GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 2025

Chișinău

Pentru aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice

---

În temeiul art. 7 alin. (4) pct. 10) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153, art. 225), cu modificările ulterioare, Guvernul HOTĂRĂȘTE,

1. Se aprobă Regulamentul privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (se anexează).

2. Controlul executării prezentei hotărâri se pune în sarcina Ministerului Dezvoltării Economice și Digitalizării.

3. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

Prim-ministru **ALEXANDRU MUNTEANU**

Contrasemnează:

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării Eugeniu OSMOCHESCU

Aprobat
prin Hotărârea Guvernului nr. /2025

REGULAMENT
privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (în continuare – *Regulament*) stabilește cadrul juridic material și procedural pentru notificarea, evaluarea, remedierea și divulgarea coordonată a vulnerabilităților produselor și serviciilor tehnologiei informației și comunicațiilor (TIC), în vederea îmbunătățirii securității cibernetice.

2. Scopul prezentului Regulament este de a promova un proces sigur, previzibil și eficient de raportare, evaluare și remediere a vulnerabilităților în produsele și serviciile TIC, prin încurajarea cooperării între raportori, organizațiile responsabile și autoritățile competente, în vederea consolidării securității cibernetice naționale.

3. Prezentul Regulament se aplică cu respectarea prevederilor legislației naționale relevante în domeniul securității cibernetice, al protecției datelor cu caracter personal, al protecției consumatorilor, a drepturilor de autor și a altor reglementări aplicabile.

4. În prezentul Regulament se utilizează noțiunile definite în Legea nr. 48/2023 privind securitatea cibernetică, precum și următoarele noțiuni:

4.1. *entități neautorizate* – persoane fizice sau juridice care desfășoară acțiuni neautorizate asupra rețelelor și sistemelor informatice, exploatând vulnerabilități în scopul compromiterii confidențialității, integrității sau disponibilității datelor ori perturbării funcționării acestora;

4.2. *autoritate competentă sectorială* – autoritate publică cu atribuții de reglementare, supraveghere și control în domeniile financiar-bancar, energetic și al comunicațiilor electronice, precum și alte autorități desemnate pentru supravegherea entităților din sectoare critice;

4.3. *cercetător sau participant în domeniul securității cibernetice* – persoană fizică sau juridică care deține cunoștințele, experiența și competențele necesare și care, acționând cu bună-credință și în conformitate cu cadrul

normativ, identifică, evaluează și raportează vulnerabilități în produsele și serviciile TIC, în scopul îmbunătățirii securității acestora;

4.4. *coordonator național al procesului de divulgare coordonată a vulnerabilităților în domeniul securității cibernetice* (*coordonator național*) – Agenția pentru Securitate Cibernetică, care acționează în calitate de intermediar neutru și de încredere între raportori și organizațiile responsabile, la cererea oricărei părți, asigurând coordonarea, monitorizarea și facilitarea procesului de divulgare coordonată a vulnerabilităților;

4.5. *divulgare publică* – comunicarea informațiilor referitoare la o vulnerabilitate publicului, în condițiile și în termenele prevăzute de prezentul Regulament;

4.6. *organizație responsabilă* – furnizor de servicii care produce, pune la dispoziție sau administrează produsele sau serviciile TIC prevăzute la pct. 5;

4.7. *raportor* – orice persoană fizică sau juridică, inclusiv cercetători, specialiști ori alți participanți în domeniul securității cibernetice, care notifică, în mod voluntar și cu bună-credință, o vulnerabilitate identificată într-un produs sau serviciu TIC;

4.8. *remediere* – procesul de eliminare sau atenuare a vulnerabilității prin implementarea corecțiilor, a versiunilor noi, a actualizărilor de securitate sau a altor măsuri tehnice și organizatorice.

5. Prezentul Regulament se aplică vulnerabilităților descoperite în:

5.1. produsele și serviciile TIC utilizate de către furnizorii de servicii în Republica Moldova, indiferent de proveniența acestora;

5.2. componentele infrastructurii critice naționale din domeniul digital, inclusiv sistemele și rețelele informatice esențiale pentru funcționarea serviciilor de interes public sau național;

5.3. produsele și serviciile TIC dezvoltate, furnizate sau gestionate de furnizorii de servicii care își au sediul sau filiala în Republica Moldova;

5.4. serviciile TIC furnizate prin intermediul infrastructurilor de tip cloud, indiferent de localizarea geografică a infrastructurii, dacă acestea sunt utilizate de persoane fizice și/sau juridice din Republica Moldova.

6. Procesul de divulgare coordonată a vulnerabilităților se desfășoară cu respectarea următoarelor principii fundamentale:

6.1. *buna-credință* – standard de conduită a unei părți implicate (raportori, organizații responsabile, coordonatorul național), caracterizat prin corectitudine, onestitate, deschidere și respect față de interesele celeilalte părți, în scopul exclusiv al îmbunătățirii securității produselor și serviciilor TIC;

6.2. *responsabilitatea părților implicate* – raportarea, analiza și remedierea vulnerabilităților se realizează printr-o cooperare între raportori, organizațiile afectate și coordonatorul procesului, fiecare acționând potrivit rolului, competențelor și obligațiilor ce îi revin conform prezentului Regulament;

6.3. *proporționalitatea* – acțiunile întreprinse în cadrul procesului trebuie să fie limitate la ceea ce este strict necesar pentru identificarea, verificarea și raportarea vulnerabilităților, fără a afecta integritatea sau disponibilitatea sistemelor și datelor;

6.4. *confidențialitatea* – informațiile sensibile referitoare la vulnerabilitate, datele cu caracter personal ale raportorului și detaliile tehnice sunt tratate cu un nivel adecvat de confidențialitate, pentru a preveni exploatarea neautorizată sau divulgarea prematură;

6.5. *transparența și trasabilitatea* – procesul de divulgare și acțiunile subsecvente sunt documentate și trasabile, astfel încât să permită verificarea, auditarea și evaluarea eficienței acestora.

7. Toate persoanele fizice și juridice vizate de prevederile prezentului Regulament, inclusiv organizațiile responsabile și furnizorii de produse sau servicii TIC, au obligația de a coopera în mod activ și cu bună-credință cu coordonatorul național în procesul de notificare, analiză și remediere a vulnerabilităților, cu respectarea principiilor prevăzute în art. 5 din Legea nr. 48/2023 privind securitatea cibernetică și în pct. 6 din prezentul Regulament.

8. Coordonatorul național și toate părțile implicate în procesul de divulgare coordonată a vulnerabilităților au obligația de a păstra confidențialitatea informațiilor obținute pe durata procesului și după finalizarea acestuia, cu excepția cazurilor în care:

8.1. divulgarea este necesară pentru prevenirea unui risc iminent de compromitere a securității infrastructurilor critice sau a serviciilor esențiale, în baza unei evaluări documentate de risc efectuate de către coordonatorul național;

8.2. divulgarea este acceptată în mod expres, în scris, de către părțile interesate;

8.3. divulgarea este impusă de lege sau de o hotărâre judecătorească.

Capitolul II
ROLURI ȘI RESPONSABILITĂȚI ÎN CADRUL PROCESULUI DE DIVULGARE COORDONATĂ

Secțiunea 1
Coordonatorul național

9. Coordonatorul național, în calitate de autoritate responsabilă de procesul de divulgare coordonată a vulnerabilităților în domeniul securității cibernetice, are următoarele responsabilități principale:

9.1. acționează ca intermediar neutru și de încredere, facilitând, la cererea oricărei părți, comunicarea și cooperarea între raportor și organizația responsabilă de produsul sau serviciul TIC afectat;

9.2. asigură coordonarea generală a procesului, de la recepționarea notificării privind o vulnerabilitate până la închiderea cazului;

9.3. garantează protejarea informației privind identitatea raportorilor și confidențialitatea informațiilor sensibile furnizate pe parcursul procesului;

9.4. monitorizează evoluția procesului de remediere a vulnerabilităților notificate și intervine, la necesitate sau la cererea părților, pentru facilitarea dialogului sau medierea neînțelegerilor între părți;

9.5. asigură evidența raportorilor și a cercetătorilor în cadrul Registrului de stat al incidentelor cibernetice, care poate fi accesat de către organizațiile responsabile.

10. În vederea realizării responsabilităților sale, coordonatorul național desfășoară următoarele activități specifice:

10.1. identifică și contactează părțile relevante implicate în procesul de divulgare, inclusiv organizațiile responsabile de produsele sau serviciile TIC afectate;

10.2. oferă asistență tehnică și procedurală raportorilor, sprijinindu-i în întocmirea notificării și în înțelegerea cadrului legal și metodologic aplicabil;

10.3. instituie și menține un mecanism securizat pentru primirea notificărilor privind vulnerabilitățile, care asigură integritatea, confidențialitatea și disponibilitatea datelor transmise;

10.4. evaluează și prioritizează vulnerabilitățile raportate în funcție de nivelul de risc, de potențialul de exploatare și de impactul asupra infrastructurii critice sau a serviciilor esențiale;

10.5. stabilește și negociază, după caz, termenele pentru remediere și divulgare publică, cu implicarea ambelor părți (raportor și organizație responsabilă);

10.6. asigură trasabilitatea cazurilor, prin menținerea unei evidențe detaliate a vulnerabilităților notificate, a comunicărilor realizate și a măsurilor luate de către organizațiile implicate;

10.7. elaborează și aprobă norme metodologice, ghiduri, formulare și recomandări pentru aplicarea unitară a prezentului Regulament;

10.8. instituie și administrează un program de recompense, inclusiv financiare, pentru identificarea vulnerabilităților;

10.9. elaborează anual un raport privind divulgarea coordonată a vulnerabilităților, incluzând statistici agregate și recomandări pentru îmbunătățirea procesului, care se publică pe pagina oficială a instituției;

10.10. organizează activități de informare și sensibilizare, destinate raportorilor, organizațiilor responsabile și altor părți interesate;

10.11. colaborează cu autoritățile publice relevante din Republica Moldova, precum și cu partenerii internaționali.

11. În cazul în care o vulnerabilitate raportată ar putea avea un impact semnificativ asupra persoanelor fizice sau juridice din mai multe state sau ar afecta infrastructura critică cu caracter transfrontalier, în contextul realizării atribuțiilor prevăzute de Legea nr. 48/2023 privind securitatea cibernetică sau în temeiul obligațiilor care decurg dintr-un tratat internațional, coordonatorul național cooperează cu subdiviziunea responsabilă din cadrul Ministerului Afacerilor Externe și cu omologii din alte state și/sau organizații internaționale relevante în domeniul securității cibernetice.

12. Coordonatorul național acționează cu imparțialitate și evită orice conflict de interese în procesul de gestionare a vulnerabilităților, inclusiv în relația cu organizațiile responsabile sau raportorii implicați.

13. Coordonatorul național promovează notificarea voluntară a vulnerabilităților, asigurând respectarea drepturilor raportorilor în procesul de divulgare.

14. Coordonatorul național garantează confidențialitatea deplină a identității raportorului pe întreaga durată a procesului de divulgare coordonată a vulnerabilității, cu excepția cazurilor în care raportorul își exprimă în mod expres consimțământul scris pentru dezvăluirea identității sale.

15. Accesul la informațiile de identificare a raportorului este permis exclusiv persoanelor din cadrul coordonatorului național desemnate pentru a se implica direct în procesul de analiză și gestionare a vulnerabilității.

16. Coordonatorul național aplică măsuri tehnice și organizatorice necesare pentru protejarea informației privind identitatea raportorului.

Secțiunea a 2-a
Raportorii

17. Raportorii, în procesul de raportare a unei vulnerabilități, au obligația să respecte următoarele cerințe:

17.1. să acționeze cu bună-credință, fără intenție frauduloasă, fără a urmări obținerea unui beneficiu nejustificat sau provocarea prejudiciilor organizației responsabile, utilizatorilor finali ori terților;

17.2. să acționeze în limitele cadrului legal și cu respectarea principiului proporționalității, fără a compromite confidențialitatea datelor, integritatea produselor TIC ori disponibilitatea serviciilor TIC, exclusiv în măsura strict necesară pentru verificarea existenței vulnerabilității și asigurarea acurateței raportării;

17.3. să nu divulge public sau către terți, fără consimțământul expres al coordonatorului național, informații referitoare la vulnerabilitatea identificată, la produsul sau serviciul TIC afectat și la eventualele consecințe, până la remedierea completă a vulnerabilității sau până la expirarea unui termen rezonabil stabilit de comun acord cu coordonatorul național;

17.4. să obțină, înainte de efectuarea oricăror testări pentru identificarea vulnerabilităților, acordul expres și documentat al proprietarului sau administratorului sistemului TIC, care să cuprindă cel puțin identificarea părților, obiectul și perioada testărilor, tipurile de testări admise, limitările aplicabile și măsurile de confidențialitate;

17.5. să desfășoare testările strict în limitele acordului proprietarului sau administratorului sistemului TIC și să se abțină de la orice acțiuni neautorizate, precum și de la practici care ar putea crea riscul comiterii unor fapte din imprudență;

17.6. să nu utilizeze cunoștințele dobândite sau vulnerabilitățile identificate în scopuri personale, comerciale, competitive ori pentru obținerea de avantaje nelegitime;

17.7. să coopereze activ cu coordonatorul național și/sau cu organizația responsabilă pe durata întregului proces de gestionare a vulnerabilității, oferind, la solicitare, clarificări și informații suplimentare relevante;

17.8. să respecte eventualele măsuri de securitate, confidențialitate și condiții suplimentare stabilite în cadrul politicii de divulgare coordonată, publicate de către coordonatorul național sau de către organizația responsabilă;

17.9. să nu exploateze vulnerabilitatea sub nicio formă care depășește strictul necesar pentru confirmarea existenței și documentarea impactului potențial al acesteia.

18. Coordonatorul național poate institui și menține mecanisme de recunoaștere publică a raportorilor care au contribuit semnificativ la îmbunătățirea securității cibernetice, cu consimțământul prealabil al acestora. De asemenea, coordonatorul național încurajează organizațiile responsabile să implementeze propriile programe de recunoaștere sau de recompensare pentru raportarea vulnerabilităților.

Secțiunea a 3-a
Cercetătorii și participanții în domeniul securității cibernetice

19. Suplimentar cerințelor prevăzute la pct. 17, cercetătorii și participanții în domeniul securității cibernetice asigură respectarea următoarelor cerințe:

19.1. să desfășoare activitățile de cercetare și testare în conformitate cu prevederile cadrului normativ și cu limitele acordului coordonatorului național sau al organizației responsabile;

19.2. să respecte limitele și restricțiile specifice ale acordului coordonatorului național sau al organizației responsabile, inclusiv domeniile de aplicare, tipurile de produse sau servicii TIC și metodele de testare permise;

19.3. să documenteze în mod transparent metodele utilizate pentru identificarea vulnerabilităților și să păstreze un jurnal tehnic, care să poată fi pus la dispoziția coordonatorului național, la cerere, în scopul verificării și auditului, incluzând cel puțin:

19.3.1. descrierea testărilor și metodologiilor utilizate;

19.3.2. data și ora desfășurării fiecărei activități;

19.3.3. identificarea sistemelor, aplicațiilor sau componentelor testate;

19.3.4. rezultatele și constatările fiecărei etape de testare;

19.3.5. incidentele sau evenimentele neprevăzute survenite;

19.3.6. măsurile pentru protecția datelor și integritatea sistemelor;

19.3.7. persoanele implicate și responsabilitățile acestora;

19.4. să documenteze și să raporteze coordonatorului național orice conflict de interese, actual sau potențial, care ar putea influența obiectivitatea cercetării sau raportării;

19.5. să participe, la solicitarea coordonatorului național, la activități de clarificare, testare suplimentară sau evaluare de impact, în scopul sprijinirii procesului de remediere;

19.6. să nu desfășoare activități de identificare a vulnerabilităților asupra produselor sau serviciilor TIC în afara unui cadru controlat, agreat cu organizația responsabilă sau cu coordonatorul național;

19.7. să înștiințeze coordonatorul național, fără întârziere nejustificată, despre orice incident de securitate care ar putea compromite confidențialitatea informațiilor privind vulnerabilitățile în curs de investigare.

Secțiunea a 4-a
Obligațiile organizațiilor responsabile de produsele și serviciile TIC

20. Organizațiile responsabile de produsele sau serviciile TIC afectate de vulnerabilități au următoarele obligații:

20.1. să desemneze un punct de contact oficial pentru comunicarea cu coordonatorul național și cu raportorii;

20.2. să coopereze activ și cu bună-credință cu coordonatorul național și raportorii în procesul de evaluare și remediere a vulnerabilităților;

20.3. să confirme recepționarea notificării într-un termen de o zi lucrătoare și să inițieze, fără întârziere, măsurile de analiză și remediere necesare;

20.4. să informeze periodic coordonatorul național cu privire la progresul implementării remediilor și eventualele obstacole întâmpinate, prin mijloacele și în termenele stabilite de procedurile aprobate de către coordonatorul național;

20.5. să implementeze măsuri pentru remedierea vulnerabilităților într-un termen proporțional cu riscul identificat, stabilit pe baza evaluării riscului și detaliat în planul de remediere transmis coordonatorului național;

20.6. să evite inițierea măsurilor administrative, a procedurilor disciplinare sau a altor acțiuni interne împotriva raportorilor care acționează cu bună-credință, respectă cerințele legale și procedurale prevăzute de prezentul Regulament, cu excepția situațiilor în care există motive obiective și documentate, care indică o încălcare a legii ori provocarea unui prejudiciu;

20.7. să respecte termenele și condițiile convenite cu coordonatorul național privind divulgarea publică;

20.8. să analizeze și să integreze concluziile proprii și recomandările coordonatorului național rezultate în cadrul procesului de divulgare în politicile interne de securitate și dezvoltare a produselor TIC;

20.9. să evalueze dacă vulnerabilitatea raportată poate afecta și alți furnizori, clienți sau parteneri și, după caz, să informeze coordonatorul național, pentru o abordare coordonată.

21. Organizațiile responsabile pot elabora o politică proprie de divulgare coordonată a vulnerabilităților în corespundere cu prevederile prezentului Regulament, care se avizează de către coordonatorul național.

CAPITOLUL III
Etapele procesului de divulgare coordonată

Secțiunea 1
Notificarea inițială și recepționarea acesteia

22. Orice persoană fizică sau juridică, inclusiv cercetătorii și participanții în domeniul securității cibernetice, poate notifica, în mod voluntar și cu bună-credință, o vulnerabilitate identificată într-un produs sau serviciu TIC, utilizând platforma digitală pusă la dispoziție de către coordonatorul național.

