neautorizată a resurselor, drepturilor de autor, *masquerada*, *phishing*

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

Eșecul procesului: cauza incidentului a fost o proiectare 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). Se pot selecta una sau mai multe opțiuni din următoarele categorii:

Monitorizare și control deficitare: de exemplu, în ceea ce privește operațiunile în curs de desfășurare, datele de expirare a unui certificat, datele de expirare a unei licențe, datele de expirare a unor *patch*-uri, valorile maxime definite ale contorului, nivelurile de completare a bazei de date, gestionarea drepturilor utilizatorilor, principiul controlului dual.

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

Operațiuni necorespunzătoare: de exemplu, nu există niciun schimb de certificate, memoria *cache* este complet utilizată.

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

Neadekvare a 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, gestionare a situațiilor de urgență, redundanță inadecvată.

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

Eșecul sistemului: cauza incidentului este asociată cu o proiectare, execuție, componente, specificații, integrare sau complexitate necorespunzătoare a sistemelor, rețelelor, infrastructurilor și bazelor de date care sprijină activitatea de prestare a serviciilor de plată. Se pot selecta una sau mai multe opțiuni din următoarele categorii:

Eșecul echipamentului: defectarea echipamentelor tehnologice fizice implicate în desfășurarea proceselor și/sau stocarea datelor necesare PSP pentru a-și desfășura serviciile aferente plăților (de exemplu, defectarea unităților de hard-disk, a centrelor de date, a altor infrastructuri)

Eșecul rețelei: funcționarea necorespunzătoare a rețelelor de telecomunicații, publice sau private, care permit schimbul de date și informații (de exemplu, prin internet) în timpul desfășurării proceselor aferente plăților

Deficiențe ale bazei de date: structura datelor care stochează informațiile cu caracter personal și informațiile legate de plăți necesare pentru executarea operațiunilor de plată

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

Daună fizică: de exemplu, daune neintenționate cauzate de condiții inadecvate, lucrări de construcții.

Altele: cauza incidentului nu este niciuna dintre cele de mai sus. Trebuie furnizate detalii suplimentare în câmpul aferent textului 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, energia electrică este întreruptă în mod accidental, iar activitatea de plată este suspendată). Se pot selecta una sau mai multe opțiuni din următoarele categorii:

Neintenționată: de exemplu, greșeli, erori, omisiuni, lipsa de experiență și de cunoștințe

Lipsă de acțiune: de exemplu, din cauza lipsei de abilități, competențe, cunoștințe, experiență, conștientizare

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

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

Eveniment extern: cauza este asociată cu evenimente aflate în general în afara controlului direct al PSP. Se pot selecta una sau mai multe opțiuni din următoarele categorii:

Eșec la nivelul unui furnizor/prestator de servicii tehnice: de exemplu, întreruperi ale alimentării cu energie electrică, întreruperi ale internetului, aspecte juridice, aspecte legate de afaceri, dependențe ale serviciului

Forță majoră: de exemplu, întreruperea alimentării cu energie electrică, incendii, cauze naturale precum cutremure, inundații, precipitații abundente, vânturi puternice

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

Alte informații relevante privind cauza principală: trebuie furnizate orice detalii suplimentare privind cauza principală, inclusiv concluziile preliminare rezultate din analiza cauzelor principale.

Acțiuni/măsuri corective principale luate sau planificate pentru prevenirea reparației incidentului în viitor, dacă se

cunosc deja: trebuie descrise 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 prestatori de servicii de plată în scopul informării?: trebuie furnizate informații cu privire la comunicarea incidentului altor PSP contactați, pe cale oficială sau neoficială, prezentând detalii despre PSP care au fost informați, informațiile care au fost comunicate și motivele care au stat la baza comunicării acestor informații.

A fost luată vreo măsură cu caracter legal împotriva prestatorului de servicii de plată?: trebuie precizat dacă la data completării raportului final PSP a făcut obiectul vreunei acțiuni în justiție (de exemplu, a fost adus în instanță sau și-a pierdut licența) ca urmare a manifestării incidentului.

Evaluarea eficacității măsurilor aplicate: trebuie indicată, dacă este cazul, o autoevaluare a eficacității măsurilor întreprinse pe durata incidentului, inclusiv a lecțiilor învățate în urma incidentului.

---

---

**EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR**



„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; 012329  
C.I.F. RO427282, IBAN: RO55RNCB0082006711100001 BCR  
și IBAN: RO12TREZ7005069XXX000531 DTCPMB (alocat numai persoanelor juridice bugetare)  
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, www.monitoruloficial.ro

Adresa Biroului pentru relații cu publicul este:  
Str. Parcului nr. 65, intrarea A, sectorul 1, București; 012329.  
Tel. 021.401.00.73, e-mail: concursurifp@ramo.ro, convocariaga@ramo.ro  
Pentru publicări, încărcați actele pe site, la: <https://www.monitoruloficial.ro/brp/>

