GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. _____

din_____

cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice

În temeiul art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153), Guvernul HOTĂRĂȘTE:

1. Se aprobă Regulamentul cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice (se anexează).

2. Ministerul Dezvoltării Economice și Digitalizării, în comun cu Agenția pentru Securitate Cibernetică, în termen de 12 luni de la data intrării în vigoare a prezentei hotărâri, va elabora și va prezenta Guvernului pentru aprobare Metodologia privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică.

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

Prim-ministru

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării

Aprobat prin
Hotărârea Guvernului nr._____
din_____

REGULAMENTUL
cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice

Capitolul I. Dispoziții generale

1. Regulamentul cu privire la supravegherea și controlul de stat asupra respectării de către furnizorii de servicii în sectoarele critice a cadrului normativ în domeniul securității cibernetice (în continuare – *Regulament*) stabilește cadrul juridic, organizatoric și procedural de exercitare de către Agenția pentru Securitate Cibernetică a funcției de supraveghere și control de stat al modului în care furnizorii de servicii în sectoarele critice asigură conformitatea cu prevederile cadrului normativ în domeniul securității cibernetice.

2. În sensul prezentului Regulament se utilizează noțiunile definite în Legea nr. 48/2023 privind securitatea cibernetică și Legea nr. 131/2012 privind controlul de stat.

3. Supravegherea și controlul de stat asupra respectării de către furnizorii de servicii în sectoarele critice a prevederilor cadrului normativ în domeniul securității cibernetice se realizează de către Agenția pentru Securitate Cibernetică (în continuare - *Agenția*) în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică, Legii nr. 131/2012 privind controlul de stat și a prezentului Regulament.

4. Agenția exercită controlul de stat asupra respectării de către furnizorii de servicii a cadrului normativ în domeniul securității cibernetice în baza rezultatelor evaluării riscurilor de securitate cibernetică la nivel național, sectorial/subsectorial, intersectorial sau pe tipuri de furnizori de servicii în conformitate cu cadrul metodologic aprobat în conformitate cu art. 16 alin. (2) din Legea nr. 131/2012 privind controlul de stat.

5. La solicitarea unei autorități de supraveghere și control a gestionarilor de infrastructură critică națională, Agenția efectuează un control inopinat al furnizorului de servicii în cauză și informează autoritatea de supraveghere și control

de stat în sectorul corespunzător despre încălcările constatate într-un termen care nu depășește 5 zile calendaristice de la data finalizării controlului.

6. Principiile specifice supravegherii și controlului de stat asupra respectării cadrului normativ în domeniul securității cibernetice sunt:

6.1. *proporționalitatea* – măsurile adoptate în procesul de realizare a funcției de supraveghere și control de stat de către Agenție trebuie să fie echilibrate în raport cu scopul general de evaluare a respectării prevederilor cadrului normativ în domeniul securității cibernetice și cu obiectivele specifice ale activității de supraveghere și control, evitând astfel sarcini administrative excesive și nejustificate pentru furnizorii de servicii și asigurând adaptarea resurselor și a intensității activității de supraveghere și control de stat la riscurile, importanța și dimensiunea furnizorilor de servicii;

6.2. *eficacitatea* – măsurile de supraveghere și de asigurare a respectării legislației trebuie să fie capabile să producă efectul urmărit, asigurând conformarea continuă a furnizorilor de servicii;

6.3. *efectul de descurajare* – măsurile adoptate trebuie să reducă probabilitatea încălcării prevederilor cadrului normativ, prin certitudinea și proporționalitatea aplicării acestora;

6.4. *cooperarea* – Agenția promovează colaborarea permanentă cu alte autorități și instituții publice, cu furnizorii de servicii în sectoarele critice, în scopul prevenirii și reducerii riscurilor de securitate cibernetică;

6.5. *protecția drepturilor fundamentale* – în exercitarea atribuțiilor, Agenția pentru Securitate Cibernetică asigură respectarea dreptului la viață privată, a protecției datelor cu caracter personal și a altor date ce constituie secret comercial pentru furnizorii de servicii în sectoarele critice, precum și a altor drepturi fundamentale stabilite de cadrul normativ.