23. Notificarea se face prin completarea formularului electronic disponibil pe platforma oficială a coordonatorului național, în conformitate cu procedurile și instrucțiunile publicate.

24. Coordonatorul național se asigură că vulnerabilitatea raportată este urmărită cu diligență și că identitatea raportorului este protejată.

25. Notificarea privind o vulnerabilitate trebuie să conțină cel puțin următoarele elemente esențiale:

25.1. identificarea produsului sau serviciului TIC afectat (nume, versiune, furnizor, context de utilizare);

25.2. descrierea detaliată a vulnerabilității, inclusiv natura, cauzele și mecanismul de exploatare;

25.3. evaluarea preliminară a impactului potențial asupra confidențialității, integrității și disponibilității sistemului sau serviciului;

25.4. metodologia utilizată pentru identificarea vulnerabilității, inclusiv instrumentele;

25.5. dovezile tehnice privind existența vulnerabilității, dacă sunt disponibile;

25.6. recomandările preliminare de remediere, în cazul în care pot fi formulate;

25.7. datele de contact ale raportorului (dacă nu optează pentru anonimat) și preferințele privind confidențialitatea identității și implicarea ulterioară.

26. Coordonatorul național confirmă primirea notificării în termen de o zi lucrătoare de la recepționare, atribuie un identificator unic cazului pentru trasabilitate și notifică acest fapt organizației responsabile.

27. În cazul notificărilor incomplete, dacă raportorul este identificabil, coordonatorul național solicită completarea informațiilor lipsă în termen de două zile lucrătoare.

28. Dacă notificarea primită nu conține toate elementele esențiale necesare pentru evaluare, iar raportorul nu are posibilitatea de a completa informațiile lipsă în termenul prevăzut la pct. 27, coordonatorul național inițiază procedura de verificare din oficiu, utilizând surse și instrumente proprii, precum și informațiile disponibile din alte registre sau sisteme relevante, în scopul confirmării și completării datelor necesare pentru continuarea procesului de divulgare coordonată a vulnerabilităților.

29. În cazul în care nu se confirmă existența vulnerabilității sau nu pot fi obținute elementele esențiale lipsă, coordonatorul național închide procedura de notificare, informând raportorul (dacă este identificabil) despre imposibilitatea continuării procesului, cu indicarea motivelor care au determinat închiderea acesteia.

30. Notificarea poate fi transmisă și direct organizației responsabile. În acest caz, aceasta are obligația să o redirecționeze coordonatorului național fără întârziere, dar nu mai târziu de o zi lucrătoare de la primirea acesteia.

31. În cazul în care vulnerabilitatea raportată poate afecta rețele sau sisteme informatice proprietate a statului la nivel guvernamental, organizația responsabilă transmite notificarea Centrului guvernamental de răspuns la

incidente cibernetice (CERT-Gov) în termen de o zi lucrătoare de la primirea acesteia, pentru a asigura gestionarea rapidă și coordonată a riscului.

32. În situația prevăzută la pct. 31, Centrul guvernamental de răspuns la incidente cibernetice participă activ la întregul proces de verificare, evaluare și remediere a vulnerabilității raportate, asigurând suport tehnic și monitorizarea implementării măsurilor corective.

33. Organizația responsabilă care primește o notificare directă trebuie să furnizeze coordonatorului național, în termen de 14 zile lucrătoare, următoarele documente:

33.1. confirmarea că raportorul a fost informat despre transferul notificării către coordonatorul național;

33.2. evaluarea preliminară a validității vulnerabilității raportate;

33.3. planul inițial de analiză și remediere, inclusiv persoanele de contact desemnate.

34. Dacă vulnerabilitatea raportată implică un risc iminent și critic pentru securitatea națională, infrastructura critică ori siguranța publică, coordonatorul național poate interveni și prelua integral coordonarea procesului, indiferent de destinatarul inițial al notificării. Coordonatorul național va informa organizația responsabilă cu privire la etapele examinării notificărilor de raportare.

35. În situații excepționale sau în cazul în care vulnerabilitatea raportată prezintă un risc iminent și critic pentru securitatea națională, infrastructura critică sau siguranța publică, coordonatorul național poate accepta notificări care nu conțin toate elementele esențiale, solicitând completarea ulterioară a informațiilor esențiale.

36. În sensul pct. 35, situația este calificată ca fiind excepțională dacă survine oricare dintre următoarele condiții:

36.1. afectează servicii esențiale;

36.2. exploatarea activă a vulnerabilității este efectuată de către entități neautorizate;

36.3. există posibilitatea de compromitere a infrastructurii critice sau a sistemelor guvernamentale;

36.4. există posibilitatea producerii unui prejudiciu patrimonial și/sau moral major asupra persoanelor fizice sau juridice;

36.5. există impact asupra securității datelor cu caracter personal.

37. În cazul identificării unei situații excepționale, coordonatorul național:

37.1. procesează notificarea în regim prioritar;

37.2. informează autoritățile competente sectoriale în termen de maximum două ore lucrătoare de la confirmarea riscului;

37.3. poate autoriza măsuri temporare de protecție sau limitare a impactului înainte de finalizarea investigației, cum ar fi suspendarea temporară a funcționalităților afectate, izolarea sistemelor compromise, restricționarea accesului la date sensibile, sau alte măsuri proporționale cu riscul identificat;

37.4. stabilește un calendar accelerat pentru procesul de remediere și divulgare.

38. În cazul notificărilor în masă (multiple vulnerabilități în același produs sau vulnerabilități similare în produse diferite), coordonatorul național este în drept să grupeze cazurile pentru o gestionare eficientă, să stabilească proceduri simplificate de raportare, să coordoneze o abordare unitară cu organizațiile responsabile și să prioritizeze vulnerabilitățile în funcție de impactul potențial.

39. În cazul în care vulnerabilitatea raportată este identificată într-un produs sau serviciu TIC furnizat de o parte terță, organizația responsabilă are obligația de a notifica de urgență furnizorul componentei respective și de a coopera cu acesta pentru obținerea unui remediu. Organizația responsabilă va informa periodic coordonatorul național despre stadiul comunicării cu furnizorul terț. Coordonatorul național poate, la rândul său, să faciliteze contactul cu furnizorul terț sau cu alți coordonatori naționali, dacă este cazul.

40. Coordonatorul național asigură interoperabilitatea cu platformele internaționale de raportare a vulnerabilităților, facilitând schimbul de informații cu partenerii din alte state sau organizații internaționale relevante.

Secțiunea a 2-a
Evaluarea și clasificarea vulnerabilităților

41. După recepționarea notificării complete, coordonatorul național inițiază procesul de evaluare tehnică, procedurală și contextuală a vulnerabilității raportate.

42. Evaluarea are ca scop determinarea următoarelor elemente:

42.1. validitatea tehnică a vulnerabilității raportate;

42.2. impactul potențial asupra confidențialității, integrității și disponibilității sistemelor afectate;

42.3. complexitatea exploatării și nivelul de cunoștințe necesare pentru valorificarea acesteia;

42.4. gradul de afectare a infrastructurilor, a serviciilor esențiale sau a utilizatorilor finali;

42.5. riscul de utilizare abuzivă sau de exploatare activă în lipsa unei gestionări corespunzătoare;

42.6. caracterul izolat sau sistemic al vulnerabilității (de exemplu, dacă afectează o clasă largă de produse, configurații sau implementări similare).

43. În cadrul evaluării, coordonatorul național este în drept:

43.1. să solicite clarificări tehnice suplimentare de la raportor sau de la organizația responsabilă;

43.2. să consulte alți experți tehnici sau organizații relevante (naționale sau internaționale), cu respectarea cerințelor de confidențialitate;

43.3. să utilizeze instrumente tehnice de testare și analiză pentru validarea vulnerabilității.

44. Vulnerabilitățile sunt clasificate în funcție de nivelul de risc estimat, utilizând o metodologie standardizată, cum ar fi sistemul CVSS (*Common Vulnerability Scoring System*), sau alte metodologii recunoscute la nivel internațional.

45. Evaluarea și clasificarea se realizează de către coordonatorul național în termen de cinci zile lucrătoare de la primirea notificării complete, cu posibilitatea de extindere a termenului în cazuri complexe, iar vulnerabilitățile sunt încadrate în una dintre următoarele categorii:

45.1. nivel critic – vulnerabilitate cu impact major asupra infrastructurii critice, ce permite compromiterea totală a sistemului fără a necesita interacțiunea utilizatorului;

45.2. nivel ridicat – vulnerabilitate care compromite date sensibile, integritatea sistemului sau funcționalități esențiale;

45.3. nivel mediu – vulnerabilitate cu impact localizat sau care necesită condiții specifice pentru a fi exploatată;

45.4. nivel scăzut – vulnerabilitate cu impact redus, dificultate mare de exploatare și risc minim.

46. În funcție de clasificare, coordonatorul național stabilește:

46.1. termenul maxim recomandat pentru remedierea vulnerabilității;

46.2. necesitatea de intervenție urgentă sau escaladare instituțională;

46.3. necesitatea de notificare a altor autorități;

46.4. planul preliminar pentru divulgarea controlată/publică, inclusiv termene și condiții.

47. Coordonatorul național comunică raportorului și organizației responsabile concluziile evaluării, incluzând:

47.1. rezultatele analizei tehnice și argumentele aferente;

47.2. nivelul de risc atribuit vulnerabilității;

47.3. termenele recomandate pentru implementarea măsurilor corective;

47.4. următoarele etape planificate, inclusiv cerințele de cooperare între părți.

48. La solicitarea oricărei părți, în cazul divergențelor între raportor și organizația responsabilă privind existența, gravitatea sau impactul vulnerabilității, coordonatorul național facilitează un proces de mediere tehnică, care poate include organizarea unei analize tehnice comune.

49. Analiza tehnică se efectuează în termen de 15 zile lucrătoare și poate include, după caz, testarea supervizată în mediu controlat, simularea scenariilor de exploatare sau alte acțiuni necesare, stabilite de comun acord între părțile implicate.

50. La finalizarea analizei tehnice comune, coordonatorul național emite o opinie tehnică motivată în termen de cinci zile lucrătoare, care cuprinde confirmarea sau infirmarea vulnerabilității, evaluarea impactului potențial și recomandările privind remedierea acesteia.

51. Coordonatorul național asigură trasabilitatea completă a procesului de evaluare, prin documentarea tuturor activităților desfășurate, a corespondenței cu părțile implicate, a metodologiilor aplicate și a concluziilor adoptate, în vederea asigurării auditabilității și transparenței decizionale.

Secțiunea a 3-a
Remedierea vulnerabilității și monitorizarea progresului

52. După finalizarea evaluării și clasificării, coordonatorul național transmite organizației responsabile toate informațiile relevante privind vulnerabilitatea și solicită un plan de remediere.

53. Organizația responsabilă elaborează și transmite coordonatorului național, în termen de 14 zile lucrătoare de la data recepționării informației indicate la pct. 52, un plan de remediere, care include:

53.1. confirmarea vulnerabilității și a nivelului de risc;

53.2. măsurile tehnice și organizatorice planificate pentru remediere;

53.3. termenele estimate pentru implementarea remediilor;

53.4. persoanele responsabile de implementare și comunicare;

53.5. eventualele constrângeri sau dependențe care pot afecta procesul de remediere.

54. Coordonatorul național analizează planul propus și, în cazul în care identifică riscuri sau întârzieri nejustificate, formulează observații motivate sau

solicită completarea planului cu măsuri suplimentare, notifică fără întârziere orice modificare a planului inițial, inclusiv amânări, schimbări de responsabilități sau descoperirea unor noi vulnerabilități asociate.

55. Pe toată durata procesului de remediere, organizația responsabilă comunică periodic coordonatorului național stadiul implementării măsurilor și notifică fără întârziere orice modificare a planului inițial sau apariția unor obstacole semnificative, prin mijloacele și în termenele stabilite de procedurile aprobate de către coordonatorul național.

56. Coordonatorul național este în drept să ofere, la solicitare, sprijin tehnic suplimentar, recomandări de bune practici sau consultări cu alți actori relevanți, în scopul facilitării unui proces eficient de remediere.

57. După finalizarea implementării măsurilor, organizația responsabilă transmite coordonatorului național un raport final de remediere, care cuprinde:

57.1. acțiunile realizate și termenele respectate;

57.2. testele de validare a eficienței remediilor;

57.3. eventualele măsuri preventive suplimentare implementate pentru produsul sau serviciul TIC, inclusiv modificări, controale sau proceduri menite să prevină exploatarea vulnerabilităților identificate;

57.4. concluziile formulate și modificările aduse proceselor interne.

58. Coordonatorul național validează închiderea cazului pe baza raportului final și a întrunirii condițiilor cumulative de la pct. 74, consemnează decizia în Registrul de stat al incidentelor cibernetice și informează raportorul, cu respectarea cerințelor de confidențialitate.

Secțiunea a 4-a
Procedura de divulgare publică

59. Divulgarea publică a unei vulnerabilități se realizează doar după finalizarea procesului de remediere sau dacă există un risc major pentru securitatea publică, iar organizația responsabilă nu a remediat vulnerabilitatea în termenul stabilit.

60. Coordonatorul național stabilește împreună cu raportorul și organizația responsabilă momentul optim și forma divulgării publice, în funcție de:

60.1. gradul de remediere atins și eficiența măsurilor implementate;

60.2. existența riscului sau existența unor exploatări active în spațiul cibernetic;

60.3. riscul rezidual și potențialul impact asupra utilizatorilor finali și asupra serviciilor esențiale;

60.4. interesul public, dreptul la informare și necesitatea protejării utilizatorilor prin măsuri de prevenție.

61. Divulgarea publică a unei vulnerabilități, efectuată după finalizarea procesului de remediere, va include o descriere generală a vulnerabilității, fără a menționa explicit furnizorul, serviciul sau sistemul afectat.

62. În cazul în care vulnerabilitatea identificată prezintă un risc major pentru securitatea publică și organizația responsabilă nu a remediat-o în termenul stabilit conform prezentului Regulament, coordonatorul național poate adopta decizia de divulgare publică a informațiilor privind vulnerabilitatea.

63. Decizia de divulgare se adoptă pe baza unei evaluări documentate și transparente a riscurilor, care include:

63.1. analiza gradului de severitate al vulnerabilității conform scalei sistemului CVSS (*Common Vulnerability Scoring System*);

63.2. evaluarea impactului potențial asupra securității publice, a infrastructurilor critice sau a serviciilor esențiale;

63.3. analiza probabilității de exploatare a vulnerabilității de către entități neautorizate;

63.4. justificarea organizației responsabile privind imposibilitatea remedierii în termen;

63.5. identificarea măsurilor alternative de protecție disponibile pentru utilizatori.

64. Coordonatorul național notifică în scris organizației responsabile, raportorului vulnerabilității și altor părți direct afectate decizia de divulgare publică cu cel puțin trei zile lucrătoare înainte de publicare.

65. În situații excepționale, în care întârzierea divulgării ar expune la riscuri semnificative și imediate securitatea publică sau siguranța persoanelor, coordonatorul național poate proceda la divulgare fără respectarea termenului de notificare prevăzut la pct. 64, cu condiția documentării motivelor care justifică urgența și a comunicării acestora părților implicate.

66. Decizia de divulgare publică este însoțită de recomandări practice pentru utilizatori privind măsurile de protecție și atenuare a riscurilor până la remedierea vulnerabilității.

67. Divulgarea publică a unei vulnerabilități, în situația în care există un risc major pentru securitatea publică și organizația responsabilă nu a remediat vulnerabilitatea în termenul stabilit, poate include următoarele informații:

67.1. descrierea generală a vulnerabilității fără detalii tehnice care ar putea facilita exploatarea;

67.2. produsele sau serviciile TIC afectate;

67.3. potențialul impact asupra utilizatorilor sau infrastructurilor;

67.4. recomandările tehnice destinate utilizatorilor pentru prevenire sau atenuare;

67.5. stadiul actual al remedierii (dacă este disponibil);

67.6. contactele utile pentru suport tehnic suplimentar din partea organizației responsabile sau a autorităților relevante.

68. Nu se vor publica date sensibile, detalii de exploatare sau informații care pot facilita atacuri cibernetice decât în cazurile în care această informație este deja cunoscută public sau este necesară pentru protecția utilizatorilor.

69. Divulgarea publică a unei vulnerabilități care afectează entități din domeniile financiar-bancar, energetic sau al comunicațiilor electronice se efectuează de către coordonatorul național după consultarea prealabilă a autorității competente sectoriale și cu luarea în considerare a recomandărilor acesteia privind momentul și modul divulgării.

70. Dacă o vulnerabilitate este confirmată într-un produs sau serviciu TIC declarat oficial de către organizația responsabilă ca fiind la sfârșitul ciclului de viață (*End of Life – EoL*), iar organizația refuză să ofere un remediu, coordonatorul național, după o evaluare de risc, poate decide o divulgare publică accelerată. Divulgarea va include, pe lângă informațiile standard, o avertizare clară pentru utilizatori privind statutul EoL al produsului și va oferi, în măsura posibilităților, recomandări de atenuare a riscului (măsuri compensatorii) sau de migrare către produse alternative suportate.

71. Coordonatorul național utilizează canale oficiale de comunicare (pagina oficială, platforme de alertare, buletine de securitate) și colaborează cu asociații profesionale și alți parteneri pentru diseminarea eficientă și responsabilă a informației.

72. După divulgarea publică, coordonatorul național continuă să monitorizeze posibile reacții, amenințări sau incidente asociate cu vulnerabilitatea divulgată și cooperează cu părțile implicate pentru a răspunde adecvat oricăror evoluții ulterioare.

Secțiunea a 5-a
Închiderea cazului

73. După finalizarea procesului de remediere și, după caz, a divulgării publice, coordonatorul național inițiază procedura de închidere a cazului și informează organizația responsabilă despre decizia respectivă.

74. Pentru închiderea formală a cazului sunt necesare următoarele condiții cumulative:

74.1. transmiterea, de către organizația responsabilă, a raportului final de remediere, conform pct. 57;

74.2. validarea, de către coordonatorul național, a eficienței măsurilor de remediere;

74.3. lipsa unor riscuri reziduale semnificative, care să necesite acțiuni suplimentare imediate;

74.4. informarea raportorului, cu respectarea cerințelor de confidențialitate, privind închiderea cazului.

75. Coordonatorul național întocmește o fișă de închidere a cazului, care include cel puțin:

75.1. data închiderii și identificatorul unic al cazului;

75.2. sinteza etapelor parcurse: notificare, evaluare, remediere, divulgare;

75.3. măsurile implementate și eficiența acestora;

75.4. concluzii și recomandări pentru îmbunătățirea procesului;

75.5. orice aspecte juridice, instituționale sau tehnice relevante constatate pe parcurs.

