GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 2025

Chișinău

cu privire la 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), Guvernul HOTĂRĂȘTE,

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

Prim-ministru **DORIN RECEAN**

Contrasemnează:

Viceprim-ministru,

ministrul dezvoltării economice și digitalizării **DOINA NISTOR**

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 și procedural pentru notificarea, evaluarea, remedierea și divulgarea coordonată a vulnerabilităților produselor și serviciilor tehnologiei informației și comunicațiilor (TIC), în vederea îmbunătățirii securității cibernetice și protejării interesului public.

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 și a protejării interesului public.

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

4. În sensul prezentului Regulament, următoarele noțiuni semnifică:

4.1.*cercetător sau participant în domeniul securității* – persoană fizică sau juridică care deține experiența, competențele și/sau certificările 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, fiind înregistrată de către coordonatorul procesului de divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice;

4.2.*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, asigurând coordonarea, monitorizarea și facilitarea procesului de divulgare coordonată a vulnerabilităților;

4.3.*divulgare coordonată a vulnerabilităților* - cu sensul definit în Legea nr. 48/2023 privind securitatea cibernetică;

4.4.*divulgare publică* – comunicarea înainte de remediere a informațiilor despre vulnerabilitate către publicul larg sau către o audiență extinsă, inclusiv prin publicarea în baze de date publice, forumuri, platforme de social media sau mass-media;

4.5.furnizor de servicii - cu sensul definit în Legea nr. 48/2023 privind securitatea cibernetică;

4.6.*organizație responsabilă* – producător, furnizor, dezvoltator sau administrator al unui produs sau serviciu TIC afectat de vulnerabilitate;

4.7.*produs al tehnologiei informației și comunicațiilor (produs TIC)* - cu sensul definit în Legea nr. 48/2023 privind securitatea cibernetică;

4.8.*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;

4.9.*remediere* - procesul de eliminare sau atenuare a vulnerabilității prin implementarea de corecții, versiuni noi, actualizări de securitate sau alte măsuri tehnice și organizatorice;

4.10. *serviciu al tehnologiei informației și comunicațiilor (serviciu TIC)* - cu sensul definit în Legea nr. 48/2023 privind securitatea cibernetică;

4.11. *vulnerabilitate* - cu sensul definit în Legea nr. 48/2023 privind securitatea cibernetică;

5. Prezentul Regulament se aplică vulnerabilităților descoperite în:

5.1.produse și servicii TIC utilizate de 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.produse și servicii TIC dezvoltate, furnizate sau gestionate de furnizorii de servicii care își au sediul sau filiala în Republica Moldova;

5.4.servicii TIC furnizate prin intermediul infrastructurilor de tip cloud, indiferent de localizarea geografică a infrastructurii, dacă acestea sunt utilizate de entități din Republica Moldova sau în cadrul infrastructurii digitale naționale.

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

6.1.*buna-credință* – toate părțile implicate (raportori, organizații responsabile, coordonatorul național) acționează cu bună-credință, în scopul exclusiv al îmbunătățirii securității produselor și serviciilor TIC;

6.2.*responsabilitatea comună* – raportarea, analiza și remedierea vulnerabilităților reprezintă o responsabilitate partajată între raportori, organizațiile afectate și coordonatorul procesului, fiecare acționând în limitele competențelor proprii;

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 raportorului și detalii 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 entitățile vizate de prezentul Regulament, inclusiv organizațiile responsabile și furnizorii de produse sau servicii TIC, au obligația de a coopera în mod activ și de bună-credință cu coordonatorul național în procesul de notificare, analiză și remediere a vulnerabilităților, cu respectarea principiilor prevăzute la pct. 6.