Capitolul II. Supravegherea respectării cadrului normativ în domeniul securității cibernetice de către furnizorilor de servicii în sectoarele critice

7. Agenția realizează activitățile de supraveghere la furnizorii de servicii în sectoarele critice, în mod sistematic și continuu, cu scopul de a monitoriza respectarea obligațiilor prevăzute de Legea 48/2023 privind securitatea cibernetică și actelor normative de punere în aplicare a acesteia precum și de a monitoriza remedierea eventualelor deficiențe constatate, contribuind astfel la asigurarea oportună a unui nivel comun ridicat de securitate cibernetică la nivel național.

8. Activitatea de supraveghere se realizează de către personalul Agenției. În exercitarea competenței sale,de supraveghere, Agenția aplică măsuri care nu au caracter coercitiv și nu constituie forme ale controlului de stat, în scopul monitorizării și evaluării continue a modului în care prevederile cadrului normativ în domeniul securității cibernetice este aplicat de către furnizorii de servicii în sectoarele critice.

9. În cazul în care pe parcursul desfășurării activității de supraveghere se constată săvârșirea unor fapte care întrunesc elemente constitutive ale unor contravenții sau infracțiuni, Agenția implică la necesitate, autoritățile competente.

10. În exercitarea funcției de supraveghere, Agenția aplică următoarele măsuri de supraveghere:

10.1. monitorizarea continuă a spațiului cibernetic național pentru identificarea amenințărilor, riscurilor și vulnerabilităților de securitate cibernetică și *s*chimbul continuu de informații cu furnizorii de servicii prin emiterea de avertizări timpurii, alerte, anunțuri privind amenințările cibernetice, vulnerabilitățile și incidentele cibernetice în spațiul cibernetic național;

10.2. acordarea asistenței consultative furnizorilor de servicii în asigurarea conformității cu prevederile cadrului normativ în domeniul securității cibernetice, inclusiv prin furnizarea de orientări metodologice, inclusiv ghiduri, modele de proceduri și politici;

10.3. solicitarea informațiilor necesare pentru determinarea gradului de conformitate cu cadrul normativ și a nivelului de maturitate și reziliență a furnizorilor de servicii;

10.4. acordarea suportului consultativ furnizorilor de servicii în crearea mecanismelor de autoevaluare a conformității cu cerințele de securitate a rețelelor și sistemelor informatice stabilite de cadrul normativ;

10.5. evaluarea nivelului de conformitate a furnizorilor de servicii, inclusiv în baza rapoartelor de evaluare a riscurilor, a planurilor de tratare a riscurilor și a rapoartelor de evaluare a conformității, realizate de furnizorii de servicii în baza prevederilor normative;

10.6. înaintarea recomandărilor corespunzătoare furnizorilor de servicii, în baza rapoartelor de evaluare a riscurilor, a planurilor de tratare a riscurilor și a rapoartelor de evaluare a conformității, realizate de furnizorii de servicii în baza prevederilor normative;

10.7. organizarea de exerciții și simulări în materie de securitate cibernetică în vederea determinării nivelului de pregătire a furnizorilor de servicii în sectoarele critice în realizarea obligațiilor de asigurarea a securității cibernetice stabilite de cadrul normativ în acest domeniu;

10.8. organizarea și efectuarea de teste la stres, precum și, la solicitarea furnizorilor de servicii în sectoarele critice, a testelor de penetrare și a scanărilor rețelelor și sistemelor informatice ale acestora în vederea identificării vulnerabilităților și determinării măsurilor de securitate ce necesită a fi implementate.

11. Rezultatele măsurilor de supraveghere sunt utilizate de către Agenție pentru planificarea activității de control în baza analizei riscurilor pe domeniile de competență ale acesteia.