76. În cazurile cu relevanță semnificativă (incidente recurente, vulnerabilități sistemice, întârzieri nejustificate), coordonatorul național propune:

76.1. recomandări specifice autorităților competente privind îmbunătățirea cadrului normativ;

76.2. actualizarea procedurilor sau a ghidurilor tehnice de raportare și remediere;

76.3. includerea cazului într-un raport public anonimizat de bune practici sau avertismente.

77. După închiderea cazului, raportorul are dreptul să transmită, inclusiv în mod anonim, opinii privind procesul de interacțiune cu coordonatorul național și/sau cu organizația responsabilă, pentru a contribui la îmbunătățirea procesului de divulgare coordonată. Coordonatorul național colectează și analizează periodic aceste date pentru îmbunătățirea practicilor și a relațiilor de încredere.

78. Coordonatorul național, după închiderea unui caz, este în drept să desfășoare o analiză ulterioară împreună cu organizația responsabilă și, dacă este cazul, cu raportorul, pentru a emite recomandări privind îmbunătățirea proceselor interne de securitate, dezvoltare și testare.

79. Datele și documentația aferente cazurilor închise sunt păstrate în Registrul de stat al incidentelor cibernetice, pentru o perioadă de trei ani, în scopul asigurării trasabilității, auditabilității și evaluării periodice a eficienței procesului de divulgare coordonată.

NOTĂ DE FUNDAMENTARE

la proiectul Hotărârii Guvernului cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
Proiectul Hotărârii Guvernului cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice este elaborat de către Ministerul Dezvoltării Economice și Digitalizării, cu suportul Agenției pentru Securitate Cibernetică.
2. Condițiile ce au impus elaborarea proiectului actului normativ
2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ
Temeiul legal al elaborării proiectului de act normativ constituie art. 7 alin. (4) pct. 10) din Legea nr. 48/2023 privind securitatea cibernetică. Norma în cauză abilitează Agenția pentru Securitate Cibernetică (ASC), în calitate de autoritate competentă la nivel național în domeniul securității cibernetice, cu atribuțiile de coordonator al procesului de divulgare coordonată a vulnerabilităților, conform cadrului normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. Totodată, aprobarea proiectului derivă din angajamentele asumate prin Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029 (Capitolul 10 – Societatea informațională și mass-media, acțiunea nr. 36) și Planul național de reglementări pentru anul 2025 (acțiunea nr. 13).
2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative
Conform Programului de activitate al Guvernului „UE, pace, dezvoltare”, unul dintre obiectivele fundamentale din cadrul Priorității sectoriale „Guvernare eficientă” a Programului menționat, stabilește consolidarea securității cibernetice și a infrastructurii IT critice . În acest sens, în martie 2023, a fost adoptată Legea nr. 48/2023 privind securitatea cibernetică (în continuare – Legea nr. 48/2023), care stabilește cadrul normativ primar în domeniul securității cibernetice. Intrată în vigoare la data de 1 ianuarie 2025, Legea nr. 48/2023 are drept obiectiv general reglementarea principalelor elemente indispensabile implementării unui model de guvernanță eficient la nivel național în vederea protecției și asigurării securității rețelelor și sistemelor informatice, utilizate de către persoanele juridice, publice sau private, în procesul de prestare a serviciilor considerate a fi esențiale pentru susținerea unor activități societale și economice critice. Art.7 alin. (4) pct. 10) din Legea nr. 48/2023 desemnează Agenția pentru Securitate Cibernetică (ASC) în calitate de coordonator al procesului de divulgare coordonată a vulnerabilităților, conform cadrului normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. În exercitarea atribuțiilor de coordonator al procesului de divulgare coordonată a vulnerabilităților, Agenția urmează să: intermedieze și faciliteze interacțiunea dintre

persoana fizică sau juridică, care raportează o vulnerabilitate, și producătorul sau furnizorul de produse TIC ori servicii TIC, potențial vulnerabile, la cererea oricărei dintre persoanele respective; identifice și contacteze persoanele fizice sau juridice implicate; acorde asistență persoanelor fizice sau juridice care raportează o vulnerabilitate; negocieze calendarele de divulgare și gestionare a vulnerabilităților care afectează mai multe persoane; asigure anonimatul persoanelor fizice sau juridice care raportează o vulnerabilitate, în cazul în care acestea o solicită.

Conform publicațiilor Agenției UE pentru Securitate Cibernetică (ENISA), politicile naționale privind divulgarea coordonată a vulnerabilităților trebuie să cuprindă un cadru în care cercetătorii în domeniul securității cibernetice sunt autorizați și încurajați să analizeze produsele și serviciile TIC, respectând un set de norme și raportând vulnerabilitățile identificate autorităților naționale sau furnizorilor respectivelor produse. Un astfel de cadru contribuie semnificativ la creșterea nivelului general de securitate cibernetică, sporind transparența și consolidând încrederea în serviciile și produsele digitale utilizate la nivel național. În plus, acesta facilitează cooperarea între părțile implicate și eficientizează procesul de dezvoltare a patch-urilor sau a altor măsuri de atenuare, reducând astfel timpul în care vulnerabilitățile pot fi exploatate.[1]

Divulgarea coordonată a vulnerabilităților este esențială pentru protecția utilizatorilor, asigurând că informațiile despre vulnerabilități devin publice doar după ce părțile responsabile au implementat soluții sau măsuri de reducere a riscului de exploatare. Procesul implică de regulă cooperarea între multiple părți și se desfășoară conform unor reguli și pași convenți, cu implicarea activă a cercetătorilor, a coordonatorilor și a furnizorilor sau producătorilor de produse și servicii TIC.[2]

La nivelul Uniunii Europene, contextul politic și juridic actual reflectă o evoluție accelerată a politicilor privind divulgarea coordonată a vulnerabilităților (Coordinated Vulnerability Disclosure – CVD). Directiva NIS 2 instituie obligația pentru fiecare stat membru de a desemna un CSIRT național care să coordoneze divulgarea vulnerabilităților. CSIRT-ul național este investit cu rolul de intermediar de încredere, facilitând raportarea vulnerabilităților (inclusiv anonimă, la cererea raportorului), negociind termenele de divulgare și asigurând gestionarea adecvată a vulnerabilităților cu impact transfrontalier. De asemenea, Actul privind reziliența cibernetică (Cyber Resilience Act – CRA), intrat în vigoare la 10 decembrie 2024, introduce cerințe privind gestionarea, coordonarea și divulgarea vulnerabilităților, impunând obligații producătorilor de produse cu elemente digitale și ajustând practicile de coordonare la nivel administrativ.

Un rol central în gestionarea procesului CVD la nivel european îl deține Agenția UE pentru Securitate Cibernetică (ENISA). Aceasta dezvoltă și menține baza de date europeană a vulnerabilităților (European Vulnerability Database) și funcționează ca „CVE Numbering Authority" pentru vulnerabilitățile raportate prin rețeaua CSIRT a UE, atribuind identificatori unici CVE (Common Vulnerabilities and Exposures) și asigurând uniformitatea catalogării acestora. Totodată, ENISA oferă suport rețelei CSIRT în gestionarea raportării și coordonării vulnerabilităților, facilitează schimbul de informații și cooperarea între părți, și elaborează orientări, metodologii și recomandări pentru implementarea politicilor CVD la nivel național și sectorial, promovând astfel coerența și armonizarea practicilor între statele membre.

[1] European Union Agency for Cybersecurity (ENISA), *Coordinated Vulnerability Disclosure policies in the EU*, aprilie 2022, p.6.

[2] European Union Agency for Cybersecurity (ENISA), *Vulnerability Disclosure,* https://www.enisa.europa.eu/topics/vulnerability-disclosure (accesat 14.08.2025).

Totuși, implementarea politicilor naționale privind CVD în statele UE rămâne inegală și fragmentată: unele țări, precum Belgia, Franța, Lituania și Țările de Jos, au adoptat deja politici, în timp ce altele sunt în faza de evaluare, adoptare sau nu au demarat încă procesul de elaborare. Această diversitate reflectă provocările juridice, economice și politice cu care se confruntă guvernele naționale în dezvoltarea inițiativelor CVD, iar lipsa armonizării practicilor, terminologiei și metodelor de evaluare reprezintă un obstacol semnificativ pentru implementarea coerentă a politicilor și cooperarea între statele membre. În plus, statele membre au identificat provocări specifice precum riscurile legale pentru cercetători, stimulentele economice limitate pentru investigarea vulnerabilităților și dificultățile politice legate de rolul guvernului și de asigurarea unui cadru de protecție legală pentru cercetători.[3]

În prezent, în Republica Moldova nu există un mecanism juridic și procedural clar care să reglementeze procesul de raportare, evaluare, remediere și divulgare a vulnerabilităților în produsele și serviciile TIC. Absența unui cadru normativ coerent are mai multe consecințe negative: descurajează raportarea voluntară și responsabilă a vulnerabilităților, expune raportorii de bună-credință la riscuri, limitează capacitatea instituțională de a răspunde coordonat la amenințările cibernetice și, în cele din urmă, afectează securitatea infrastructurilor critice, subminând încrederea în serviciile publice digitale.

Proiectul hotărârii de Guvern are drept scop stabilirea cadrului normativ pentru implementarea unui mecanism standardizat de identificare, raportare și remediere a vulnerabilităților, contribuind la consolidarea securității cibernetice naționale și la alinierea cu standardele europene din domeniu. Intervenția este necesară pentru punerea în aplicare a prevederilor art. 7 alin. (4) pct. 10) din Legea nr. 48/2023 și transpunerea obligațiilor prevăzute în Directiva (UE) 2022/2555 (Directiva NIS 2), precum și asigurarea unui cadru coerent care să sprijine și reglementeze procesul de divulgare coordonată a vulnerabilităților în domeniul securității cibernetice.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul stabilește un cadru procedural pentru procesul de divulgare coordonată a vulnerabilităților în domeniul TIC. Elementele de noutate includ:

- definirea rolurilor și responsabilităților subiecților implicați (coordonator național, raportori, organizații responsabile, cercetători etc.);
- instituirea unui mecanism sigur de notificare și gestionare a vulnerabilităților;
- garanții legale pentru protejarea identității raportorilor;
- proceduri detaliate pentru evaluarea, clasificarea, remedierea și divulgarea publică a vulnerabilităților;
- stabilirea principiilor fundamentale ale procesului: bună-credință, proporționalitate, confidențialitate, trasabilitate și responsabilitate partajată.

Instituirea cadrului de divulgare coordonată a vulnerabilităților răspunde necesității de a echilibra interesele diferitelor categorii de actori implicați în securitatea cibernetică. Raportorii și cercetătorii în domeniul securității cibernetice care identifică vulnerabilități au nevoie de un cadru normativ clar, pentru a putea raporta vulnerabilitățile în mod responsabil, fără temeri privind consecințe negative. În același timp, organizațiile responsabile de produse

[3] European Union Agency for Cybersecurity (ENISA), *Coordinated Vulnerability Disclosure policies in the EU*, pp.6-7

și servicii TIC necesită un interval adecvat pentru remedierea vulnerabilităților înainte de divulgarea publică, pentru a preveni exploatarea acestora. Utilizatorii finali beneficiază de protecție directă, fiind informați și protejați împotriva exploatării vulnerabilităților nerezolvate. Procedurile standardizate și predictibile, precum și intermedierea de către un coordonator național neutru, facilitează cooperarea și reduc conflictele între părți. Mecanismul permite identificarea rapidă și remedierea eficientă a vulnerabilităților, sporind securitatea cibernetică la nivel național.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

Opțiunile alternative nu au fost analizate deoarece Republica Moldova, conform prevederilor art. 7 alin. (4) pct. 10) din Legea nr. 48/2023 privind securitatea cibernetică, care transpune Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), urmează să instituie un mecanism de divulgare coordonată a vulnerabilităților.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Implementarea Regulamentului privind divulgarea coordonată a vulnerabilităților va genera următorul impact asupra sectorului public:

- consolidarea capacității instituționale de gestionare a vulnerabilităților cibernetice prin instituirea unui mecanism standardizat și coordonat;
- îmbunătățirea nivelului de securitate cibernetică a sistemelor informaționale din sectorul public prin identificarea și remedierea vulnerabilităților;
- armonizarea practicilor de securitate cibernetică cu standardele europene, contribuind la procesul de integrare europeană;
- reducerea riscurilor de incidente cibernetice prin implementarea unui sistem proactiv de gestionare a vulnerabilităților;
- reducerea costurilor incidentelor. Conform studiilor ENISA, costul mediu al unui incident cibernetic major depășește semnificativ investițiile în prevenire; prin remedierea proactivă a vulnerabilităților, se evită costurile directe (recuperare sisteme, compensații) și indirecte (reputaționale, pierdere de încredere publică);
- îmbunătățirea colaborării interinstituționale în domeniul securității cibernetice;
- conformitatea cu standardele europene prin alinierea la cerințele Directivei NIS 2 care facilitează cooperarea cu CSIRT-urile din statele membre UE și accesul la resurse și expertiza la nivel european.

4.2. Impactul financiar și argumentarea costurilor estimative

Aprobarea proiectului nu implică costuri suplimentare imediate.

Totodată, menționăm că în scopul eficientizării cheltuielilor, datele și documentația aferente procesului de divulgare coordonată a vulnerabilităților vor fi luate la evidență în Registrul de stat al incidentelor cibernetice.

La moment proiectul HG privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice este în procedură de avizare.

4.3. Impactul asupra sectorului privat

Implementarea prevederilor Regulamentului vor genera următorul impact asupra sectorului privat:

- îmbunătățirea securității produselor și serviciilor digitale prin implementarea unui mecanism standardizat de raportare a vulnerabilităților;
- creșterea încrederii consumatorilor în produsele și serviciile digitale oferite;
- minimizarea daunelor reputaționale prin descoperirea și remedierea coordonată a vulnerabilităților care are rolul de a preveni scenariile în care acestea sunt făcute publice fără avertisment, afectând grav reputația companiei;
- armonizarea cu practicile internaționale în domeniul securității cibernetice, facilitând accesul pe piețele externe;
- dezvoltarea unei culturi proactive de securitate cibernetică în sectorul privat;
- reducerea riscurilor reputaționale și financiare asociate incidentelor cibernetice.

4.4. Impactul social

Implementarea Regulamentului privind divulgarea coordonată a vulnerabilităților va genera impact pentru societate prin:

- îmbunătățirea securității digitale și protejarea mai eficientă a datelor personale ale cetățenilor și a sistemelor pe care aceștia le utilizează;
- creșterea încrederii publice în serviciile digitale guvernamentale și private prin implementarea unor standarde înalte de securitate.

4.4.1. Impactul asupra datelor cu caracter personal

Proiectul a fost elaborat în conformitate cu Legea nr. 133/2011 privind protecția datelor cu caracter personal, iar toate părțile implicate sunt obligate să respecte cerințele privind confidențialitatea și protecția informațiilor sensibile.

4.4.2. Impactul asupra echității și egalității de gen

Nu este aplicabil.

4.5. Impactul asupra mediului

Nu este aplicabil.

4.6. Alte impacturi și informații relevante

Nu este aplicabil.

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Proiectul nu are ca scop transpunerea unui act juridic al Uniunii Europene, dar este compatibil cu bunele practici și recomandările în materie de divulgare coordonată (ex. ENISA, NIS2).

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Nu este aplicabil.

6. Avizarea și consultarea publică a proiectului actului normativ

În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional, la data de 22.07.2025 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de hotărâre de Guvern pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md (https://particip.gov.md/ro/document/stages/*/14884).

Proiectul a fost plasat pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md (https://particip.gov.md/ro/document/stages/*/15158).

Proiectul Hotărârii de Guvern a fost transmis Comisiei Europene pentru consultare la data de 03.12.2025. La data de 22.12.2025 reprezentanții DG ENEST au informat că opinia oficială urmează să fie transmisă după data de 15.01.2026 (întârziere cauzată de perioada concediilor). Totodată, s-a menționat că pentru a respecta termenul limită din Agenda de Reforme, este esențial ca Republica Moldova să aprobe proiectul Hotărîrii de Guvern în forma actuală, în timp ce ajustări suplimentare pot fi făcute ulterior în caz de necesitate, după eventualele comentarii parvenite din partea DG CNECT.

7. Concluziile expertizelor

Proiectul a fost supus expertizei juridice, cu luarea în considerare a obiecțiilor și propunerilor Ministerului Justiției.

Proiectul a fost examinat de Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător, cu luarea în considerare a obiecțiilor și propunerilor formulate.

Proiectul a fost supus expertizei anticorupție și expertizei juridice repetat în rezultatul cărora nu au fost prezentate obiecții și propuneri.

8. Modul de încorporare a actului în cadrul normativ existent

Ca urmare a aprobării proiectului dat nu va fi necesară operarea unor modificări în cuprinsul altor acte normative.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

După aprobarea proiectului, Agenția pentru Securitate Cibernetică:

- va asigura crearea Registrului de stat al incidentelor cibernetice;
- va dezvolta platforma digitală destinată recepționării, procesării și gestionării notificărilor privind vulnerabilitățile în domeniul securității cibernetice;
- va elabora ghiduri metodologice pentru implementarea procedurilor de divulgare coordonată a vulnerabilităților;
- va organiza sesiuni de informare pentru raportori și organizații responsabile.