8. Coordonatorul național, precum și toate părțile implicate în procesul de divulgare coordonată a vulnerabilităților, au obligația de a păstra confidențialitatea informațiilor obținute pe durata și ulterior finalizării procesului, 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 coordonatorul național;

8.2.divulgarea este autorizată 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 pentru 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 pentru 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 identității raportorilor și confidențialitatea informațiilor sensibile furnizate pe parcursul procesului;

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

9.5.asigură evidența raportorilor și cercetătorilor înregistrați în registrul național de evidență a vulnerabilităților gestionate, care poate fi accesat de organizațiile responsabile.

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

10.1. identifică și contactează entitățile relevante implicate în procesul de divulgare, inclusiv organizațiile responsabile pentru 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, potențialul de exploatare și impactul asupra infrastructurii critice sau 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, comunicărilor realizate și măsurilor luate de către organizațiile implicate;

10.7. elaborează, aprobă și actualizează proceduri și ghiduri metodologice;

10.8. elaborează anual un raport privind divulgarea coordonată a vulnerabilităților, care include statistici agregate și recomandări pentru îmbunătățirea procesului.

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

10.10.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 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.

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.

Secțiunea 2

Raportorii

14. Raportorii, în procesul de raportare a unei vulnerabilități, au obligația de a respecta următoarele cerințe:

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

14.2. să acționeze în limitele cadrului legal și cu respectarea principiului proporționalității, fără a compromite confidențialitatea datelor, integritatea produselor TIC sau disponibilitatea serviciilor TIC, doar în măsura strict necesară pentru a verifica existența vulnerabilității și pentru a asigura acuratețea raportării;

14.3. notificarea trebuie să includă identificarea clară și precisă a produsului sau serviciului TIC afectat de vulnerabilitate, o descriere detaliată a vulnerabilității potențiale, impactul estimativ, metodologia de identificare și, dacă este posibil, recomandări preliminare de remediere, fără întârziere nejustificată de la descoperirea unei vulnerabilități potențiale, către coordonatorul național și/sau organizația responsabilă;

14.4. 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 expirarea unui termen rezonabil stabilit de comun acord cu coordonatorul național;

14.5. să obțină acordul expres și documentat al proprietarului sau administratorului sistemului TIC înainte de efectuarea oricăror teste de identificare a vulnerabilităților care presupun accesarea, modificarea sau interferența cu funcționarea sistemului, și să se abțină de la utilizarea oricăror practici lipsite de etică, ilicite, nerezonabile sau imprudente, inclusiv acțiuni care ar putea perturba funcționarea produselor TIC, compromite disponibilitatea serviciilor TIC, afecta confidențialitatea sau integritatea datelor-;

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

14.7. 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;

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

Secțiunea 3

Cercetătorii și participanții în domeniul securității înregistrați de coordonatorul național

15. Suplimentar, cerințelor prevăzute la pct. 14, cercetătorii și participanții în domeniul securității înregistrați de coordonatorul național asigură respectarea următoarelor cerințe:

15.1. să mențină și să actualizeze periodic certificările profesionale relevante în domeniul securității cibernetice, conform standardelor stabilite de coordonatorul național;

15.2. să desfășoare activitățile de cercetare și testare în conformitate cu prevederile cadrului normativ și cu limitele autorizării acordate de coordonatorul național sau organizația responsabilă;

15.3. să respecte limitele și restricțiile specifice ale autorizației de cercetare, inclusiv domeniile de aplicare, tipurile de produse sau servicii TIC și metodele de testare permise;

15.4. 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;

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

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

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

15.8. 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 4

Organizațiile responsabile

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

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

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

16.3. să confirme recepționarea notificării într-un termen rezonabil și să inițieze, fără întârziere, măsurile necesare de analiză și remediere;

16.4. să informeze periodic coordonatorul național cu privire la progresul remediilor și la eventualele obstacole întâmpinate;

16.5. să implementeze măsuri pentru remedierea vulnerabilităților într-un termen rezonabil, proporțional cu riscul identificat;

16.6. să evite inițierea de acțiuni 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;

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

16.8. 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;

16.9. să instituie mecanisme interne pentru recepționarea și gestionarea notificărilor privind vulnerabilitățile, inclusiv proceduri standardizate și personal instruit în domeniu;

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

16.11.să asigure disponibilitatea resurselor necesare pentru procesul de remediere a vulnerabilităților în funcție de nivelul de risc identificat.