Capitolul III. Controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept privat, identificate ca furnizori de servicii în sectoarele critice

Secțiunea 1. Planificarea controlului de stat

12. Agenția efectuează controale de stat în privința furnizorilor de servicii persoane juridice de drept privat (furnizori de servicii privați) în baza Legii nr. 131/2012 privind controlul de stat și în baza prezentei hotărâri.

13. Agenția poate efectua controale dacă dacă a depistat și, în urma unei investigații preliminare, a confirmat fapte de încălcare a prevederilor Legii nr. 48/2023 privind securitatea cibernetică și/sau a fost sesizată cu privire la încălcări, neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor prevăzute de aceasta de către furnizorul de servicii privat.

14. Controlul se efectuează în temeiul delegației de control de către cel puțin doi inspectori ai Agenției.

15. În procesul de efectuare a controlului, inspectorii pot coopta alți angajați ai Agenției cu experiență profesională în domeniul de activitate al furnizorului de servicii privat supus controlului, cu condiția includerii acestora în delegația de control.

16. În procesul de efectuare a controlului, Agenția poate solicita suportul altor autorități sau instituții publice cu competențe în domeniul securității cibernetice,

inclusiv prin realizarea unui control comun, cu respectarea prevederilor legale care reglementează activitatea acestor entități.

17. Documentele întocmite în procesul de planificare se înregistrează în cadrul Agenției.

Secţiunea 2. Pregătirea și realizarea controlului

18. Agenția în exercitarea funcției de control:

18.1 realizează verificarea sistematică a modului de îndeplinire a obligațiilor privind respectarea măsurilor de securitate impuse de cadrul normativ;

18.2 constată abateri de la obligațiile prevăzute la pct. 18.1;

18.3 emite dispoziții cu caracter obligatoriu în vederea conformării și remedierii deficiențelor constatate în cursul activităților de control;

18.4 stabilește termene de conformitate cu măsurile de securitate impuse de cadrul normativ;

18.5. dispune, după caz, de aplicarea de sancțiuni prevăzute de cadrul normativ în vigoare.

19. Agenția înștiințează în prealabil furnizorul de servicii privat supus controlului cu privire la demararea activității de control.

20. La începutul controlului, Agenția pune la dispoziția furnizorului de servicii privat supus controlului toate documentele în baza căruia se efectuează controlul, inclusiv delegația de control și alte materiale și documente întocmite sau deținute în legătură cu exercitarea controlului și a căror divulgare nu poate afecta procesul de control.

21. În limitele admisibile, controlul se efectuează fără a influența desfășurarea activităților curente a furnizorului de servicii privat supus controlului.

22. Drepturile și obligațiile inspectorilor și furnizorilor de servicii privați pe parcursul desfășurării controlului sunt stabilite de articolele 23 - 26 ale Legii nr. 131/2012 privind controlul de stat.

23. În cazul în care personalul furnizorului de servicii privat supus controlului se află în imposibilitate de a participa la procesul de control, controlul se realizează în lipsa acestuia.

24. În cazul în care în timpul desfășurării controlului, inspectorii constată încălcări ce conțin semne ale unei infracțiuni, aceștia sunt obligați să ia măsuri de conservare a locului săvârșirii infracțiunii și de conservare a mijloacelor materiale de probă.

Aceștia au obligația de a consemna în procesul-verbal de control eventualele precizări sau explicații date de persoanele prezente la locul constatării.

25. Agenția sesizează organele de urmărire penală sau procurorul cu privire la încălcări constatate ce conțin semne ale unei infracțiuni, respectând procedura stabilită de Legea nr. 131/2012 privind controlul de stat și alte acte normative relevante.

26. Agenția poate solicita declanșarea imediată a măsurilor de remediere a anumitor deficiențe în situații de risc major sau care impun măsuri urgente.