Secretar de Stat **Michelle ILIEV**

SINTEZA

obiecțiilor și propunerilor/recomandărilor la proiectul de hotărâre de Guvern

„Cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice”

(număr unic 714/MDED/2025)

PRIMA AVIZARE

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Cancelaria de Stat** *(Nr. 10-108-9591 din 12.09.2025)*		Proiectul de act normativ instituie cadrul procedural pentru raportarea coordonată a vulnerabilităților (CVD) pentru autorități/instituții publice și prestatori de servicii TIC aferente. Totodată, Nota de fundamentare la proiect descrie necesitatea, impactul estimat și corelările cu cadrul normativ în vigoare. În acest context, constatăm unele diferențe de abordare în procesul de reglementare și venim cu unele propuneri la proiect: - Uniformizarea terminologiei pe tot parcursul textului (ex.: „control” vs. „inspecție”; „raportare” vs. „sesizare”).	Se acceptă. Proiectul a fost revizuit ținând cont de propunerea formulată.
			- Trimiteri clare la prevederile actelor normative invocate, cu integrarea acestora în context.	Se acceptă. Proiectul a fost revizuit ținând cont de propunerea formulată.
			- Referitor la domeniul de aplicare, se va asigura precizarea expresă a autorităților/instituțiilor vizate și a prestatorilor (inclusiv operatori critici, entități cu servicii digitale publice).	Se acceptă. Conform prevederilor art. 7 alin. (4) pct. 10 din Legea nr. 48/2023, autoritatea națională competentă în domeniul securității cibernetice, desemnată de Guvern (Agenția pentru Securitate Cibernetică), exercită atribuțiile de coordonator al procesului de divulgare coordonată a vulnerabilităților. În ceea ce privește prestatorii asupra cărora se aplică prezentul regulament, este de menționat că definiția noțiunii de „organizație responsabilă” a fost

				revizuită. Conform acesteia, regulamentul se aplică furnizorilor de servicii care produc, pun la dispoziție sau administrează produse sau servicii TIC prevăzute la pct. 5 din Regulament și pentru care a fost identificată o vulnerabilitate. Noțiunea de „furnizor de servicii” este definită în a vulnerabilităților.
			- La compartimentul definiții, urmează a fi asigurată clarificarea mai explicită a termenilor de „vulnerabilitate”, „divulgare coordonată”, „cercetător în securitate”, precum și includerea semnificației pentru „activitatea de testare responsabilă”.	Precizare. Termenii „vulnerabilitate” și „divulgare coordonată a vulnerabilităților” sunt definiți în Legea nr. 48/2023 și, în cadrul prezentului regulament, sunt utilizați cu sensul stabilit de lege. Proiectul nu utilizează noțiunea de „activitate de testare responsabilă”.
			- Referitor la Punct de contact oficial, este necesară stabilirea modalității de raportare (adrese, platformă, chei PGP), cu termene fixe pentru confirmarea primirii (de ex. 7 zile), pentru triere (de ex. 14 zile) și pentru răspuns/remediere etapizată.	Se acceptă. Prevederile Capitolului III din proiectul Regulamentului au fost revizuite și completate cu norme din care să rezulte cu certitudine modul și de termenii de notificare și raportare. De asemenea, coordonatorul național în conformitate cu prevederile Regulamentului va elabora și aproba proceduri și ghiduri metodologice care vor detalia aspectele procedurale ale procesului de divulgare coordonată a vulnerabilităților în domeniul securității cibernetice.
			- În partea ce vizează rolurile și responsabilitățile în cadrul procesului de divulgare coordonată, se va include rolul CERT guvernamental/național în coordonarea interinstituțională,	Se acceptă parțial. Proiectul Regulamentului a fost completat cu noi prevederi din care

			mecanismele de escaladare și de raportare a incidentelor majore.	rezultă necesitatea informării și implicării Centrului guvernamental de răspuns la incidente cibernetice în procesul de de evaluare, remediere și verificare a vulnerabilității. Centrul guvernamental de răspuns la incidente cibernetice urmând să acționeze în conformitate cu prevederile Legii nr. 48/2023 și a cadrului normativ subsecvent aplicabil. În partea ce ține de rolul de CERT național este de menționat că autoritatea competentă în conformitate cu art. 7 alin. (4) pct. 10 din Legea nr. 48/2023, în realizarea funcției de echipă de răspuns la incidentele cibernetice la nivel național exercită atribuțiile de coordonator al procesului de divulgare coordonată a vulnerabilităților.
			- În ceea ce ține de procesul de publicare în bazele de date publice, devine necesară asigurarea unei politici de divulgare a informațiilor coordonată (cu termene fixe sau orientative de publicare după remediere; excepții motivate etc).	Se acceptă. Proiectul a fost revizuit ținând cont de propunerile formulate.
			- Referitor la procesul de raportare a unei vulnerabilități de către raportori, se vor include indicatorii de monitorizare și raportare (ex. număr rapoarte, timp mediu de remediere), responsabilitățile și periodicitatea procesului.	Se acceptă. Proiectul a fost revizuit ținând cont de propunerile formulate.
			- Sub aspectul corelărilor normative, se va asigura verificarea compatibilității cu regimul contravențional/penal și cu legislația privind securitatea cibernetică, achizițiile publice și serviciile publice digitale în caz de încălcare a obligațiilor instituite prin proiect.	Se acceptă. Proiectul a fost revizuit ținând cont de propunerile formulate.

			- În Nota de fundamentare, urmează a fi consolidat aspectul ce vizează implementarea proiectului, și anume în: resursele, procesul de instruire și calendarul instructiv aferent; estimarea impactului bugetar și asupra capacităților instituționale.	Se acceptă parțial. Nota de fundamentare a fost completată cu prevederi suplimentare privind costurile. În etapa inițială, gestionarea procesului de divulgare coordonată a vulnerabilităților va fi asigurată de personalul existent al Agenției pentru Securitate Cibernetică, care dispune de competențele necesare în domeniul securității cibernetice. Resursele umane suplimentare, procesul de instruire specializată și calendarul instructiv aferent nu pot fi estimate cu precizie la acest moment, deoarece depind de factorii operaționali care vor deveni evidenți în practica aplicării regulamentului, precum volumul și complexitatea raportărilor de vulnerabilități. Planificarea detaliată a acestor aspecte va fi realizată pe baza datelor și experiențelor acumulate în primele perioade de implementare, permițând o dimensionare adecvată a capacităților instituționale în raport cu cerințele reale.
2.	**Aparatul Președintelui Republicii Moldova** *(Nr. 2/2-06-1442 din 18.09.2025)*		Lipsa de obiecții.	S-a luat act.
3.	**Ministerul Infrastructurii și Dezvoltării Regionale** *(Nr. 05-5103 din 24.09.2025*		Lipsa de obiecții și propuneri.	S-a luat act.

4.	**Ministerul Energiei** *(Nr. 02-2503 din 23 septembrie 2025)*		În Capitolul II, Secțiunea 4 propunem să fie modificată denumirea secțiunii din „Organizațiile responsabile” în „Obligațiile organizațiilor responsabile pentru produse și servicii TIC”. La aceiași secțiune având în vedere că domeniul energetic face parte din sectoarele infrastructurii critice, impactul vulnerabilităților cibernetice identificate în acest domeniu poate genera consecințe grave la nivel social, economic și de siguranță. În acest context, termenele de notificare și remediere nu pot fi lăsate exclusiv la negocierea părților. Pentru infrastructurile critice se stabilesc termene stricte notificarea către Coordonatorul național și către autoritatea competentă sectorială în maximum 24–48 de ore de la identificarea vulnerabilității, implementarea măsurilor de remediere în termene clare și obligatorii, stabilite prin acte normative secundare. Proiectul Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice prevede obligația păstrării confidențialității pe parcursul procesului de notificare și remediere a vulnerabilităților. Totuși, în forma actuală a documentului nu sunt clar definite mecanismele de clasificare și protecție a informațiilor sensibile care ar putea fi transmise în cadrul acestui proces. Această lipsă de reglementare explicită generează riscul ca informații cu caracter sensibil sau chiar critic pentru funcționarea unor infrastructuri esențiale să fie divulgate neautorizat ori utilizate abuziv. Pentru a asigura un cadru coerent și sigur, este necesară completarea Regulamentului cu prevederi detaliate privind clasificarea informațiilor, nivelurile de acces, procedurile de stocare, transmitere și distrugere a acestora.	Se acceptă parțial. Regulamentul stabilește cadrul general și responsabilitățile părților, iar termenele de remediere trebuie adaptate în funcție de gravitatea, complexitatea și contextul fiecărui caz, fără a impune limite rigide prin actul de bază. Termenele stricte pentru infrastructurile critice pot fi stabilite ulterior prin reglementări sectoriale sau proceduri operaționale specifice. Vulnerabilitățile conform prevederilor proiectului urmează a fi clasificate în funcție de nivelul de risc estimat, utilizând o metodologie standardizată, cum ar fi sistemul CVSS (Common Vulnerability Scoring System). Raportarea vulnerabilităților și activitățile de remediere se vor realiza prin intermediul unor soluții informatice puse la dispoziție de ASC, iar reglementarea și modul de funcționare a acestora se va stabili în conformitatea cu Legea nr. 467/2003 cu privire la informatizare şi la resursele informaţionale de stat, la etapa instituirii acestora.
5.	**Ministerul Finanțelor**		***Referitor la proiectul hotărârii:***	*(aviz plasat pe platforma legiferare.gov.md)*

	(Nr. 07/3-03-172/1417 din 30.08.2025)			
			În pct. 4 subpct.4.1 la noțiunea ,,cercetător sau participant în domeniul securității” se va completa cu cuvîntul ,,cibernetice”, prin prisma subpunctului 15.1 și a punctului 19 din prezentul proiect. De asemenea, proiectul se va completa cu un punct nou despre entitatea care va asigura controlul asupra executării prezentei hotărâri.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Referitor la prevederile pct.10 subpct.8, privind responsabilitatea coordonatorului național de elaborare a unui raport anual privind divulgarea coordonată a vulnerabilităților, se consideră necesară completarea proiectului de act normativ cu prevederi referitor la finalitatea acestui raport (către cine se va prezenta, dacă va fi publicat pe pagina web etc)	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La pct. 58 pentru asigurarea clarității, înțelegerii corecte și evitării ambiguității, se sugerează revederea sintagmei ,,media de specialitate”, întrucît legislația Republicii Moldova nu operează cu astfel de termeni.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La pct. 61, subpct.61.1, se propune revizuirea referinței la pct. 51, deoarece acesta prevede atribuțiile coordonatorului național în caz de neremediere de către organizația responsabilă a vulnerabilităților, și nu prevede obligativitatea acesteia de transmitere a raportului vizat. În același timp, se recomandă revizuirea și a expresiei ,,raport final de remediere”, având în vedere că pct. 49 operează cu termenul de ,,raport de finalizare”.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La pct. 64 se propune înlocuirea expresiei ,,entitate responsabilă” cu noțiunea ,,organizație responsabilă”, pentru a evita interpretările eronate și pentru a uniformiza utilizarea acestei noțiuni pe tot parcursul textului Regulamentului vizat.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			În același timp, în prevederile Regulamentului se indică despre faptul că datele și documentația aferente procesului de divulgare coordonată sunt păstrate în registrul național de evidență a vulnerabilităților gestionate, însă, pe lîngă faptul că acesta este ținut de Coordonatorul național, precum și perioada de păstrare	Se acceptă parțial. Proiectul a fost revizuit, datele și documentația aferente procesului de divulgare coordonată a vulnerabilităților vor fi luate la

			a datelor și documentației din registru, nu există o altă reglementare despre forma (fizică sau electronică) și conținutul acestuia sau dacă aceste aspecte vor fi reglementate de Guvern sau de sine stătător printr-un act normativ intern al Coordonatorului național. Prin urmare, considerăm necesar reglementarea de către autor în prezentul proiect despre aceste aspecte referitoare la registrul național de evidență a vulnerabilităților gestionate.	evidență în Registrul de stat al incidentelor cibernetice. La moment proiectul HG privind privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice este în procedură de avizare.
			Referitor la Nota de fundamentare la proiect.	
			Potrivit argumentărilor expuse la compartimentul 4.2 privind impactul financiar și argumentarea costurilor estimatative, autorul indică că implementarea prevederilor proiectului nu implică costuri suplimentare imediate. Totuși, proiectul prevede ca Agenția pentru Securitate Cibernetică să implementeze soluții digitale pentru gestionarea divulgării coordonate și menținerea registrului național de evidență a vulnerabilităților. Însă autorul nu prezintă costurile estimative și sursa de acoperire a acestora. Prin urmare, în nota informativă urmează a fi clarificat subiectul privind costurile necesare pentru fiecare acțiune în parte, volumul cheltuielilor planificat în acest sens și subprogramele bugetare relevante, precum și susținerea/asistența ce se planifică a fi oferită de partenerii de dezvoltare. Cu titlu de informare, în proiectul Cadrului bugetar pe termen mediu pentru anii 2026- 2028 care se află la etapa de promovare au fost incluse cheltuieli la Subprogramul 1504 „Tehnologii informaționale" pentru asigurarea activităților Agenției pentru Securitate Cibernetică după cum urmează: 25 916,5 mii lei (anul 2026), 25 916,5 mii lei (anul 2027) și 20 916,5 mii lei (anul 2028). Aceste cheltuieli includ alocațiile suplimentare în anii 2026 și 2027 în sumă a câte 5,0 mil lei, pentru dezvoltarea	Se acceptă parțial. Nota de fundamentare a fost revizuită. Totodată, menționăm că în scopul eficientizării cheltuielilor, datele și documentația aferente procesului de divulgare coordonată a vulnerabilităților vor fi luate la evidență în Registrul de stat al incidentelor cibernetice. La moment proiectul HG privind privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice este în procedură de avizare.

			și configurarea infrastructurii digitale și a sistemelor informaționale necesare în domeniul securității cibernetice.	
6.	**Ministerul Mediului** *(Nr. 13-05/2626 din 22.09.2025)*		Lipsa de obiecții și propuneri.	S-a luat act.
7.	**Ministerul Sănătății** *(Nr. 27/3035 din 25.09.2025)*		Lipsa de obiecții și propuneri.	*(aviz plasat pe platforma legiferare.gov.md)*
8.	**Ministerul Agriculturii și Industriei Alimentare** *(Nr. 2025PHG-2627 din 19.09.2025)*		**1. Obiecţii argumentate la Regulament:**	
			pct. 4, în urma analizei listei de noțiuni, putem constata că normele care definesc noțiunile (divulgare coordonată a vulnerabilităților, furnizor de servicii, produs al tehnologiei informației și comunicațiilor (produs TIC), serviciu al tehnologiei informației și comunicațiilor (serviciu TIC), vulnerabilitate) fac trimitere la Legea nr. 48/2023 privind securitatea cibernetică, în acest sens recomandăm excluderea noțiunilor respective din lista stabilită la pct. 4 din Regulament, având ca obiectiv eliminarea prevederilor legislative redundante;	Se acceptă. Proiectul a fost revizuit conform propunerii.
			pct.6.1, propunem expunerea principiului bunei-credințe în următoarea redacție *„standard de conduită a unei părți implicate (raportori, organizații responsabile, coordonatorul național), caracterizat prin corectitudine, onestitate, deschidere şi luarea în cont a intereselor celeilalte părți, în scopul exclusiv al îmbunătățirii securității produselor și serviciilor TIC”*, deoarece actuala formulare a principiului bunei-credințe nu conține o individualizare a elementelor bunei-credințe;	Se acceptă. Proiectul a fost revizuit conform propunerii.
			pct. 7, propunem înlocuirea termenului *„entități”* cu sintagma *„persoane fizice și juridice”*, deoarece inclusiv persoanele fizice au obligația de a coopera cu coordonatorul național, în situația în care raportează o vulnerabilitate;	Se acceptă. Proiectul a fost revizuit conform propunerii.
			pct. 18, autorul proiectului menționează că toate părțile implicate în procesul de divulgare coordonată trebuie să respecte principiile transparenței, responsabilității și proporționalității, în opinia	Se acceptă de principiu.

			Ministerului părțile implicate trebuie să respecte în primul rând principiile enunțate la art. 5 din Legea nr. 48/2023, în al doilea rând principiile enumerate la pct. 6 din Proiect, deci autorul urmează să modifice conținutul pct. 18;	Prevederile de la pct. 18 au fost excluse din proiect și pct. 7 a fost completat cu trimiteri la art. 5 din Legea nr. 48/2023 privind securitatea cibernetică.
			pct. 20, faptul că autorul proiectului exhaustiv enumeră limbile în care poate fi făcută o notificare, în opinia Ministerului îngrădește dreptul raportorului de a comunica o vulnerabilitate a produselor/serviciilor TIC, or din interpretarea pct. 20 reiese că formularea unei notificări într-o altă limbă, decât cele enumerate, duce la refuzul de a examina o asemenea notificare;	Se acceptă. Proiectul a fost revizuit conform propunerii.
			pct. 21, autorul proiectului stabilește că *„Persoanele fizice sau juridice care raportează cu bună credință o vulnerabilitate cibernetică, în condițiile prevăzute de prezentul regulament, beneficiază de protecție împotriva răspunderii juridice, civile sau penale”*, în urma analizei normei vizate rezultă că, printr-o hotărâre de Guvern sunt stabilite forme de protecție împotriva răspunderii juridice, ceea ce contravine ierarhiei actelor normatice, și anume art. 72 alin. (3) lit. n) prevede că prin lege organică se reglementează infracţiunile, pedepsele şi regimul executării acestora, în acest sens dreptul de a beneficia de protecție și formele acesteia trebuie să fie aprobate în Legea nr. 48/2023 privind securitatea cibernetică;	Se acceptă. Prevederile de la pct. 21 au fost excluse din proiect.
			Capitolul III, Secțiunea 1, propunem completarea secțiunii cu un pct. care să reglementeze modul de autosesizare a coordonatorului național în cazul parvenirii unei notificări care nu conține toate elementele esențiale și raportorul nu are posibilitate de suplinire a notificărilor cu elementele lipsă, în termen de 48 de ore lucrătoare;	Se acceptă. Proiectul a fost completat cu prevederi din care rezultă obligația coordonatorului național de întreprinde unele acțiuni atunci când notificarea este incompletă.
			pct. 62.2, conform pct. 53 din proiect, divulgarea publică a vulnerabilității se realizează după finalizarea procesului de remediere, deci rezultă că divulgarea publică este o etapă obligatorie a procesului de remediere, în acest sens mențiunea *„(după caz)”* de la pct. 62.2 urmează să fie exclusă;	Se acceptă. Proiectul a fost revizuit conform propunerii.
			pct. 66, considerăm necesar substituirea textului *„orice neconformitate gravă sau repetată cu prevederile prezentului*	Se acceptă de principiu. Punctul a fost exclus.