17. Organizațiile responsabile pot elabora o politică proprie de divulgare coordonată a vulnerabilităților, în corespundere cu prevederile prezentului Regulament și agreată de coordonatorul național.

Secțiunea 5

Dispoziții comune

18. Toate părțile implicate în procesul de divulgare coordonată au obligația de a respecta principiile transparenței, responsabilității și proporționalității în toate acțiunile întreprinse.

CAPITOLUL III

Etapele procesului de divulgare coordonată

Secțiunea 1

Notificarea inițială și recepționarea acesteia

19. 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 coordonatorul național.

20. Notificarea se face în formă scrisă, în limba română sau, după caz, în limba engleză ori limba rusă, prin completarea formularului electronic disponibil pe platforma oficială a coordonatorului național, în conformitate cu procedurile și instrucțiunile publicate.

21. 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.

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

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

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

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

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

23.4. metodologia utilizată pentru identificarea vulnerabilității, inclusiv instrumentele;

23.5. dovezi tehnice privind existența vulnerabilității, dacă sunt disponibile;

23.6. recomandări preliminare de remediere, în cazul în care pot fi formulate;

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

24. Coordonatorul național confirmă primirea notificării în termen de maximum 24 de ore lucrătoare de la recepționare și atribuie un identificator unic cazului pentru trasabilitate.

25. În cazul notificărilor incomplete, coordonatorul național solicită completarea informațiilor lipsă în termen de maximum 48 de ore lucrătoare.

26. Notificarea poate fi transmisă și direct organizației responsabile. În acest caz, aceasta are obligația să informeze coordonatorul național fără întârziere, dar nu mai târziu de 24 de ore lucrătoare de la primirea notificării.

27. Organizația responsabilă care primește o notificare directă trebuie să furnizeze coordonatorului național:

27.1. copia integrală a notificării primite;

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

27.3. o evaluare preliminară a validității vulnerabilității raportate;

27.4. un plan inițial de analiză și remediere, inclusiv persoanele de contact desemnate.

28. Coordonatorul național își rezervă dreptul de a prelua coordonarea integrală a procesului, chiar dacă notificarea a fost adresată inițial direct organizației responsabile.

29. În situații excepționale, când vulnerabilitatea raportată prezintă un risc iminent și critic pentru securitatea națională, infrastructura critică sau siguranța publică, coordonatorul național poate accepta notificări parțiale, solicitând completarea ulterioară a informațiilor esențiale.

30. Situația este calificată ca fiind excepțională dacă survine oricare din următoarele condiții:

30.1. afectează servicii publice esențiale (sănătate, apă, energie, telecomunicații, transport etc.);

30.2. exploatarea activă a vulnerabilității este efectuată de către actori malițioși;

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

30.4. există posibilitatea producerii unui prejudiciu fizic, financiar sau reputațional major asupra persoanelor fizice sau juridice;

30.5. există un impact asupra securității datelor cu caracter personal.

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

31.1. procesează notificarea în regim prioritar;

31.2. informează autoritățile competente în termen de maximum 2 ore de la confirmarea riscului;

31.3. poate autoriza măsuri temporare de protecție sau limitare a impactului înainte de finalizarea investigației;

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

32. 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.

33. 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 2

Evaluarea și clasificarea vulnerabilităților

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

35. Evaluarea are ca scop determinarea următoarelor elemente:

35.1. validitatea tehnică a vulnerabilității raportate;

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

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

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

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

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

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

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

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

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

37. 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.