27. Pentru a contracara o amenințare gravă și iminentă sau pentru a elimina o perturbare cauzată de un incident cibernetic, Agenția poate restricționa utilizarea unuia sau mai multe sisteme informatice sau accesul la acesta/acestea, dacă îndeplinite cumulativ următoarele condiții:

27.1. Incidentul cibernetic compromite sau afectează securitatea unui alt sistem informatic;

27.2. Administratorul sistemului informatic nu poate sau nu reușește să contracareze în timp util amenințarea gravă ori să elimine perturbarea cauzată de incidentul cibernetic;

27.3. Nu există posibilitatea de a contracara amenințarea gravă sau de a elimina perturbarea prin utilizarea unei măsuri mai puțin intruzive;

27.4. Măsurile dispuse nu cauzează un prejudiciu disproporționat persoanelor afectate în procesul de contracarare a amenințării sau de eliminare a perturbării generate de incidentul cibernetic.

28. În cazul care Agenția restricționează utilizarea unuia sau mai multe sisteme informatice sau accesul la acesta/acestea, urmare a îndeplinirii cumulative a condițiilor prevăzute la pct. 27, furnizorul de servicii privat este notificat imediat cu privire la aceasta.

Secţiunea 3. Finalizarea controlului

29. Constatările efectuate pe timpul verificărilor, concluziile și măsurile propuse se reflectă în procesul-verbal de control, care se semnează de toate persoanele cooptate pentru efectuarea controlului.

30. Proiectul procesului-verbal de control se prezintă furnizorului de servicii privat, oferind un termen de 5 zile pentru prezentarea observațiilor, cu excepția cazurilor justificate în mod corespunzător, când ar fi împiedicată de o acțiune imediată pentru a preveni sau răspunde la un incident.

31. Procesul-verbal de control se aduce la cunoștință furnizorului de servicii privat supus controlului, confirmată prin semnătura persoanei care recepționează procesul-verbal.

32. O copie a procesului-verbal de control se înmânează furnizorului de servicii privat supus controlului.

33. În caz de depistare a unor neconformități privind implementarea măsurilor de securitate, după caz, la procesul-verbal de control se anexează un plan de măsuri pentru remedierea deficiențelor și îmbunătățirea activităților furnizorului de servicii privat, care include în mod obligatoriu termene limită pentru realizare a acestora și termenul de raportare cu privire la punerea în aplicare a acestora.

34. Pe lângă prescripțiile emise și sancțiuni aplicate în temeiul procesului-verbal de control, Agenția poate:

1. emite avertismente cu privire la încălcarea prevederilor cadrului normativ în domeniul securității cibernetice;
2. emite instrucțiuni obligatorii prin care solicită furnizorilor de servicii privați să remedieze deficiențele și încălcările identificate;
3. dispune ca furnizorii de servicii privați să înceteze conduita prin care încalcă prevederile cadrului normativ în domeniul securității cibernetice și să se abțină de la repetarea conduitei respective;
4. dispune ca furnizorii de servicii privați să informeze persoanele fizice sau juridice, cărora le furnizează servicii privind o amenințare cibernetică semnificativă, inclusiv privind măsurile de protecție sau de remediere pe care le-ar putea lua persoanele fizice sau juridice în cauză ca răspuns la o amenințare cibernetică;
5. dispune ca furnizorii de servicii privați să pună în aplicare recomandările formulate în urma unui audit de securitate cibernetică într-un termen rezonabil;
6. solicită autorităților publice competente aplicarea, în conformitate cu cadrul normativ, a unei sancțiuni proporționale încălcării și impactului produs.

35. Procesul-verbal de control și anexele acestuia se secretizează dacă în conținutul acestora se regăsesc informații care presupun aplicarea prevederilor legale privind secretul de stat.

36. Procesul-verbal de control și anexele acestuia se comunică, după caz, organului de urmărire penală sau procurorului atunci când există indicii cu privire la săvârșirea unei posibile infracțiuni, respectând prevederile legale în domeniu.