			Regulament” cu textul *„încălcarea prevederilor prezentului Regulament”*, deoarece din momentul comiterei unei fapte ilicite, indiferent de circumnstanțele care o individualizează, urmează să survină răspunderea juridică;	
			pct. 67, propunem excluderea pct. vizat, din motivul că repetă prevederile pct. 10.7, 10.8, 10.9 din proiect;	Se acceptă. Proiectul a fost revizuit conform propunerii.
			2) Propuneri care poartă caracter de recomandare *În Regulament:*	
			pct. 1, propunem expunerea sintagmei *„cadrul juridic și procedural”* în următoarea redacție *„cadrul juridic material și procedural”*, din motivul că Regulamentul conține norme materiale și procedurale privind notificarea, evaluarea, remedierea și divulgarea coordonată a vulnerabilităților produselor și serviciilor tehnologiei informației și comunicațiilor (TIC);	Se acceptă. Proiectul a fost revizuit conform propunerii.
			pct. 6.4, propunem completarea sintagmei *„datele raportorului”* cu cuvintele *„cu caracter personal”*, din considerentul că Legea nr. 133/2011 privind protecția datelor cu caracter personal, definește noțiunea de *„date cu caracter personal”* și se asigură protecția datelor cu caracter personal;	Se acceptă. Proiectul a fost revizuit conform propunerii.
			pct. 29, propunem expunerea sintagmei *„notificări parțiale”* în următoarea redacție *„notificări care nu conțin toate elementele esențiale”*, fiindcă pct. 23 stabilește exhaustiv elementele esențiale ale unei notificări;	Se acceptă. Proiectul a fost revizuit conform propunerii.
			pct. 30.2, nu este clar ce se înțelege prin termenul *„actori malițioși”* și ce persoane fizice/juridice sunt atribuite la categoria respective;	Se acceptă. Termenul „actori malițioși” a fost substitui cu termenul „entități neautorizate”.
			pct. 30.4, propunem substituirea expresiei *„fizic, financiar sau reputațional major”* cu cuvintele *„patrimonial și/sau moral”* din motivul că prejudiciul poate avea două forme patrimonial sau moral conform art. 1998 alin. (1) Cod civil.	Se acceptă. Proiectul a fost revizuit conform propunerii.
9.	**Ministerul Apărării** *(Nr. 11/1147 din 16.09.2025)*		Lipsa de obiecții.	S-a luat act.
10.	**Ministerul Afacerilor Interne**		Lipsa de obiecții și propuneri.	S-a luat act.

	(Nr. 30/ 3399 din 23.09.2025)			
11.	**Ministerul Afacerilor Externe** *(Nr. DI/3/041-9792 din 22.09.2025)*		Expunerea punctului 11 în următoarea redacție: *„11. În cazul în care o vulnerabilitate raportată ar putea avea un impact semnificativ asupra organizațiilor responsabile sau entităților din mai multe state sau ar afecta infrastructura critică cu caracter transfrontalier, coordonatorul național cooperează cu subdiviziunea responsabilă din cadrul MAE și cu omologii săi din alte state și/sau organizații internaționale relevante în domeniul securității cibernetice.”*	Se acceptă. Proiectul a fost revizuit conform propunerii.
12.	**Ministerul Educației și Cercetării** *(Nr. 08/3-09/6991 din 12.09.2025)*		Lipsa de obiecții și propuneri.	S-a luat act.
13.	**Ministerul Muncii și Protecției Sociale** *(Nr. 22/4485 din 22.09.2025)*		Lipsa de obiecții și propuneri.	S-a luat act.
14.	**Ministerul Culturii** *(Nr. 05/4-09/2695 din 16.09.2025)*		Lipsa de obiecții și propuneri.	S-a luat act.
15.	**Ministerul Justiției** *(Nr. 04/1-9296 din 22.09.2025)*		***La proiectul hotărârii***, după textul „art. 225)” se va completa cu textul „ , cu modificările ulterioare”	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La proiectul Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității ciberneticii:	
			La **pct. 1**, având în vedere caracterul interpretabil și imprevizibil al expresiei „intereselor publice”, fapt confirmat și prin jurisprudența Curții Constituționale, se recomandă evitarea utilizării cuvintelor menționate în textul proiectului de act normativ.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La **pct. 4**, textul „În sensul prezentului Regulament, următoarele noțiuni semnifică” se va substitui cu textul „În	Se acceptă.

			prezentul Regulament se utilizează noțiunile definite în Legea nr. 48/2023 privind securitatea cibernetică, precum și următoarele noțiuni: ”. Totodată, având în vederea propunerea indicată *supra,* subpct. 4.3, 4.5, 4.7, 4.10 și 4.11 se vor exclude.	Proiectul a fost revizuit conform propunerii.
			La **subpct. 9.4**, după cuvintele „la nevoie” se recomandă completarea cu cuvintele „sau la cererea părților”. În acest sens, se notează că, potrivit art. 7 alin. (4) pct. 10 lit. a) din *Legea nr. 48/2023 privind securitatea cibernetică,* coordonatorul național intermediază și facilitează interacțiunea dintre persoana fizică sau juridică, care raportează o vulnerabilitate, și producătorul sau furnizorul de produse TIC ori servicii TIC, potențial vulnerabile, la cererea oricărei dintre persoanele respective.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Potrivit **pct. 11**, „În cazul în care o vulnerabilitate raportată ar putea avea un impact semnificativ asupra organizațiilor responsabile sau entităților din mai multe state sau ar afecta infrastructura critică cu caracter transfrontalier, coordonatorul național cooperează cu omologii săi din alte state și/sau organizații internaționale relevante în domeniul securității cibernetice.” În acest sens, se consideră relevantă desfășurarea/concretizarea modalității/regulilor în baza cărora se va desfășura cooperarea între autoritățile statelor vizate în contextul raportării unei vulnerabilități (ex. tratate/acorduri sau alte instrumente de colaborare în materia asigurării securității cibernetice la nivel regional/internațional).	Se acceptă. Proiectul a fost revizuit conform propunerii.
			În conformitate cu **subpct. 14.5** din proiect, anterior efectuării unor testări în vederea identificării unor vulnerabilități, raportorul urmează să obțină „acordul expres și documentat” al proprietarului sau administratorului sistemului TIC. Cu referire la acest aspect, având în vedere că acordul nominalizat reprezintă actul în baza căruia urmează a fi permisă realizarea unor testări de către raportor, se consideră judicioasă indicarea elementelor/mențiunilor obligatorii ale acestuia (ex. identificarea părților, obiectul testării, perioada de testare,	Se acceptă. Proiectul a fost revizuit conform propunerii.

			tipurile de testări admisibile, limitări, măsuri de confidențialitate, etc.). Recomandarea indicată mai sus se consideră relevantă în vederea neadmiterii unor neclarități sau abuzuri/depășiri ale limitelor de acționare a raportorului în procesul de testare a vulnerabilităților unui sistem TIC. În continuare, potrivit aceleiași prevederi, raportorul se va abține de la utilizarea oricăror „practici lipsite de etică”. În acest context, nu este clar care sunt acele acțiuni ce pot fi considerate ca fiind practici lipsite de etică, fapt care ar putea crea interpretări diferențiate și improprii în raport cu anumite cazuri. Drept urmare, se consideră necesară clarificarea aspectului evidențiat. Adițional, din punct de vedere logico-juridic, este eronată utilizarea verbului „a se abține” în raport cu cuvintele „practici imprudente”. Din aceste considerente, se recomandă substituirea cuvintelor „sau imprudente” cu cuvintele „sau care ar putea crea riscul comiterii unor fapte din imprudență”.	
			La **subpct. 15.4**, se consideră oportună indicarea expresă a conținutului/categoriilor de informații ce urmează a fi incluse în jurnalul tehnic.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La **subpct. 15.7**, se face referire la necesitatea obținerii unei „autorizații prealabile”. Totodată, la subpct. 15.3 se indică asupra „autorizației de cercetare”, limitele și restricțiile căreia urmează a fi respectate. În acest sens, nu este clar dacă se are în vedere unul și același act sau autorizații distincte. Astfel, în vederea neadmiterii unor neclarități ulterioare de aplicare în practică a Regulamentului, se consideră necesară clarificarea aspectului dat.	Se acceptă. Proiectul a fost revizuit ținând cont de propunerea formulată.
			Potrivit **subpct. 16.6**, organizațiile responsabile pentru produsele sau serviciile TIC afectate de vulnerabilități au, printre altele, obligația de a evita inițierea de acțiuni împotriva raportorilor care acționează cu bună-credință, respectă cerințele legale și procedurale prevăzute de Regulament, cu excepția	Se acceptă. Proiectul a fost revizuit conform propunerii.

			situațiilor în care există motive obiective și documentate care indică o încălcare a legii ori provocarea unui prejudiciu. Cu referire la norma prenotată, nu este clar la care tip de acțiuni se referă autorul proiectului. În ipoteza în care se subînțelege instituția acțiunii civile, atunci norma nu poate fi acceptată în forma actuală, or, dreptul de a înainta o acțiune civilă nu poate fi îngrădit prin instituirea unei asemenea obligații în cadrul unei hotărâri de Guvern. Mai mult, aprecierea existenței sau inexistenței bunei-credințe a raportorului nu poate fi pusă pe seama organizației responsabile, acesta fiind un exercițiu complex asupra căruia urmează să se expună instanța de judecată în cadrul unui proces civil. Drept urmare, se necesită concretizarea tipurilor de acțiuni de la care urmează să se abțină organizația responsabilă în sensul subpct. 16.6.	
			La **pct. 17**, se consideră relevant de a indica cum și sub ce formă coordonatorul național urmează să agreeze o politică proprie a organizațiilor responsabile aferent procesului de divulgare a vulnerabilităților. Cu referire la cuprinsul secțiunii a 5-a din cadrul capitolului II, se menționează că, capitolele și secțiunile reprezintă elemente de structură complexe ale actului normativ. Prin urmare, acestea nu pot fi constituite dintr-un singur punct. Mai mult, obligația prevăzută la pct. 18 se regăsește deja în cadrul pct. 7 din Regulament și, drept urmare, este pasibilă excluderea elementului structural nominalizat.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			În conformitate cu **pct. 21** din proiect, „Persoanele fizice sau juridice care raportează cu bună credință o vulnerabilitate cibernetică, în condițiile prevăzute de prezentul regulament, beneficiază de protecție împotriva răspunderii juridice, civile sau penale, pentru acțiunile întreprinse în scopul identificării vulnerabilității, cu condiția respectării principiilor de proporționalitate, legalitate și responsabilitate.” În raport cu norma indicată mai sus, aceasta nu poate fi acceptată în redacția propusă. Or, regimul juridic al răspunderii	Se acceptă. Proiectul a fost revizuit conform propunerii.

			civile sau penale este stabilit în exclusivitate prin normele Codului civil și, respectiv, Codului penal. Totodată, se notează că, în ipoteza excluderii normei din proiect, nu se creează automat riscul atragerii la răspundere civilă sau penală a persoanelor care, acționând cu bună-credință și în limitele legii, întreprind anumite acțiuni în scopul identificării unei vulnerabilități într-un produs sau serviciu TIC. În speță, acțiunile persoanei sunt lipsite de caracterul culpabil și intenționat, element obligatoriu pentru constatarea existenței atât a unei fapte ilicite în sensul Codului civil, cât și pentru o infracțiune care reprezintă o faptă (acţiune sau inacţiune) prejudiciabilă, prevăzută de legea penală, săvârșită cu vinovăție și pasibilă de pedeapsă penală.	
			La **pct. 25**, cuvântul „maximum” se va exclude ca fiind excedent, or, indicarea termenului în cauză prezumă nedepășirea celor 48 ore.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La **pct. 26**, se menționează că notificarea privind identificarea unei vulnerabilități într-un produs sau serviciu TIC poate fi transmisă și direct organizației responsabile. În acest sens, se consideră judicioasă stabilirea unei obligații de transmitere a notificării atât coordonatorului național, cât și organizației responsabile. Or, ultima, fiind direct vizată de vulnerabilitatea identificată de către raportor, urmează a fi informată primordial și în termeni proximi în vederea întreprinderii unor măsuri urgente preventive de remediere/eliminare a deficienței ce poate fi exploatată de o amenințare cibernetică.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Potrivit **subpct. 31.3**, în cazul identificării unei situații excepționale, coordonatorul național, printre altele, poate autoriza măsuri temporare de protecție sau limitare a impactului înainte de finalizarea investigației. În acest sens, pentru o mai bună claritate și previzibilitate a normei, se consideră relevant de a indica tipul/categoria măsurilor temporare de care poate face uz coordonatorul național în contextul unei situații excepționale. Mai mult, aceasta intervenție va minimaliza riscul	Se acceptă. Proiectul a fost revizuit conform propunerii.

			unui eventual abuz prin autorizarea unor măsuri disproporționate.	
			La **pct. 44**, după textul „5 zile calendaristice” se recomandă a fi substituit cu textul „5 zile din momentul recepționării informației indicate la pct. 43”. Precizăm că, cuvântul „calendaristice” este inutil, deoarece reprezintă regula generală de calculare a termenului.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La **subpct. 44.5**, textul normei se va completa cu cuvintele „de remediere”.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La **pct. 46**, se apreciază drept oportun de a desfășura informația ce urmează a fi inclusă în raportul de progres săptămânal (ex. starea actuală, măsuri întreprinse, blocaje întâmpinate, evoluția riscului etc.).	Precizare. Prevederile de la pct. 46 au excluse din proiect.
			La **pct. 47**, după cuvintele „comunică periodic” se va completa cu cuvintele „coordonatorului național”.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La **subpct. 49.3**, nu este clar la care „măsuri preventive suplimentare” se face referire. În ipoteza în care se are în vedere măsuri de securitate pentru produsul sau serviciul TIC, acestea se vor concretiza în cuprinsul normei.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Pct. 50, după cuvintele „pe baza raportului final” se va completa cu textul „și întrunirii condițiilor cumulative de la pct. 61”.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Cu referire la **pct. 52**, având în vedere obiectul de reglementare specific al normei, se consideră justificată excluderea acesteia din cadrul secțiunii a 3-a și, respectiv, includerea în cadrul secțiunii a 5-a din același capitol.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La **pct. 61:** În cuprinsul dispoziției de la subpct. 61.1, în vederea respectării trimiterii corecte, textul „pct. 51” se va substitui cu textul „pct. 49”. Complementar, se consideră judicioasă completarea punctului cu o normă nouă privind necesitatea informării și a organizației responsabile despre decizia de închidere a cazului.	Se acceptă. Proiectul a fost revizuit conform propunerii.

			La **pct. 64**, în vederea utilizării unei terminologii uniforme în tot cuprinsul proiectului, cuvântul „entitatea” se va substitui cu cuvântul „organizația”.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La **pct. 65**, în scopul neadmiterii dispunerii unor perioade diferențiate de păstrare a datelor și a documentației aferente cazurilor închise, se recomandă indicarea expresă și concretă de păstrare a acestora, prin evitarea utilizării expresiilor „pe o perioadă de minimum/maximum […] ani”.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Cu referire la cuprinsul capitolului IV – „Dispoziții finale”, se consemnează că acesta nu corespunde rigorilor stabilite în *Legea nr. 100/2017 cu privire la actele normative*. Astfel, potrivit art. 47 alin. (1) din *Legea nr. 100/2017*, dispoziţiile finale cuprind momentul intrării în vigoare şi măsurile necesare punerii în aplicare a actului normativ. Totodată, potrivit alin. (2) din cadrul aceluiași articol, în dispoziţiile finale se includ reglementările privind obligaţia autorităţilor responsabile de a executa actul normativ, de a întreprinde măsurile şi de a realiza procedurile necesare executării.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Pct. 66 poartă un caracter declarativ, motiv pentru care se va exclude.	Se acceptă. Proiectul a fost revizuit conform propunerii.
16.	**Serviciul de Informații și Securitate** *(Nr. IE/10051 din 24.09.2025)*		În ansamblu, proiectul de Regulament stabilește bazele unei abordări structurale și metodologice pentru gestionarea vulnerabilităților cibernetice, dar există unele lacune și ambiguități care pot conduce la întârzierea în procesul de remediere și divulgare, la apariția unor riscuri pentru securitatea utilizatorilor și la încărcarea administrativă excesivă. Definirea clară a termenelor, procedurilor și responsabilităților ar putea asigura o mai mare eficiență și transparență în aplicarea mecanismului de gestionare a vulnerabilităților cibernetice.	Precizare. La propunerea MJ prevederile de la pct. 21 au fost excluse din proiect.

			1. Una dintre cele mai frecvente preocupări ale organizațiilor și cercetătorilor de securitate cibernetică este legată de protecția identității raportorilor de vulnerabilități. Astfel, punctul 21 al proiectului de Regulament prevede protecția identității persoanelor fizice sau juridice care raportează o potențială vulnerabilitate cibernetică, iar în anumite cazuri, există riscul ca organizațiile responsabile sau autoritățile să nu acorde suficientă importanță acestui aspect.	
			Subsidiar, la subpunctul 23.7 a proiectului de Regulament, este menționată despre opțiunea ca raportorul să-și exprime preferințele cu privire la confidențialitatea identității și implicarea ulterioară, însă, în textul proiectului nu este prevăzut și reiterat la fel de explicit modul de a fi implementate pe aspecte entități, și modalitatea de a asigura confidențialitatea completă în practică. Prin urmare, s-ar putea crea anumite temeri din partea raportorilor de a nu fi expuși unor repercusiuni juridice sau financiare, în special, în contextul vulnerabilităților majore care pot afecta infrastructuri critice.	Se acceptă. Proiectul a fost completat conform propunerii.
			2. Conform punctului 43 a proiectului de Regulament, procesul de remediere al vulnerabilităților este reglementat într-un mod detaliat, însă din conținutul proiectului nu sunt suficiente de clare mecanismele de control al progresului. Or, termenul de 5 zile pentru transmiterea unui plan preliminar de acțiuni este relativ scurt și nu ține cont de complexitatea reală a problemelor tehnice ce pot apărea. De asemenea, nu sunt menționate sancțiuni clare sau măsuri de constrângere care să motiveze organizațiile responsabile să respecte termenele, în situațiile în care există întârzieri sau dificultăți în implementarea remediilor prevăzute la punctul 45.	Se acceptă parțial Stabilirea sancțiunilor depășește obiectul prezentului Regulament, care reglementează exclusiv procedura de divulgare coordonată a vulnerabilităților. Aspectele privind răspunderea și sancțiunile vor fi tratate separat, în cadrul actelor normative ce vor stabili regimul răspunderii juridice pentru încălcarea legislației în domeniul securității cibernetice.
			3. Subsidiar, la punctul 21 a proiectului de Regulament se menționează despre buna-credință a raportorilor și protecția	Precizare.

			acestora în fața răspunderii juridice, însă în conținutul proiectului nu sunt prevăzute sancțiuni clare pentru raportările false sau nejustificate, care ar putea încărca sistemul și compromite securitatea. În plus, nu există o delimitare clară a responsabilității legale a coordonatorului național sau a autorităților implicate în cazurile de divulgare publică sau de neimplementare a măsurilor de remediere.	La propunerea MJ prevederile de la pct. 21 au fost excluse din proiect.
			Totodată, la punctul 56 a proiectului de Regulament se menționează că divulgarea publică va include evaluarea riscurilor reziduale, însă nu există o explicație clară a semnificației acestora, iar procesul de evaluare nu oferă suficiente detalii pentru a ajunge la o concluzie obiectivă asupra riscurilor rămase. În acest sens, această prevedere poate crea dificultăți la luarea unor decizii contradictorii sau subiective, în funcție de perspectiva diferitelor părți implicate.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			4. La punctul 66 a proiectului de Regulament se menționează că neconformitatea cu prevederile Regulamentului poate atrage răspunderea civilă sau penală, iar, în conținutul proiectului nu sunt prevăzute sancțiuni clare sau mecanisme de executare pentru organizațiile care nu respectă termenii și condițiile de remediere sau divulgare. Astfel, proiectul de Regulament riscă să devină mai mult un cadru procedural, fără instrumente clare de aplicare.	Precizare. La propunerea MJ prevederile de la pct. 66 au fost excluse din proiect. Stabilirea sancțiunilor depășește obiectul prezentului Regulament, care reglementează exclusiv procedura de divulgare coordonată a vulnerabilităților. Aspectele privind răspunderea și sancțiunile vor fi tratate separat, în cadrul actelor normative ce vor stabili regimul răspunderii juridice pentru încălcarea legislației în domeniul securității cibernetice.
17.	**Serviciul Tehnologia Informației și Securitate Cibernetică** *(Nr. 1.4/1491/25 din 18.09.2025)*		La sbp. 61.1. din proiectul Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice, numărul *„51”* se va substitui cu numărul *„49”*.	Se acceptă. Proiectul a fost revizuit conform propunerii.