38. Evaluarea și clasificarea se realizează de coordonatorul național în termen de maximum 5 zile lucrătoare de la primirea notificării complete, cu posibilitate de extindere a termenului în cazuri complexe, iar vulnerabilitățile sunt încadrate în una dintre următoarele categorii:

38.1. nivel critic - vulnerabilitate cu impact sever asupra infrastructurii critice sau care permite compromiterea completă a unui sistem, fără interacțiune din partea utilizatorului;

38.2. nivel ridicat - vulnerabilitate care compromite date sensibile, integritatea sistemului sau funcționalități esențiale;

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

38.4. nivel scăzut - vulnerabilitate cu impact redus, dificultate mare de exploatare și risc minim.

39. În funcție de clasificare, coordonatorul național stabilește:

39.1. termenul maxim recomandat pentru remedierea vulnerabilității;

39.2. necesitatea de intervenție urgentă sau escaladare instituțională;

39.3. necesitatea de notificare a altor autorități;

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

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

40.1. rezultatele analizei tehnice și argumentele aferente;

40.2. nivelul de risc atribuit vulnerabilității;

40.3. termenele recomandate pentru implementarea măsurilor corective;

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

41. În cazul în care apar divergențe între raportor și organizația responsabilă privind existența, gravitatea sau impactul vulnerabilității, coordonatorul național facilitează un proces de mediere tehnică, incluzând, dacă este necesar, organizarea unei analize comune.

42. 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 3

Remedierea vulnerabilității și monitorizarea progresului

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

44. Organizația responsabilă elaborează și transmite coordonatorului național, în termen de maximum 5 zile calendaristice, un plan preliminar de acțiuni, care include:

44.1. confirmarea vulnerabilității și nivelului de risc;

44.2. măsurile tehnice și organizatorice planificate pentru remediere;

44.3. termenele estimate pentru implementarea remediilor;

44.4. persoanele responsabile de implementare și comunicare;

44.5. eventualele constrângeri sau dependențe care pot afecta procesul.

45. 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.

46. În cazul vulnerabilităților critice sau cu risc ridicat, coordonatorul național poate solicita rapoarte de progres săptămânale sau poate organiza întâlniri tehnice periodice cu organizația responsabilă.

47. Pe toată durata procesului de remediere, organizația responsabilă comunică periodic stadiul implementării măsurilor și notifică fără întârziere orice modificare a planului inițial sau apariția unor obstacole semnificative.

48. 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.

49. După finalizarea implementării măsurilor, organizația responsabilă transmite coordonatorului național un raport de finalizare, care cuprinde:

49.1. acțiunile realizate și termenele respectate;

49.2. testele de validare a eficienței remediilor;

49.3. eventualele măsuri preventive suplimentare introduse;

49.4. concluziile formulate și modificările aduse proceselor interne.

50. Coordonatorul național validează închiderea cazului pe baza raportului final, consemnează decizia în registrul național de evidență a vulnerabilităților gestionate și informează raportorul, cu respectarea cerințelor de confidențialitate.

51. 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 național este în drept să recomande public și utilizatorilor măsuri temporare de protecție sau atenuare.

52. După închiderea cazului, coordonatorul național 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.

Secțiunea 4

Procedura de divulgare publică

53. Divulgarea publică a unei vulnerabilități se realizează doar după finalizarea procesului de remediere sau atunci când există un risc major pentru securitatea publică și organizația responsabilă nu a remediat vulnerabilitatea în termenul stabilit.

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

54.1. gradul de remediere atins și eficiența măsurilor implementate;

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

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

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

55. 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.

56. Divulgarea publică include următoarele informații:

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

56.2. produsele sau serviciile TIC afectate;

56.3. potențialul impact asupra utilizatorilor sau infrastructurilor;

56.4. recomandări tehnice destinate utilizatorilor pentru prevenire sau atenuare;

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

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

57. 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.

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

59. 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 5

Închiderea cazului

60. După finalizarea procesului de remediere și, după caz, a divulgării publice, coordonatorul național inițiază procedura de închidere a cazului.