Secţiunea 4. Monitorizarea măsurilor stabilite

37. Agenția monitorizează implementarea măsurilor stabilite pentru remedierea deficiențelor și îmbunătățirea activității furnizorului de servicii privat, constatate în cadrul controlului și incluse în anexa la procesul-verbal de control.

38. Nivelul de realizare a implementării măsurilor pentru remedierea deficiențelor și îmbunătățirea activității furnizorului de servicii privat se comunică Agenției în conformitate cu termenii stabiliți în anexa la procesul-verbal de control.

39. În cazul în care anumite măsuri prevăzute în anexa la procesul-verbal de control nu pot fi realizate în termen, furnizorul de servicii privat poate solicita Agenției extinderea termenului de realizare.

40. Decizia cu privire la extinderea termenului de realizare a măsurilor prevăzute în anexa la procesul-verbal de control se aprobă de Directorul Agenției.

41. Verificarea nivelului de realizare a măsurilor se realizează în baza evaluării rapoartelor transmise de entitatea supusă controlului, prin solicitarea de informații suplimentare sau prin realizarea activităților de supraveghere.

Capitolul IV. Controlul de stat al respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept public, identificate ca furnizori de servicii în sectoarele critice

Secțiunea 1. Planificarea controlului

42. Controlul respectării de către furnizorii de servicii în sectoarele critice care sunt persoane juridice de drept public (*în continuare - furnizorii de servicii publici*) se efectuează de Agenție în conformitate cu Planul anual al controlului respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii publici (în continuare - Planul).

43. Planul se aprobă de către Directorul Agenției și se publică pe pagina oficială în Internet a acesteia nu mai târziu de data de 15 a lunii care precedă perioada de gestiune.

44. Planificarea controalelor furnizorilor de servicii publici se efectuează în funcție de:

44.1. rezultatele evaluărilor de riscuri la nivel național, intersectorial, sectorial, și subsectorial;

44.2. categoria și nivelul de criticitate al furnizorului de servicii public;

44.3. rezultatele auditurilor de securitate cibernetică efectuate în conformitate cu Cerințele de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii în sectoarele critice, aprobate prin Hotărârea Guvernului nr. 562/2025;
44.4. rezultatele aplicării măsurilor de supraveghere prevăzute la punctul 10;
45. Planul cuprinde cel puțin, următoarele părți componente:
45.1. furnizorul de servicii public supus controlului;
45.2. obiectivele controlului;
45.3. perioada controlului.
46. Planul poate fi revizuit pe parcursul anului atunci când apar modificări semnificative ale riscurilor, incidente cibernetice cu impact semnificativ sau crize cibernetice.
47. Controlul inopinat al furnizorului de servicii public poate fi efectuat în următoarele cazuri:
47.1. producerea unui incident cibernetic în rețelele și sistemele informatice deținute de furnizorul de servicii respectiv;
47.2. deținerea de către Agenție a unor informații veridice privind existența unei amenințări cibernetice semnificative asupra rețelelor și sistemelor informatice deținute de furnizorul de servicii public;
47.3. deținerea de către Agenție a informațiilor privind neîndeplinirea sau îndeplinirea necorespunzătoare de către furnizorul de servicii public a obligațiilor de asigurare a securității cibernetice care prezintă un pericol iminent și imediat pentru viața și sănătatea persoanelor, pentru securitatea națională sau ordinea publică.
47.4. deținerea de către Agenție a informațiilor privind neîndeplinirea sau îndeplinirea necorespunzătoare de către furnizorul de servicii public a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ.
47.5. solicitarea din partea organului ierarhic superior sau a autorității publice care exercită supravegherea administrativă și controlul administrativ al furnizorului de servicii public.
48. Controlul inopinat se motivează. Nota de motivare se anexează la delegația de control.