			La pct. 66 prevederea privind atragerea la răspundere contravențională, civilă sau penal, ținând cont de cadrul normativ în vigoare, are un caracter pur declarativ, prin urmare se propune a se revedea necesitatea menținerii acesteia în proiect.	Se acceptă. Proiectul a fost revizuit conform propunerii.
18.	**Agenția de Guvernare Electronică** *(Nr. 3007-183 din 16.09.2025)*		Deși prevederile pct.14 acoperă cumulativ interdicția de exploatare (14.2, 14.5 și 14.6), acestea sunt formulate ca obligații de abținere și sunt separate. Absența unei declarații directe și concise ar putea crea ambiguitate. O clauză explicită, singulară, care definește clar linia dintre cercetarea de securitate și exploatarea ilegală, ar oferi o mai mare certitudine juridică atât pentru cercetători (care știu exact care sunt limitele), cât și pentru organele de drept (care au un criteriu clar de evaluare a intenției). În acest sens, propunem **completarea Capitolului II, Secțiunea 2, cu subpct. distinct „14.9”**, cu următorul cuprins: „*14.9. să nu exploateze vulnerabilitatea în orice formă care depășește strictul necesar pentru confirmarea existenței și documentarea impactului potențial al acesteia. Acțiunile care duc la modificarea, ștergerea sau extragerea neautorizată a datelor (exfiltrare) (excepție poate fi o mostră minimă de date, absolut necesară ca dovadă tehnică), întreruperea sau degradarea serviciilor, sau obținerea de acces neautorizat la alte sisteme sau date, sunt strict interzise și atrag încetarea aplicării protecției legale oferite de prezentul regulament.”*	Se acceptă. Proiectul a fost completat conform propunerii.
			În vederea edificării unei relații de încredere și pentru a încuraja participarea activă, este important ca efortul comunității de securitate să fie recunoscut. Acest lucru nu implică neapărat recompense financiare. Recunoașterea publică a raportorilor, cu consimțământul lor, prin listarea într-o secțiune de mulțumiri pe pagina web instituțională, poate fi un stimulent puternic și nu implică costuri semnificative pentru Guvern. Controlul A.8.8 din ISO/IEC 27002 menționează expres posibilitatea programelor de „bug bounty”. Astfel, propunem **completarea Capitolului II, Secțiunea 2, după pct. 14, cu un pct. nou - „15”**, cu următorul cuprins:	Se acceptă. Proiectul a fost completat conform propunerii.

			„*15. Coordonatorul național poate institui și menține mecanisme de recunoaștere publică a raportorilor care au contribuit semnificativ la îmbunătățirea securității cibernetice, cu consimțământul prealabil al acestora. De asemenea, Coordonatorul încurajează organizațiile responsabile să implementeze propriile programe de recunoaștere sau de recompensare pentru raportarea vulnerabilităților.”*	
			La **pct. 20**, textul „în formă scrisă,” se propune a fi exclus pe motiv că „completarea formularului electronic” exclude notificarea scrisă, or dacă intenția autorului a fost reglementarea ambelor proceduri, atât „scrisă” cât și „electronică”, proiectul urmează a fi completat corespunzător	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La **subpct. 30.1.** textul „publice” urmează a fi exclus pe motiv că termenul utilizat se contrapune cu prevederile Legii nr. 234/2021 cu privire la serviciile publice, unde „*servicii publice reprezintă activități administrative necomerciale cu caracter individual, realizate în regim de putere publică de prestatorul de servicii publice, cu sau fără solicitarea beneficiarilor de servicii, și care vizează realizarea drepturilor, libertăților, obligațiilor și intereselor legitime ale acestora, asigurându-le, după caz, beneficiile materiale sau nemateriale corespunzătoare*” or sensul normei descris la acest subpct. este reglementarea „serviciilor în unul sau mai multe sectoare și/sau subsectoare critice”, care este reglementat la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Proiectul de regulament nu abordează scenariul, din ce în ce mai frecvent, în care o vulnerabilitate nu se află în produsul final al organizației responsabile, ci într-o componentă software terță (ex: o bibliotecă open-source) pe care aceasta o utilizează. Atacurile asupra lanțului de aprovizionare software sunt o amenințare majoră. Adesea, organizația responsabilă (dezvoltatorul produsului final) nu poate remedia direct vulnerabilitatea, ci depinde de un alt furnizor (proiectul open-source, altă companie). Ghidul ENISA pentru NIS2 și standardul ISO/IEC 27002 (în special controalele A.5.19-	Se acceptă. Proiectul a fost completat conform propunerii.

			A.5.22) pun un accent deosebit pe securitatea în relația cu furnizorii. În acest sens, propunem **completarea Capitolului III, Secțiunea 1, după pct. 32 cu un pct. nou „33”,** cu următorul cuprins: „*33. În cazul în care vulnerabilitatea notificată este identificată într-un produs sau serviciu TIC furnizat de o parte terță, organizația responsabilă are obligația de a notifica de urgență furnizorul componentei respective și de a coopera cu acesta pentru obținerea unui remediu. Organizația responsabilă va informa periodic Coordonatorul național despre stadiul comunicării cu furnizorul terț. Coordonatorul național poate, la rândul său, să faciliteze contactul cu furnizorul terț sau cu alți coordonatori naționali, dacă este cazul.”*	
			Normele proiectului de Regulament nu definesc un proces clar pentru situația în care o vulnerabilitate este descoperită într-un produs TIC sau serviciu TIC pe care producătorul nu îl mai suportă (End of Life - EoL) sau a declarat că nu îl va mai actualiza. Utilizatorii continuă adesea să folosească produse EoL, fiind expuși unui risc major, deoarece producătorul nu mai oferă actualizări de securitate. În acest sens, considerăm necesar reglementarea clară a acestor procese pentru a proteja interesul public, chiar și atunci când remedierea directă (patching) nu mai este o opțiune, prin completarea Capitolului II, Secțiunea 4, după pct. 57 cu un pct. nou „58”, cu următorul cuprins: *„58. Dacă o vulnerabilitate este confirmată într-un produs sau serviciu TIC declarat oficial de organizația responsabilă ca fiind la sfârșitul ciclului de viață (End of Life - EoL), iar organizația refuză să ofere un remediu, Coordonatorul național, după o evaluare de risc, poate decide o divulgare publică accelerată. Divulgarea va include, pe lângă informațiile standard, o avertizare clară pentru utilizatori privind statutul EoL al produsului și va oferi, în măsura posibilităților, recomandări de atenuare a riscului (măsuri compensatorii) sau de migrare către produse alternative suportate.”*	Se acceptă. Proiectul a fost completat conform propunerii.
19.	**Agenția Servicii Publice**		Lipsa de obiecții și propuneri.	S-a luat act.

	(Nr. 01/11586 din 17.09.2025)			
20.	**Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației** *(Nr. 01-DRA/1711 din 23.09.2025)*		La pct. 44 din proiectul hotărârii de Guvern, textul *"5 zile calendaristice"* se substituie cu textul *"5 zile lucătoare",* modificarea propusă este bazată pe măsurile complexe necesare pentru remediere a incidentelor/vulnerabilităților identificate;	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La pct. 66 din proiectul hotărârii de Guvern, textul *"refuzul de a coopera"* este reflectat ca o neconformitate stabilită la modul general și nu cade sub incidența neconformității grave, în acest sens, solicităm autorului proiectului de a desfășura descrierea tuturor neconformităților stabilite, corelarea acestora cu gradul de risc prestabilit, precum și stabilirea sancțiunilor aplicate pentru admiterea încălcărilor vizate.	Precizare. La propunerea MJ prevederile de la pct. 66 au fost excluse.
21.	**Banca Națională a Moldovei** *(Nr. 31-002/131/4910 din 26.09.2025)*		Referitor la subpct. 4.2 din proiectul Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice *(în continuare - Regulament*), prin care se definește termenul „coordonator național", observăm, că potrivit art. 12 alin. (1) din Directiva NIS 2 (Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022), coordonatorul național acționează ca intermediar de încredere la cererea oricărei părți. Respectiv, pentru a se determina în mod clar că mecanismul de intermediere de către coordonatorul național nu este unul obligatoriu, ci intervine doar la solicitarea fie a persoanei care raportează vulnerabilitatea, fie a producătorului sau furnizorului de produse/servicii TIC, recomandăm completarea după cuvintele „organizațiile responsabile" cu cuvintele „<u>la cererea oricărei părți</u>", după cum este prevăzut și la subpct. 9.1 din Regulament. În acest sens, propunem a se examina necesitatea revizuirii pct. 28 din Regulament, din cuprinsul căruia ar rezulta implicarea obligatorie a coordonatorului național, atunci când consideră necesar, chiar și în lipsa unei cereri a raportorului sau a organizației responsabile.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La subpct. 4.4 din Regulament, observăm o necorelare terminologică între noțiunea **„divulgare publică"**, formulată ca	Se acceptă.

			„*comunicarea <u>înainte de remediere</u> a informațiilor despre vulnerabilitate către publicul larg*”, și procedura expusă în secțiunea 4 din capitolul III al Regulamentului, care stabilește expres în pct. 53 din Regulament, că *divulgarea publică a unei vulnerabilități se realizează <u>doar după finalizarea procesului de remediere</u> sau atunci când există un risc major pentru securitatea publică și organizația responsabilă nu a remediat vulnerabilitatea în termenul stabilit*. Totodată, expresia „către o audiență extinsă” este ambiguă și nu corespunde cerințelor de previzibilitate și claritate a normei juridice, fiind problematică aprecierea numărului sau a calității persoanelor care ar putea fi considerate „audiență extinsă”. În acest sens, pentru a elimina neconcordanța juridică menționată *supra*, propunem reformularea subpunctului 4.4, după cum urmează: „*divulgare publică – comunicarea către public a informațiilor referitoare la o vulnerabilitate, în condițiile și termenele prevăzute de prezentul Regulament*”, cu menținerea regulii de la pct. 53 ca normă procedurală de principiu. Această clarificare unifică terminologia și previne interpretările divergente privind momentul publicării.	Proiectul a fost revizuit conform propunerii.
			Recomandăm a se revedea subpct. 6.2 din Regulament, or, responsabilitatea partajată, în limita competențelor fiecărui subiect implicat în proces, nu pare a fi o responsabilitate comună a tuturor subiecților respectivi, întrucât, fiecare din ei răspunde în limita obligațiilor sale. Totodată, recomandăm a se reevalua în ce măsură raportorii sunt responsabili pentru raportarea și remedierea vulnerabilităților, având în vedere că raportarea este voluntară (conform subpct. 4.8 din Regulament), iar remedierea vulnerabilităților ar fi în competența organizațiilor responsabile.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			La pct. 7 din Regulament se utilizează sintagma *”toate entitățile vizate”*, iar pct. 8 din Regulament se referă la *”toate părțile implicate”*. În acest sens, recomandăm a se examina necesitatea uniformizării terminologiei utilizate, în măsura în care sintagmele menționate au același sens.	Se acceptă. Proiectul a fost revizuit conform propunerii.

			În acord cu subpct. 5.2., Regulamentul se aplică explicit și „*componentelor infrastructurii critice naționale din domeniul digital*”, inclusiv sistemelor și rețelelor esențiale, ceea ce include și infrastructurile de plăți. În acest context, principiul confidențialității consacrat la pct. 8 din Regulament și excepția din subpct. 8.1. a Regulamentului sunt adecvate, iar rolul coordonatorului de a evalua și prioritiza vulnerabilitățile în funcție de „*impactul asupra infrastructurii critice sau serviciilor esențiale*” și de a negocia termene pentru remediere și divulgare sunt bine-venite. Totuși, pentru a evita efecte adverse asupra încrederii publice și pentru a preveni exploatarea ulterioară a unor breșe sensibile, propunem ca, în ceea ce privește vulnerabilitățile care afectează infrastructura critică de plăți și entitățile supravegheate de Banca Națională a Moldovei, **decizia privind divulgarea publică să fie precedată de consultarea obligatorie a Băncii Naționale a Moldovei,** și după caz a operatorilor de infrastructură relevantă. Adițional, sugerăm ca, până la confirmarea implementării remediilor la toți participanții afectați, comunicarea publică să fie gradată și, pe cât posibil, anonimizată, ținând cont de prevederile pct. 57 din Regulament care permite păstrarea confidențialității detaliilor de exploatare și publicarea unor rapoarte anonimizate. Această calibrare a transparenței, la care Banca Națională a Moldovei subscrie, reduce riscul sistemic fără a compromite obiectivul de securitate prin divulgare responsabilă.	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Având în vedere obligația coordonatorului național de a „*colabora cu autoritățile publice relevante*”, precum și regimul de alertă rapidă către „*autoritățile competente*” în două ore în situații excepționale și obligația de notificare a autorităților competente când remedierea întârzie, propunem ca Regulamentul să precizeze explicit că, **pentru sectorul financiar și infrastructura de plăți, Banca Națională a Moldovei este autoritatea sectorială competentă care trebuie informată** și consultată în toate etapele sensibile: evaluare de risc, stabilirea termenelor de remediere, decizia de divulgare	Se acceptă. Proiectul a fost revizuit conform propunerii.

			publică și recomandările temporare către utilizatori. O asemenea precizare în text ar crește previzibilitatea pentru entități și ar facilita o reacție coordonată în cazurile cu impact sistemic.	
			Recomandăm a se evalua opțiunea completării pct. 10 din Regulament cu activități privind implementarea *„Financial reward programme/bug bounty programme”.*	Se acceptă. Proiectul a fost completat conform propunerii.
			Referitor la subpct. 14.5 din Regulament, ținem să remarcăm că, obligația de a obține „*acordul expres și documentat al proprietarului sau administratorului sistemului TIC*” înaintea „*oricăror teste care presupun accesarea, modificarea sau interferența cu funcționarea sistemului*”, coroborată cu cerința ca activitățile să se desfășoare doar „în limitele autorizării acordate” (subpct. 15.2) și cu interdicția pentru cercetătorii înregistrați de a testa „fără autorizație prealabilă”, poate descuraja identificarea timpurie a vulnerabilităților în sisteme expuse public, inclusiv din sectorul financiar. În această ordine de idei, fără a diminua protecția infrastructurilor, propunem definirea termenului *„interferență”* ca ingerință semnificativă (de natură să afecteze disponibilitatea, integritatea sau cercetătorilor înregistrați activități limitate, neintruzive, de constatare cu bună-credință a vulnerabilităților, urmate imediat de notificare.	Precizare. Prevederile de la pct 14.5 a fost revizuit la propunerea MJ.
			Remarcăm, că pct. 18 din Regulament nu expune corespunzător principiile enunțate în pct. 6 din Regulament. Astfel, recomandăm corelarea pct. 18 cu prevederile pct. 6, ținând cont de redacția principiilor enunțate la subpunctele 6.1-6.5, fie includerea în pct. 18 a unei referințe generice la pct. 6 (*”18. Toate părțile implicate în procesul de divulgare coordonată au obligația de a respecta principiile enunțate în pct. 6.”*).	Se acceptă. Prevederile de la pct. 18 au fost excluse din proiect și pct. 7 a fost completat cu trimiteri la art. 5 din Legea nr. 48/2023 privind securitatea cibernetică.
			La pct. 19 din Regulament, propunem punerea la dispoziția raportorilor a mai multor canale de comunicare, inclusiv email.	Nu se acceptă. Utilizarea unei platforme digitale dedicate asigură un nivel superior de securitate, trasabilitate și confidențialitate a informațiilor

				transmise, comparativ cu canalele nesecurizate, precum e-mailul. Aceasta permite gestionarea centralizată, verificarea automată și arhivarea controlată a notificărilor, protejând integritatea procesului și datele sensibile. În același timp, platforma este practică și facilă pentru raportor, oferind o experiență intuitivă, confirmări automate de primire și posibilitatea de a urmări în timp real statutul raportării.
			La pct. 21, opinăm că, în măsura în care răspunderea civilă sau penală, fie altă formă de răspundere juridică, este instituită prin lege, exceptarea anumitor categorii de persoane de la răspunderea juridică respectivă urmează a fi reglementată tot prin lege, or, excepțiile stabilite într-un act normativ subordonat legii nu pot fi opuse unei prevederi legale imperative.	Precizare. La propunerea MJ prevederile de la pct. 21 au fost excluse.
			Punctele 14.3 și 23 din Regulament reglementează elementele esențiale pe care trebuie să le conțină o notificare privind o vulnerabilitate. În această ordine de idei, pentru a evita dublarea prevederii sau o eventuală confuzie în delimitarea acestor două reglementări, se recomandă corelarea punctelor menționate supra pentru precizie și claritate, eventual, cu păstrarea reglementării din pct. 23, având în vedere denumirea capitolului și a secțiunii *(Capitolul III Etapele procesului de divulgare coordonată, Secțiunea 1 Notificarea inițială și recepționarea acesteia).*	Se acceptă. Proiectul a fost revizuit conform propunerii.
			În textul Regulamentului (inclusiv în punctele 24-26) este utilizată sintagma „*ore lucrătoare”.* În acest sens, în vederea excluderii ambiguităților privind modul de calcul a termenelor respective (termenul se va determina în funcție de numărul de ore lucrătoare în cursul unei zile, care poate varia în funcție de regimul de muncă în cadrul entității și regimul de muncă al	Se acceptă. Proiectul a fost revizuit conform propunerii.