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

61.1. transmiterea de către organizația responsabilă a raportului final de remediere, conform pct. 51;

61.2. validarea de către coordonatorul național a eficienței măsurilor de remediere;

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

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

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

62.1. data închiderii și identificatorul unic al cazului;

62.2. sinteza etapelor parcurse: notificare, evaluare, remediere, divulgare (după caz);

62.3. măsurile implementate și eficiența acestora;

62.4. concluzii și recomandări pentru îmbunătățirea procesului;

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

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

63.1. recomandări specifice către autoritățile competente privind îmbunătățirea cadrului normativ;

63.2. actualizarea procedurilor sau ghidurilor tehnice de raportare și remediere;

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

64. După închiderea unui caz, raportorul are dreptul să transmită, inclusiv în mod anonim, feedback privind procesul de interacțiune cu Coordonatorul național și/sau entitatea responsabilă, pentru a contribui la îmbunătățirea procesului de divulgare coordonată. Coordonatorul național colectează și analizează periodic aceste date în vederea îmbunătățirii practicilor și relațiilor de încredere.

65. 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.

CAPITOLUL IV

Dispoziții finale

66. Orice neconformitate gravă sau repetată cu prevederile prezentului Regulament, în special privind utilizarea abuzivă a informațiilor despre vulnerabilități, divulgarea neautorizată sau refuzul de a coopera cu Coordonatorul național, poate atrage răspunderea contravențională, civilă sau penală, după caz, în conformitate cu legislația în vigoare.

67. Coordonatorul național este în drept să elaboreze și să aprobe norme metodologice, ghiduri, formulare și recomandări pentru aplicarea unitară a prezentului Regulament, inclusiv modele pentru notificare, clasificare și documentare a vulnerabilităților.

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 „Moldova prosperă, sigură, europeană”, unul dintre obiectivele fundamentale este prevenirea și combaterea amenințărilor hibride pe palierul securității cibernetice și informaționale. În acest context, una dintre prioritățile în domeniul asigurării securității statului este fortificarea structurilor responsabile pentru lupta împotriva amenințărilor hibride și asigurarea securității cibernetice în vederea sporirii nivelului de siguranță pentru societate, instituțiile statului și pentru mediul privat. 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 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 conveniți, 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

[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).

orientări, metodologii și recomandări pentru implementarea politicilor CVD la nivel național și sectorial, promovând astfel coerența și armonizarea practicilor între statele membre.

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 legale, 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 și interzicerea represaliilor;
- proceduri detaliate pentru evaluarea, clasificarea, remedierea și divulgarea publică a vulnerabilităților;
- introducerea registrului național de evidență a cazurilor gestionate;
- stabilirea principiilor fundamentale ale procesului: bună-credință, proporționalitate, confidențialitate, trasabilitate și responsabilitate partajată.

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

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;
- îmbunătățirea colaborării interinstituționale în domeniul securității cibernetice.

4.2. Impactul financiar și argumentarea costurilor estimative

Aprobarea proiectului nu implică costuri suplimentare imediate.

Totuși, în vederea implementării prevederilor Regulamentului privind divulgarea coordonată a vulnerabilităților, Agenția pentru Securitate Cibernetică urmează să implementeze soluții digitale pentru gestionarea divulgării coordonate și menținerea registrului național de evidență a vulnerabilităților. Costurile pentru dezvoltarea și implementarea acestor soluții digitale vor fi evaluate în cadrul procesului de planificare bugetară și vor fi acoperite din resursele alocate Agenției pentru Securitate Cibernetică sau prin atragerea fondurilor externe de dezvoltare.

4.3. Impactul asupra sectorului privat

Implementarea Regulamentului privind divulgarea coordonată a vulnerabilităților va 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;
- 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 următorul impact pentru societate:

- îmbunătățirea securității digitale a cetățenilor prin protejarea mai eficientă a datelor personale și a sistemelor pe care aceștia le utilizează;
- creșterea încrederii publice în serviciile digitale guvernamentale și private prin implementarea unor standarde înalte de securitate;
- educația și conștientizarea populației în domeniul securității cibernetice prin campaniile de informare asociate implementării regulamentului.