Secțiunea 2. Pregătirea și realizarea controlului

49. Controlul se inițiază și se efectuează în temeiul delegației de control emisă de Directorul Agenției.

50. Delegația de control trebuie să conțină cel puțin:
50.1. numărul și data înregistrării;
50.2. temeiul controlului;
50.3. numele prenumele persoanelor ce vor efectua controlul;
50.4. denumirea furnizorului de servicii public și numele și prenumele conducătorului acestuia;
50.5. scopul controlului;
50.6. data începerii și durata preconizată a controlului.
51. Controlul se realizează de către cel puțin doi angajați ai Agenției (în continuare – echipa de control).
52. Furnizorul de servicii public este notificat în prealabil de către Agenție cu privire la controlul planificat cu cel puțin 5 zile înaintea începerii acestuia.
53. În cazul unui control inopinat, la începutul controlului echipa de control înmânează un exemplar al delegației de control furnizorului de servicii public.
54. În procesul de efectuare a controlului, Agenția poate solicita suportul altor autorități sau instituții publice cu competențe în domeniul securității cibernetice.
55. Activitatea de control se documentează în modul stabilit de cadrul normativ.
56. Odată cu recepționarea notificării remise de către Agenție cu privire la controlul preconizat, furnizorul de servicii public întreprinde măsurile necesare de pregătire pentru efectuarea controlul, inclusiv a personalului care urmează a fi implicat în procesul controlului.
57. Până la începerea nemijlocită a controlului, echipa de control informează furnizorul de servicii public despre actele normative, în baza cărora urmează a fi evaluată conformitatea în cadrul controlului, precum și pune la dispoziția furnizorului de servicii public orice alte documente în baza cărora se realizează controlul sau care urmează a fi utilizate în cadrul controlului.
58. Echipa de control asigură desfășurarea controlului prin minimizarea caracterului intrusiv al activităților de control în activitatea curentă a furnizorului supus controlului.
59. În procesul efectuării controlului, echipa de control are următoarele drepturi:
59.1. să pătrundă în orice încăpere utilizată de furnizorul de servicii în activitatea sa, în măsura în care aceasta este parte a obiectului controlului;
59.2. să solicite și să obțină orice informații, documente sau alte tipuri de date necesare pentru realizarea controlului;

59.3. să facă copii, înregistrări foto sau video ale documentelor sau ale altor obiecte purtătoare de informații.

60. În procesul efectuării controlului, echipa de control are următoarele obligații:

60.1. să se legitimeze și să informeze furnizorul de servicii public supus controlului despre drepturile și obligațiile acestuia;

60.2. să aprecieze obiectiv și echidistant toate aspectele ce țin de efectuarea controlului și să asigure integritatea bunurilor și a documentației furnizorului de servicii public suspus controlului;

60.3. să asigure controlul accesului la informațiile și documentele de care a luat cunoștință în procesul de realizare a controlului în conformitate cu cadrul normativ relevant;

60.4. să anexeze la actul de control orice documente sau copii ale acestora și explicații în scris ale furnizorului de servicii supus controlului și/sau ale angajaților acestuia.

61. În procesul efectuării controlului, furnizorul de servicii public are următoarele drepturi:

61.1. să verifice delegația de control și să ia cunoștință de legitimația de serviciu a inspectorilor;

61.2. să prezinte dovezi și explicații;

61.3. să ceară anexarea la actul de control a oricăror documente sau copii ale acestora, pe care are dreptul să aplice semnătura și să dea explicații în scris, precum și să ceară includerea în actul de control a informațiilor privind anumite fapte relevante procesului și procedurii de control;

61.4. să solicite Agenției suspendarea sau amânarea controlului pentru o altă perioadă, dacă continuarea controlului ar putea afecta continuitatea activității furnizorului de servicii public;

61.5. să ia cunoștință de actul de control și de alte acte și informații întocmite în cadrul controlului;

61.6. să asiste la acțiunile desfășurate în procesul realizării controlului de stat.