			salariatului), recomandăm definirea termenelor în ore sau în zile/zile lucrătoare.	
			La pct. 25 din Regulament se indică următoarele: *”În cazul notificărilor incomplete, coordonatorul național solicită completarea informațiilor lipsă în termen de maximum 48 de ore lucrătoare”.* În acest context, recomandăm a se evalua modul de aplicare de către coordonatorul național a acestei prevederi în situația în care notificare este transmisă anonim, așa cum rezultă din pct. 23.7, care menționează: *”datele de contact ale raportorului* **(dacă nu optează pentru anonimat)** *și preferințele privind confidențialitatea identității și implicarea ulterioară”.*	Se acceptă. Proiectul a fost revizuit conform propunerii.
			Propunem completarea pct. 55 din Regulament cu cerința **consultării autorității sectoriale competente înainte de publicarea informațiilor cu privire la vulnerabilitatea identificată în sectoarele esențiale.** De asemenea, propunem completarea pct. 57 din Regulament cu rezerve suplimentare aferent publicării informațiilor care au tangență cu infrastructurile financiare: evitarea oricăror elemente care ar permite identificarea rapidă a vectorilor tranzacționali specifici sau a entităților critice, până la confirmarea remediilor la nivelul tuturor participanților afectați, iar acolo unde este necesar, utilizarea mecanismului de raport public anonimizat. Ajustările propuse vor păstra echilibrul între interesul public de informare și protecția stabilității financiare.	Se acceptă. Proiectul a fost revizuit ținând cont de propuneri.
			În contextul pct. 67 din Regulament, recomandăm ca normele metodologice și ghidurile pe care coordonatorul național este împuternicit să le aprobe, să includă un capitol distinct pentru sectorul financiar și infrastructurile de plăți, cu scenarii de lucru privind calendarul de remediere, criteriile de escaladare și formatele de comunicare confidențială către autoritatea sectorială și participanți, inclusiv în regim accelerat atunci când sunt întrunite condițiile de situație excepțională. Această detaliere va sprijini coordonarea inter-instituțională și va crește predictibilitatea pentru entitățile reglementate.	Precizare. La propunerea MJ prevederile de la pct. 67 au fost transferate la pct.10.7. Totodată, menționăm că obiectul de reglementare al regulamentului nu este conținutul normelor metodologice sau ghidurilor care vor fi aprobate de ASC. Respectiv, considerăm oportun ca propunerile privind conținutul

				normelor metodologice și ghidurilor să fie înaintate ASC în cadrul procedurii de elaborare a acestora.
22.	**Centrul Național pentru Protecția Datelor cu Caracter Personal** *(Nr. 04-01/972 din 18.09.2025)*		Lipsa de obiecții și propuneri.	S-a luat act.
			Cu titlu informativ, comunicăm că a fost instituită obligația operatorului de date cu caracter personal de a efectua evaluarea impactului asupra protecției datelor cu caracter personal, în cazul în care prelucrarea datelor poate genera un risc sporit pentru drepturile și libertățile persoanelor *(art. 23 din Legea nr. 133/2011 privind protecția datelor cu caracter personal).* Astfel, ținând cont de prevederile art. 23 alin. (6) din Legea 133/2011, în cazul în care, tipurile de prelucrare a datelor cu caracter personal, reglementate prin actul normativ prenotat sunt susceptibile să genereze un risc sporit pentru drepturile și libertățile persoanelor, reieșind cel puțin din faptul prelucrării la scară largă a datelor cu caracter personal, este necesară efectuarea evaluării impactului asupra prelucrării datelor cu caracter personal, în contextul adoptării respectivului act normativ.	S-a luat act.
23.	**Autoritatea Aeronautică Civilă** *(Nr. 2347 din 15.09.2025)*		Lipsa de obiecții și propuneri.	S-a luat act.
24.	**Asociația Națională a Companiilor din sectorul TIC** *(Nr. 742 din 26.09.2025)*		Reieșind din pct. 16.3 al Regulamentului, nu este clar care este totuși termenul de confirmare a recepționării notificării vulnerabilităților, or utilizarea sintagmei „într-un termen rezonabil” este interpretabilă și poate fi interpretată în detrimentul organizației responsabile pentru produsele sau serviciile TIC. Această argumentare se referă și la formularea pct. 16.5. – *e necesară clarificarea sintagmei de „termen rezonabil”, precum și completarea punctului respectiv cu posibilitatea prelungirii termenului în cazul în care organizația invocă motive întemeiate.* Deoarece în momentul depistării vulnerabilității este complicat de a determina componentele acesteia, propunem ca notificarea să poată fi depusă pe etape, de exemplu: 24 de ore lucrătoare de la depistarea vulnerabilității și 2 săptămâni pentru notificarea finală,	Se acceptă parțial. Proiectul a fost revizuit. Pentru un spor de precize normativă s-a stabilit că Organizațiile responsabile pentru produsele sau serviciile TIC confirmă recepționarea notificării într-un termen de 1 zi lucrătoare și implementează măsuri pentru remedierea vulnerabilităților într-un termen proporțional cu riscul identificat, stabilit pe baza evaluării riscului și detaliat în planul de

			ținând cont de circumstanțele fiecărui caz în parte. Astfel se propune următoare sintagmă pentru pct. 16.5: *să implementeze măsuri pentru remedierea vulnerabilităților într-un termen rezonabil, proporțional riscului identificat și nivelului vulnerabilității;*	remediere transmis coordonatorului national.
			La fel, este generală și formularea pct. 16.4 ce prevede obligația de informare periodică a coordonatorului național cu privire la progresul remediilor și la eventualele obstacole întâmpinate. – *nu este clar o dată la ce perioadă trebuie să fie realizată această informare periodică*. Propunem să fie stabilit că informarea periodică trebuie să fie efectuată în dependență de circumstanțe, însă cel puțin o dată în trimestru.	Se acceptă parțial. Raportarea trimestrială nu corespunde necesităților de prezentare promtă a informației privind remedierea vulnerabilităților către coordonatorul național.
			Pct. 16.10. indică organizațiilor obligația să evalueze dacă vulnerabilitatea notificată poate afecta și alți furnizori, clienți sau parteneri, și, după caz, să informeze coordonatorul național pentru o abordare coordonată; - *se propune modificarea acestui punct în așa fel încât în cazul notificării furnizorilor, clienților sau partenerilor de către Coordonatorul național, numele sau denumirea persoanei afectate va fi făcut public doar cu acordul organizației responsabile de produsele sau serviciile TIC.*	Nu se acceptă. Introducerea unei condiționări privind acordul organizației responsabile ar limita capacitatea Coordonatorului național de a acționa prompt și eficient în situații care pot afecta securitatea altor entități sau sectoare. Divulgarea informațiilor relevante către părțile potențial afectate se realizează strict în scopul prevenirii extinderii riscurilor și nu presupune automat publicarea datelor în spațiul public.
			Se propune ca pct. 16.11 „să asigure disponibilitatea resurselor necesare pentru procesul de remediere a vulnerabilităților în funcție de nivelul de risc identificat.”- *să fie completat cu formularea „cu respectarea principiului proporționalității.”*	Precizare. Punctul a fost exclus
			Reieșind din prevederile pct. 27, organizația responsabilă de produsele sau serviciile TIC trebuie în termen de 24 ore lucrătoare să transmită în adresa coordonatorului național: copia integrală a notificării primite; confirmarea că raportorul a fost informat despre transferul notificării către coordonatorul național; o evaluare preliminară a validității vulnerabilității raportate; un plan inițial de analiză și remediere, inclusiv persoanele de contact desemnate.	Se acceptă parțial. Termenii au fost revizuiți reieșind din divizarea proceselor operaționale.

			Considerăm că pct. 27 pune pe umerii organizației responsabile o sarcină excesivă de a transmite coordonatorului național atâtea informații într-un termen atât de scurt, mai ales în cazul vulnerabilităților complexe, care necesită o analiză minuțioasă. Se propune ca inițial în termen de 24 ore lucrătoare, organizația responsabilă să redirecționeze coordonatorului național doar notificarea recepționată și confirmarea informării raportorului despre transmiterea notificării conform competenței. Ulterior în termen de 5 zile lucrătoare, organizația să transmită în adresa coordonatorului național o evaluare preliminară a vulnerabilității raportate și persoanele de contact desemnate, iar apoi în termen maxim de 14 zile lucrătoare, organizația să transmită coordonatorului național o evaluare mai detaliată a validității vulnerabilității și un plan de analiză, acțiuni și remediere.	
			Se propune completarea pct. 28 cu formularea: *„Coordonatorul național va informa organizația responsabilă cu privire la etapele examinării notificărilor de raportare.”* *La fel, se propune completarea proiectului cu criterii obiective pentru exercitarea dreptului de preluare:* • *Lipsa de răspuns a organizației responsabile în termenul stabilit* • *Refuzul nejustificat de cooperare documentat prin cel puțin două solicitări oficiale* • *Evaluarea că vulnerabilitatea prezintă risc iminent pentru securitatea națională* • *Solicitarea expresă a organizației responsabile pentru asistență*	Se acceptă parțial. Proiectul a fost revizuit și stabilește că Coordonatorul național poate interveni și prelua integral coordonarea procesului, indiferent de destinatarul inițial al notificării, dacă vulnerabilitatea raportată implică un risc iminent și critic pentru securitatea națională, infrastructura critică ori siguranța publică.
			La elaborarea acestui Regulament urmează a se ține cont de faptul că, furnizorii de servicii de comunicații electronice deja au obligația de raportare către ANRCETI în ceea ce privește incidentele de securitate cibernetică și asigurarea continuității serviciilor. Este foarte importantă armonizarea prevederilor Regulamentului în cauză cu reglementările ANRCETI, pentru a evita careva confuzii sau suprapuneri.	Precizare. Proiectul nu stabilește obligațiile de raportare a incidentelor cibernetice, dar stabilește cadrul juridic material și procedural pentru notificarea, evaluarea, remedierea și divulgarea coordonată a vulnerabilităților

				produselor și serviciilor tehnologiei informației și comunicațiilor.
			Deși punctul 38 menționează utilizarea sistemului CVSS pentru clasificarea vulnerabilităților, nu sunt specificate versiunea utilizată, criteriile suplimentare pentru contextul local, sau procedura de contestare a clasificării. *Se propune completarea proiectului cu detalierea sistemului de clasificare:* *Utilizarea CVSS v4.0 ca standard de bază* *Criterii suplimentare pentru contextul național: impactul asupra infrastructurii critice, numărul de utilizatori afectați, disponibilitatea soluțiilor de remediere* *Procedura de contestare a clasificării cu termen de 5 zile și evaluare de către o comisie tehnică mixtă (reprezentanți ai coordonatorului și industriei).*	Nu se acceptă. Regulamentul stabilește cadrul general al procesului de divulgare coordonată, fără a detalia aspecte metodologice tehnice precum versiunea CVSS sau criteriile specifice de aplicare. Aceste elemente vor fi stabilite de coordonatorul național în funcție de evoluțiile standardelor internaționale.
			Pct. 41 prevede dreptul coordonatorului național de a facilita un proces de mediere tehnică, dar nu este o detaliere a acestui proces, ce ar presupune, cum poate avea loc, în ce termen și la ce etapă din momentul depunerii notificării.	Se acceptă. Proiectul a fost completat cu prevederi noi ținând cont de propunerea formulată.
			La pct. 44 în coroborare cu prevederile pct. 27 din proiectul Regulamentului se propune ca *inițial în termen de 24 ore lucrătoare, organizația responsabilă să redirecționeze coordonatorului național doar notificarea recepționată și confirmarea informării raportorului despre transmiterea notificării conform competenței. Ulterior, organizația să transmită în adresa coordonatorului național o evaluare preliminară a vulnerabilității raportate și persoanele de contact desemnate, organizația să transmită coordonatorului național o evaluare mai detaliată a validității vulnerabilității și un plan de analiză, remediere și acțiuni.* Aici menționăm că, în cazul vulnerabilităților complexe, în general poate fi necesar un termen mai îndelungat pentru a analiza toate circumstanțele și a întocmi un plan de acțiuni ținând cont și de posibilitățile tehnice și financiare a organizației responsabile.	Se acceptă parțial. Termenii au fost revizuiți reieșind din divizarea proceselor operaționale.
			La pct. 47 nu este clar ce termen se prezumă sub sintagma de *„comunică periodic”.* Propunem să fie completat cu sintagma ”*în*	Se acceptă parțial.

			dependență de evoluția circumstanțelor, însă cel puțin o dată în trimestru."	Menționăm că raportarea trimestrială nu corespunde necesităților de prezentare promtă a informației privind remedierea vulnerabilităților către coordonatorul național.
			Pct. 51 indică că: „În cazul în care organizația responsabilă nu remediază vulnerabilitatea într-un termen rezonabil și fără justificare obiectivă, coordonatorul național notifică autoritățile competente și decide, în condiții reglementate, divulgarea publică a vulnerabilității. În asemenea cazuri, coordonatorul national este în drept să recomande public și utilizatorilor măsuri temporare de protecție sau atenuare. *Credem că este necesar să fie discriminat faptul de divulgare publică a vulnerabilității de divulgare publică a numelui/denumirii furnizorului afectat de vulnerabilitate. Astfel, considerăm corectă oferirea dreptului coordonatorului național de a decide unilateral privitor la divulgarea publică vulnerabilității, însă divulgarea numelui și denumirii doar în coordonare cu furnizorul afectat, or acest fapt ar putea afecta foarte mult activitatea și reputația organizației responsabile. La fel, considerăm oportună implementarea unui proceduri de consultare prealabilă obligatorie a poziției furnizorului înainte de a lua decizia de divulgare publică a vulnerabilității.* *Totodată se propune crearea unei proceduri structurate pentru divulgarea publică:* 1. *Notificare prealabilă de minimum 30 zile către organizația responsabilă* 2. *Prezentarea unui dosar de justificare cu dovezi concrete ale riscului pentru securitatea publică* 3. *Acordarea unui termen suplimentar de remediere* 4. *Limitarea divulgării la informațiile strict necesare pentru protecția publicului*	Se acceptă parțial. Proiectul a fost revizuit și completat cu prevederi suplimentare pentru a asigura un proces coordonat și echilibrat de divulgare a vulnerabilităților de către Coordonatorul național.
			Pct. 55 indică: „În absența unui consens între părți, coordonatorul național adoptă decizia finală privind divulgarea, pe baza unei evaluări de risc documentate și transparente, notificând toate părțile implicate cu cel puțin 48 de ore lucrătoare înainte de publicare, dacă nu există o urgență justificată. "- *notificarea cu 48*	Se acceptă parțial. Proiectul prevede că Coordonatorul național notifică în scris organizația responsabilă, raportorul vulnerabilității și alte părți direct

			de ore înainte de publicare ar putea fi un termen insuficient, respectiv se propune ca acest termen să fie adaptat în funcție de gravitatea și impactul vulnerabilității.	afectate cu privire la decizia de divulgare publică cu cel puțin 3 zile lucrătoare înainte de publicare.
			Referitor la prevederile pct. 56 care reglementează informațiile ce vor fi incluse în divulgarea publică, menționăm că informațiile furnizate publicului urmează a fi limitate la o descriere generală făr a indica expres furnizorul, serviciul sau sistemul afectat.	Se acceptă parțial. Proiectul a fost revizuit ținând cont de propunerea formulată. Expunerea unei informații generale după finalizarea procesului de remediere este suficientă deoarece vulnerabilitatea a fost deja corectată. În schimb, atunci când vulnerabilitatea nu a fost remediată și există un risc major pentru securitatea publică, este necesară furnizarea unor informații suplimentare, precum produsele afectate, impactul potențial și recomandări pentru utilizatori, pentru a permite gestionarea corespunzătoare a riscului și reducerea efectelor negative. Astfel, gradul de detaliu al divulgării este proporțional cu nivelul de risc și cu necesitatea protejării utilizatorilor și infrastructurilor.
			Regulamentul nu oferă garanții clare pentru protejarea informațiilor comerciale sensibile și a proprietății intelectuale a furnizorilor în procesul de divulgare. Punctul 57 specifică că "nu se vor publica date sensibile" fără a defini suficient de clar acest concept. *Se propune completarea proiectului* cu un nou capitol dedicat protecției proprietății intelectuale inclusiv protecția informației ce constituie secret comercial în sensul legislației privind protecția secretelor comerciale:	Nu se acceptă. Regulamentul urmărește să reglementeze procedura de divulgare coordonată a vulnerabilităților și nu să stabilească detaliile privind protecția proprietății intelectuale sau informațiilor comerciale, care fac obiectul legislației existente privind secretul comercial și confidențialitatea datelor. Aspectele menționate, cum ar fi clasificarea

			Definirea clară a "datelor comerciale sensibile" incluzând: algoritmi proprietari, arhitectura sistemelor, detalii de implementare, informații despre furnizori și parteneri Obligația semnării acordurilor de confidențialitate de către toți participanții la proces Limitarea accesului la informații la personalul cu clearance de securitate apropiat Procedura de clasificare a informațiilor înainte de orice divulgare.	informațiilor sau semnarea acordurilor de confidențialitate, pot fi stabilite de Coordonatorul național, fără a fi incluse direct în textul Regulamentului. În plus, Regulamentul prevede deja interdicția divulgării datelor sensibile, ceea ce oferă un cadru suficient de protecție în procesul de divulgare.
			Cât privește pct. 65 care stabilește că: „Datele și documentația aferente cazurilor închise sunt păstrate în registrul național de evidență a vulnerabilităților gestionate, pe o perioadă de minimum 5 ani, în scopul asigurării trasabilității, auditabilității și evaluării periodice a eficienței procesului de divulgare coordonată. ”- *considerăm oportun a reține că organizațiile responsabile vor suporta costuri pentru păstrarea datelor pe o perioadă de 5 ani. Se propune substituirea cu tremenul de 3 ani.*	Se acceptă. Totodată, menționăm că datele și documentația aferente cazurilor închise vor fi păstrate în Registrul de stat al incidentelor cibernetice, posesor al căruia va fi Agenția pentru Securitate Cibernetică.
			Prevederile pct. 66 indică posibilitatea atragerii la răspundere contravențională, civilă sau penală a organizațiilor, însă nu prevede careva etape de avertizare, careva pași de remediere pe care coordonatorul național trebuie să le impună organizației, înainte de a aplica sancțiunile prevăzute.	Precizare. La propunerea MJ prevederile de la pct. 66 au fost excluse.
25.	**Centrul de Armonizare a Legislației** *(Nr. 31/02-69-9844 din 22.09.2025)*		Lipsa de obiecții și propuneri.	**-**

Expertizare

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător** *(Nr. 38-78-9979 din 25.09.2025)*	***La proiectul hotărârii:***		
		1.	Conform celor prevăzute la pct.4.1 și pct.15 din Regulament, desfășurarea activității (prestarea serviciilor) de cercetător sau participant în domeniul securității este condiționată de „înregistrare" oficială, „autorizare prealabilă" (de către coordonatorul procesului de divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice) și obținerea periodică a certificării de competență profesională (conform „standardele stabilite de coordonatorul național"). Aceste obligații/condiționalități au caracter primar, nu pot fi instituite de Guvern fără a fi prevăzute la nivel de lege, deși Legea nr.48/2023 nu prevede nici aceste acte/condiționalități și nici nu reglementează cumva activitatea de „cercetător sau participant în domeniul securității". Toate aceste acte sau proceduri cu caracter permisiv, în lipsa unor reglementări mai amănunțite, înțelegem că se califică ca și acte permisive. Amintim că cel puțin autorizarea și înregistrarea în calitate de acte permisive, pentru a fi impuse și solicitate de autoritatea din domeniu, trebuie să fie incluse în Nomenclatorul actelor permisive (Legea nr.160/2011), cu argumentarea preliminară corespunzătoare. Odată cu includerea în Nomenclator, este imperativ ca în primul rând la nivel de lege să fie instituie normele primare procedurale și materiale care ar reglementa regimul juridic al autorizației și înregistrării și ar prevedea cerințele și procedura de bază pentru solicitarea și obținerea acestora. Cu toate că nici în proiectul prezentat nu se prevede nici un detaliu procedural în privința acestor acte sau proceduri permisive. Aceleași obiecții se referă și la certificare, dacă aceasta ține și de persoana juridică, nu doar de persoana fizică. Cel puțin obligația primară de a obține și actualiza periodic certificarea necesită să fie prevăzută în lege ca să poată fi preluată și dezvoltată la nivel de hotărâre de Guvern.	Se acceptă. Proiectul a fost revizuit ținând cont de obiecția formulată și de prevederile Legii nr.48/2023.