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).

7. Concluziile expertizelor

Va fi completat urmare a recepționării avizelor.

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 dezvolta platforma digitală destinată primirii, procesării și gestionării notificărilor privind vulnerabilitățile identificate; • va asigura crearea Registrului național de evidență a cazurilor gestionate; • va elabora ghiduri metodologice pentru implementarea procedurilor de divulgare coordonată a vulnerabilităților; • va organiza sesiuni de formare și informare pentru raportori și organizații responsabile.

Secretar de stat **Michelle ILIEV**

Ministerul Dezvoltării
Economice și Digitalizării
al Republicii Moldova

Nr. 13/2-2478 din 21.08.2025

Cancelaria de Stat

În temeiul prevederilor pct. 38 și 185 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, se transmite *proiectul Hotărârii Guvernului cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice* pentru a fi inclus în lista proiectelor care urmează a fi examinate în cadrul ședinței secretarilor generali.

CERERE
privind înregistrarea de către Cancelaria de Stat
a proiectelor de acte ale Guvernului

Nr. crt.	**Criterii de înregistrare**	**Nota autorului**
1.	Categoria și denumirea proiectului	Proiectul Hotărârii Guvernului cu privire la aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice
2.	Autoritatea care a elaborat proiectul	Proiectul este elaborat de către Ministerul Dezvoltării Economiei și Digitalizării, cu suportul Agenției pentru Securitate Cibernetică.
3.	Justificarea depunerii cererii	Proiectul este elaborat în temeiul prevederilor art. 7 alin. (4) pct. 10) din Legea nr. 48/2023 privind securitatea cibernetică.
3[1].	Referința la documentul de planificare care prevede elaborarea proiectului *(PNA, PND, PNR, alte documente de planificare sectoriale)*	1) Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029 (Capitolul 10 – Societatea informațională și mass-media, acțiunea nr. 36); 2) Planul național de reglementări pentru anul 2025 (acțiunea nr. 13)
4.	Lista autorităților și instituțiilor a căror avizare este necesară	1. Cancelaria de Stat 2. Aparatul Președintelui Republicii Moldova 3. Ministerul Infrastructurii și Dezvoltării Regionale 4. Ministerul Energiei 5. Ministerul Finanțelor

		6. Ministerul Mediului 7. Ministerul Sănătății 8. Ministerul Agriculturii și Industriei Alimentare 9. Ministerul Apărării 10. Ministerul Afacerilor Interne 11. Ministerul Afacerilor Externe 12. Ministerul Educației și Cercetării 13. Ministerul Muncii și Protecției Sociale 14. Ministerul Culturii 15. Serviciul de Informații și Securitate 16. Serviciul Tehnologia Informației și Securitate Cibernetică 17. Agenția de Guvernare Electronică 18. Agenția Servicii Publice 19. Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației 20. Banca Națională a Moldovei 21. Centrul Național pentru Protecția Datelor cu Caracter Personal
5.	Termenul-limită pentru depunerea avizelor/expertizelor	Termen-limită de prezentare a avizelor – 10 zile lucrătoare. Termenul de avizare pentru Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător și pentru efectuarea expertizei de compatibilitate – 15 zile lucrătoare.
6.	Persoana responsabilă de promovarea proiectului	Sergiu Florea, șef al Secției politici în domeniul securității cibernetice tel.: 022 250 618, e-mail: sergiu.florea@mded.gov.md
7.	Anexe	1. Proiectul Hotărârii Guvernului 2. Nota de fundamentare
8.	Data și ora depunerii cererii	
9.	Semnătura	

Secretar de stat **Michelle ILIEV**

Ex. Sergiu Florea,
tel. 022 250 618