62. În procesul efectuării controlului de stat furnizorul de servicii public este obligat:

62.1. să prezinte documentele și informațiile ce țin de obiectul controlului, solicitate de echipa de control;

62.2. să permită accesul echipei de control în încăperile de serviciu;

63. În cazul în care personalul furnizorului de servicii public supus controlului se află în imposibilitate de a participa la activitățile desfășurate în cadrul controlului, acesta se realizează în lipsa personalului furnizorului de servicii public.
64. Agenția sesizează organele de urmărire penală sau procurorul cu privire la încălcări constatate ce conțin semne ale unei infracțiuni, respectând procedura stabilită de actele normative relevante.
65. În cazul în care obiectivele stabilite la planificarea activității de control nu au fost atinse sau au apărut circumstanțe noi pentru a căror clarificare sunt necesare acțiuni suplimentare, perioada de desfășurare a controlului se poate prelungi până la realizarea acestora, cu aprobarea Directorului Agenției.

Secțiunea 3. Finalizarea controlului

66. Constatările efectuate în timpul verificărilor, concluziile și măsurile propuse de inspectori se reflectă în procesul-verbal de control, care se semnează de toți inspectorii și, după caz, angajații Agenției cooptați pentru efectuarea controlului.
67. Procesul-verbal cuprinde:
67.1. principalele realizări;
67.2. deficiențele, disfuncțiile, neregulile și măsurile de ordin organizatoric și administrativ;
67.3. concluziile echipei de supraveghere;
67.4. alte aspecte care pot contribui la creșterea eficacității și eficienței activităților evaluate.
68. Modelul procesului verbal de control al furnizorilor de servicii publici se aprobă de Directorul Agenției.
69. Procesul-verbal se aduce la cunoștință furnizorului de servicii supus controlului, confirmată prin semnătura persoanei care recepționează procesul-verbal.
70. Proiectul procesului-verbal se prezintă furnizorului de servicii, oferind un termen de 5 zile pentru prezentarea observațiilor, cu excepția cazurilor justificate în mod corespunzător, când sunt în desfășurare acțiuni imediate pentru a preveni sau răspunde la un incident.
71. O copie a procesului-verbal se înmânează furnizorului de servicii supus activității de supraveghere.

72. La procesul-verbal se anexează un plan de măsuri pentru remedierea deficiențelor și îmbunătățirea activității furnizorului de servicii, care include în mod obligatoriu termene limită pentru realizarea acestora.

73. Procesul-verbal și anexele acestuia se secretizează dacă în conținutul acestora se regăsesc informații care presupun aplicarea prevederilor legale privind secretul de stat.

74. Procesul-verbal și anexele acestuia se comunică, după caz, organului de urmărire penală sau procurorului atunci când există indicii cu privire la săvârșirea unei infracțiuni, respectând prevederile legale în domeniu.

Secţiunea 4
Monitorizarea măsurilor stabilite

75. Agenția monitorizează implementarea măsurilor stabilite pentru remedierea deficiențelor și îmbunătățirea activităților furnizorului de servicii, constatate în procesul de efectuare a controlului și incluse în anexă la procesul-verbal.

76. Nivelul de realizare a implementării măsurilor pentru remedierea deficiențelor și îmbunătățirea activităților furnizorului de servicii se comunică Agenției în conformitate cu termenii stabiliți în anexa la procesul-verbal.

77. În cazul în care anumite măsuri prevăzute în anexa la procesul-verbal nu pot fi realizate în termen, furnizorul de servicii solicită Agenției extinderea termenului de realizare.

78. Decizia cu privire la extinderea termenului de realizare a măsurilor prevăzute în anexa la procesul-verbal se aprobă de Directorul Agenției.

79. Verificarea nivelului de realizare a măsurilor se realizează prin evaluarea rapoartelor transmise de furnizorul de servicii public Agenției la solicitarea acesteia sau periodic conform termenelor stabilite în anexa la procesul-verbal.

Nota de fundamentare
la proiectul hotărârii Guvernului cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ

Proiectul hotărârii Guvernului este elaborat de către Ministerul Dezvoltării Economice și Digitalizării, în calitate de autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice.