		2.	La pct. 16.5, 16.9, 16.11 la fel se conțin norme/obligații cu caracter primar, adică care trebuie să derive în mod expres din lege, ca să poată fi dezvoltate de Guvern, dar și care nu respectă principiile transparenței și previzibilității reglementării activității de întreprinzător. Modul de formulare a acestor norme creează dificultăți în stabilirea clară a obligațiilor care pot fi imputate operatorului economic și modul în care aceste obligații necesită a fi implementate. Inclusiv cerințele din aceste norme sunt formulate vag și incert, nu este clar cum sau în ce formă se realizează în practică și nu se indică cumva care ar fi gradul satisfăcător de realizare, corespunzător nu este prevăzut cum se poate stabili că în realitate cerințele sunt respectate sau performanța solicitată a fost atinsă. Astfel nu este clar ce presupune - implementarea măsurilor „în termen rezonabil”, ce categorii de „mecanisme interne pentru recepționarea și gestionarea notificărilor” trebuie instituie de agent economic și care este volumul de „resurse necesare” pentru eliminarea vulnerabilităților pe care trebuie să-l asigure agentul economic.	Se acceptă. Proiectul a fost revizuit ținând cont de obiecțiile formulate.
		La proiectul Notei de fundamentare:		
		3.	Nota de fundamentare conține suficiente informații pentru a stabili de principiu necesitatea și oportunitatea intervenției din perspectivă juridică, însă nu reflectă raționamentul și impactul noilor prevederi, astfel nota corespunde parțial cu cerințele metodologice prevăzute de Legea nr.100/2017 cu privire la actele normative.	Se acceptă. Nota de fundamentare a fost completată cu informații suplimentare.

SINTEZA

obiecțiilor și propunerilor/recomandărilor la proiectul de hotărâre de Guvern

„Cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice”

(număr unic 714/MDED/2025)

EXPERTIZARE

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Ministerul Apărării** nr. 11/1444 din 04.12.2025		Ministerul Apărării a examinat proiectul de hotărâre cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (număr unic 714/MDED/2025), autor – Ministerul Dezvoltării Economice și Digitalizării, și în limita competenței funcționale, comunicăm despre lipsa obiecțiilor și propunerilor.	S-a luat act
2.	**Ministerul Sănătății** nr. 27/3853 din 05.12.2025		Prin prezenta, Ministerul Sănătății a examinat repetat proiectul de hotărâre cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (număr unic 714/MDED/2025), autor – Ministerul Dezvoltării Economice și Digitalizării, și în limita competențelor funcționale, comunică lipsa obiecțiilor sau propunerilor.	S-a luat act
3.	**Ministerul Culturii**		Ministerul Culturii comunică lipsă de obiecții și propuneri.	S-a luat act
4.	**Ministerul Educației și Cercetării**		Ministerul Educației și Cercetării comunică lipsa de propuneri și obiecții.	S-a luat act
5.	**Serviciul Tehnologia Informației și Securitate Cibernetică**		Serviciul Tehnologia Informației și Securitate Cibernetică comunică lipsa de propuneri și obiecții.	S-a luat act
6.	**Ministerul Mediului**		Ministerul Mediului Vă comunică lipsa obiecțiilor și propunerilor.	S-a luat act
7.	**Ministerul Energiei**		Ministerul Energiei comunică lipsa propunerilor suplimentare la acest proiect de hotărâre.	S-a luat act
8.	**Ministerul Justiției** nr. 04/1-12121 din 09.12.2025		Urmare examinării proiectului hotărârii Guvernului cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (număr unic 714/MDED/2025), comunicăm că observațiile formulate de către	S-a luat act

			Ministerul Justiției în raportul de expertiză juridică nr. 04/1-9262 din 22.09.2025 au fost luate în considerare, proiectul fiind revizuit prin prisma acestora. Obiecții suplimentare nu avem de formulat.	
9.	**Aparatul Președintelui RM** nr. 2/2-06-1781 din 10.12.2025	1.	Aparatul Președintelui Republicii Moldova a examinat repetat proiectul Hotărârii Guvernului cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (număr unic 714/MDED/2025), însoțit de nota de fundamentare și sinteza obiecțiilor/propunerilor ajustate după etapa de avizare și, având în vedere competența sa funcțională, comunică următoarele. Deși proiectul referit urmează să parcurgă etapa expertizării juridice și o îmbunătățire de rigoare, considerăm oportun să atenționăm următoarele inadvertențe care urmează a fi ajustate. I.Referitor la proiectul Regulamentului 1. La pct. 28, se va corecta trimiterea către pct. 27.	**Se acceptă**
		2.	La pct. 31, se propune substituirea textului „rețele sau sisteme informatice aflate în proprietatea statului” cu textul „rețele sau sisteme informatice proprietate a statului la nivel guvernamental” pentru a asigura conformitatea cu subpct. 161) din Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, care stabilește atribuția CERT Gov de a asigura securitatea rețelelor și a sistemelor informatice proprietate a statului la nivel guvernamental.	**Se acceptă**
		3.	Referitor la nota de fundamentare La compartimentul 2.2. „Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative”, urmează a fi ajustată referința la Programului de activitate al Guvernului, indicând Programul de activitate al Guvernului „UE, pace, dezvoltare”, potrivit Hotărârii Parlamentului nr. 269 din 31	**Se acceptă**

			octombrie 2025. Totodată, urmează să se ajusteze și să se facă trimitere la punctul nr. 7 din cadrul Priorității sectoriale „Guvernare eficientă” a Programului de activitate al Guvernului „UE, pace, dezvoltare”, care stabilește consolidarea securității cibernetice și a infrastructurii IT critice.	
		4.	Idem, textul „cercetătorii în domeniul securității” se va completa cu cuvântul „cibernetice” pentru a asigura uniformitatea cu textul proiectului Regulamentului.	**Se acceptă**
10.	**Ministerul Muncii și Protecției Sociale**		Lipsa de obiecții și propuneri.	S-a luat act
11.	**Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației** nr. 03-DJAC/3079 din 11.12.2025		Prin prezenta, Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI) urmare a examinării proiectului de hotărâre cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (număr unic 714/MDED/2025), în limitele competențelor funcționale, comunică lipsa de obiecții și propuneri. (ANRCETI) urmare a examinării proiectului de hotărâre cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (număr unic 714/MDED/2025), în limitele competențelor funcționale, comunică lipsa de obiecții și propuneri.	S-a luat act
12.	**Ministerul Infrastructurii și Dezvoltării Regionale**		MIDR comunică despre lipsa de propuneri suplimentare	S-a luat act
13.	**Ministerul Finanțelor**		Propunerile Ministerului Finanțelor au fost luate în considerație.	S-a luat act
14.	**Centrul Naţional Anticorupţie** nr. 06/2/22539 din 15.12.2025		Prin prezenta, Vă remitem atașat raportul de expertiză anticorupție la proiectul hotărârii de Guvern cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (număr unic 714/MDED/2025). Raportul de expertiză anticorupție: la proiectul de hotărâre a Guvernului cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice (număr unic 714/MDED/2025)	
	Raport de expertiză anticorupţie nr. EHG25/11037 din 15.12.2025			

			Prezentul raport de expertiză anticorupţie a fost întocmit de Centrul Național Anticorupție al Republicii Moldova în baza Legii nr.100/2017 cu privire la actele normative, a Legii nr.1104/2002 cu privire la Centrul Național Anticorupție, a Legii integrității nr.82/2017 și a Metodologiei de efectuare a expertizei anticorupţie a proiectelor de acte legislative și normative, aprobată prin Hotărârea Colegiului Centrului nr.6 din 20 octombrie 2017. I. Analiza riscurilor de corupere a procesului de promovare a proiectului I.1. Pertinența autorului, categoriei propuse a actului și a procedurii de promovare a proiectului Autor al proiectului de act normativ este Guvernul, iar autor nemijlocit este Ministerul Dezvoltării Economice și Digitalizării, ceea ce corespunde art.102 din Constituție, art.14 din Legea nr.100/2017 cu privire la actele normative. Categoria actului normativ propus este Hotărâre a Guvernului, ceea ce corespunde art.102 din Constituție, art.6 şi art.14 din Legea nr.100/2017 cu privire la actele normative.	S-a luat act
			I.2. Respectarea rigorilor de transparenţă în procesul decizional la promovarea proiectului Potrivit art.8 al Legii nr.239/2008 privind transparenţa în procesul decizional „etapele asigurării transparenţei procesului de elaborare a deciziilor sunt: a) informarea publicului referitor la iniţierea elaborării deciziei; b) punerea la dispoziţia părţilor interesate a proiectului de decizie şi a materialelor aferente acestuia; c) consultarea cetăţenilor, asociaţiilor constituite în corespundere cu legea, altor părţi interesate; d) examinarea recomandărilor cetăţenilor, asociaţiilor constituite în corespundere cu legea, altor părţi interesate în procesul de elaborare a proiectelor de decizii; e) informarea publicului referitor la deciziile adoptate". Totodată, art.10 din Legea nr.239/2008 stabileşte expres că:	S-a luat act

			(1) Autoritatea publică asigură accesul la proiectele de decizii şi la materialele aferente acestora prin publicarea obligatorie a lor pe pagina web oficială a autorităţii publice, prin asigurarea accesului la sediul autorităţii, precum şi prin expediere prin poştă sau prin alte mijloace disponibile, la solicitarea persoanei interesate. (2) Proiectul de decizie şi materialele aferente acestuia se plasează pe pagina web oficială a autorităţii publice responsabile cel puţin pentru perioada recepţionării şi examinării recomandărilor". Se constată că anunțul privind organizarea consultării publice, proiectul şi nota de fundamentare la acesta au fost plasate pe pagina web a Ministerului Dezvoltării Economice și Digitalizării www.mded.gov.md la compartimentul Transparență decizională/Anunțuri privind consultări publice, precum și pe portalul www.particip.gov.md. În aceste condiții, se consideră că autorul a respectat prevederile legale privind transparența în procesul decizional.	
			I.3. Scopul anunţat și scopul real al proiectului În nota de fundamentare se menționează: „Proiectul hotărârii de Guvern are drept scop stabilirea cadrului normativ pentru implementarea unui mecanism standardizat de identificare, raportare și remediere a vulnerabilităților, contribuind la consolidarea securității cibernetice naționale și la alinierea cu standardele europene din domeniu. Intervenția este necesară pentru punerea în aplicare a prevederilor art. 7 alin. (4) pct. 10) din Legea nr. 48/2023 și transpunerea obligațiilor prevăzute în Directiva (UE) 2022/2555 (Directiva NIS 2), precum și asigurarea unui cadru coerent care să sprijine și reglementeze procesul de divulgare coordonată a vulnerabilităților în domeniul securității cibernetice”. În acest context, în notă se face referire că: „Temeiul legal al elaborării proiectului de act normativ constituie art. 7 alin. (4) pct. 10) din Legea nr.	s-a luat act

			48/2023 privind securitatea cibernetică. Norma în cauză abilitează Agenția pentru Securitate Cibernetică (ASC), în calitate de autoritate competentă la nivel național în domeniul securității cibernetice, cu atribuțiile de coordonator al procesului de divulgare coordonată a vulnerabilităților, conform cadrului normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. Totodată, aprobarea proiectului derivă din angajamentele asumate prin Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029 (Capitolul 10 – Societatea informațională și mass-media, acțiunea nr. 36) și Planul național de reglementări pentru anul 2025 (acțiunea nr. 13)".	
			I.4. Interesul public şi interesele private promovate prin proiect Proiectul promovează interesul public manifestat prin aprobarea cadrului procedural pentru procesul de divulgare coordonată a vulnerabilităților în domeniul securității cibernetice.	s-a luat act
			I.5. Justificarea soluțiilor proiectului I.5.1. Suficienţa argumentării din nota informativă. În conformitate cu art.30 al Legii nr.100/2017 cu privire la actele normative, proiectele de acte normative sunt însoțite de „nota de fundamentare care cuprinde: a) denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului; b) condițiile ce au impus elaborarea proiectului actului normativ; c) obiectivele urmărite și soluțiile propuse; d) analiza impactului de reglementare; e) compatibilitatea proiectului actului normativ cu legislația UE; f) avizarea și consultarea publică a proiectului actului normativ; h) modul de încorporare a actului în cadrul normativ existent; i) măsurile necesare pentru implementarea prevederilor proiectului actului normativ."	s-a luat act

			Nota de fundamentare stabilește condițiile ce au impus elaborarea proiectului, evidențiază obiectivele urmărite și soluțiile propuse prin promovarea proiectului.	
			I.5.2. Argumentarea economică-financiară. Conform art.30 lit.d) al Legii nr.100/2017 cu privire la actele normative, nota de fundamentare trebuie să conțină „d) analiza impactului de reglementare". În nota de fundamentare se menționează că: „Implementarea proiectului nu implică costuri suplimentare imediate (...)".	s-a luat act
			II. Analiza generală a factorilor de risc ale proiectului II.1. Limbajul proiectului Potrivit art.54 al Legii nr.100/2017 cu privire la actele normative „textul proiectului actului normativ se elaborează [...] cu respectarea următoarelor reguli: [...] a) se expune într-un limbaj simplu, clar şi concis [...] c) terminologia utilizată este constantă, uniformă și corespunde celei utilizate în alte acte normative, în legislația Uniunii Europene și în alte instrumente internaționale la care Republica Moldova este parte, cu respectarea prevederilor prezentei legi; [...] e) se interzice folosirea neologismelor dacă există sinonime de largă răspândire, [...] f) se evită folosirea [...] a cuvintelor și expresiilor [...] care nu sînt utilizate sau cu sens ambiguu; g) se evită tautologiile juridice; h) se utilizează, pe cât este posibil, noțiuni monosemantice, [...]". Textul proiectului este expus într-un limbaj simplu, clar şi concis, cu respectarea regulilor gramaticale şi de ortografie, întrunind cerinţele prevăzute de art.54 din Legea nr.100/2017.	s-a luat act
			II.2. Coerența legislativă a proiectului În textul proiectului nu au fost identificate norme contradictorii sau conflicte dintre prevederile acestuia cu reglementările altor acte normative în vigoare.	s-a luat act
			II.3. Activitatea agenţilor publici şi a entităților publice reglementată în proiect Prin proiect se reglementează activitatea entităților publice și a agenților publici responsabili de implementarea prevederilor proiectului. Normele din proiect nu	s-a laut act

			conțin reglementări confuze în ceea ce privește atribuțiile ce urmează să fie exercitate. II.4. Atingeri ale drepturilor omului care pot fi cauzate la aplicarea proiectului Prevederile proiectului nu aduc atingere drepturilor fundamentale ale omului consacrate de Constituţia Republicii Moldova, Declaraţia Universală a Drepturilor Omului şi Convenţia Europeană a Drepturilor Omului.	
			III. Concluzia expertizei În nota de fundamentare se menționează: „Proiectul hotărârii de Guvern are drept scop stabilirea cadrului normativ pentru implementarea unui mecanism standardizat de identificare, raportare și remediere a vulnerabilităților, contribuind la consolidarea securității cibernetice naționale și la alinierea cu standardele europene din domeniu. Intervenția este necesară pentru punerea în aplicare a prevederilor art. 7 alin. (4) pct. 10) din Legea nr. 48/2023 și transpunerea obligațiilor prevăzute în Directiva (UE) 2022/2555 (Directiva NIS 2), precum și asigurarea unui cadru coerent care să sprijine și reglementeze procesul de divulgare coordonată a vulnerabilităților în domeniul securității cibernetice”. În acest context, în notă se face referire că: „Temeiul legal al elaborării proiectului de act normativ constituie art. 7 alin. (4) pct. 10) din Legea nr. 48/2023 privind securitatea cibernetică. Norma în cauză abilitează Agenția pentru Securitate Cibernetică (ASC), în calitate de autoritate competentă la nivel național în domeniul securității cibernetice, cu atribuțiile de coordonator al procesului de divulgare coordonată a vulnerabilităților, conform cadrului normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. Totodată, aprobarea proiectului derivă din angajamentele asumate prin Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029 (Capitolul 10 – Societatea informațională și mass-media,	s-a luat act

			acțiunea nr. 36) și Planul național de reglementări pentru anul 2025 (acțiunea nr. 13)". Cu referire la Impactul financiar și argumentarea costurilor estimative, în nota de fundamentare autorul descrie informații detaliate. În final, menționăm că, **în redacția propusă, proiectul nu conține factori de risc care să genereze apariția riscurilor de corupție**.	

Secretar de Stat **Michelle ILIEV**