2. Condițiile ce au impus elaborarea proiectului actului normativ

2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ

Temeiul legal al elaborării și adoptării proiectului de act normativ îl constituie prevederile art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023 privind securitatea cibernetică (în continuare – Legea nr. 48/2023). Aceste norme stabilesc în competența Guvernului reglementarea:

- măsurilor de supraveghere și a modului de aplicare a acestora, și
- modului de efectuare a controlului de stat de către autoritatea competentă asupra respectării obligațiilor ce le revin acestora conform Legii nr. 48/2023 separat pentru furnizorii de servicii persoane juridice de drept privat și pentru furnizorii de servicii persoane juridice de drept public.

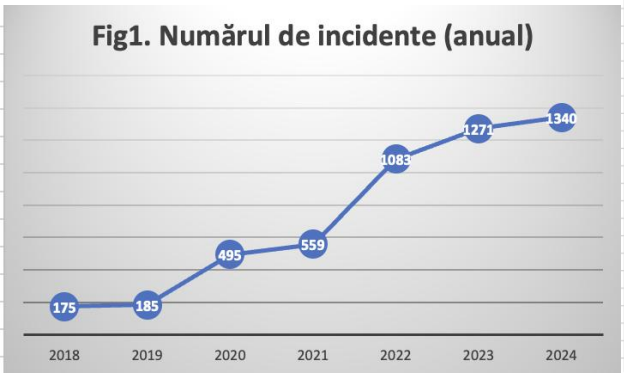
Elaborarea proiectului de act normativ propus spre examinare este prevăzută și de următoarele documente strategice ale Republicii Moldova:

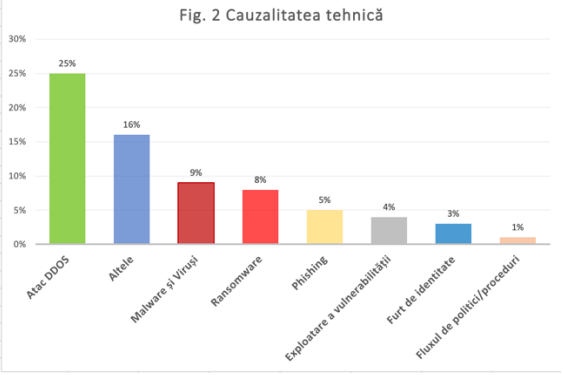
- Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 (Hotărârea Guvernului nr. 306/2025) - punctul 53, proiectul nr. 38 din Capitolul 10 „Societatea informațională și mass-media" al Clusterului 3 „Competitivitate și creștere incluzivă";
- Agenda de reforme aferentă Planului de creștere al Republicii Moldova pentru 2025-2027 (Hotărârea Guvernului nr. 260/2025) - măsura 2.3.11, indicatorul (v) „delimitarea clară și transparentă a competențelor instituțiilor de securitate cibernetică ale MD, cu ajustarea mandatelor instituțiilor relevante în urma unei note a unui expert.";
- Foaia de parcurs privind „Statul de drept" (criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană) (Hotărârea Guvernului nr. 275/2025) – acț. 4.1 și 4.3 din Rezultatul strategic nr. 4. „Consolidarea capacității de prevenire și combatere a criminalității cibernetice";
- Planul național de reglementări pentru anul 2025 (Hotărârea Guvernului nr. 841/2024) – acțiunea 18;
- Strategia de transformare digitală a Republicii Moldova (Hotărârea Guvernului nr. 650/2023) - Obiectivul general nr. 5. „Crearea unui mediu digital accesibil, sigur și incluziv direcții prioritare", direcția prioritară nr. 1) „Instituirea unei autorități competente în domeniul securității cibernetice la nivel național, cu funcții de punct unic de contact, echipă de răspuns la incidente de securitate cibernetică (CSIRT), dar și identificare, monitorizare și supraveghere, coordonare operațională a situațiilor de criză, de cooperare și interacțiune la nivel național și internațional.".

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

Între 2018 și 2024, statele membre ale Uniunii Europene au raportat un total de 5108 de incidente cibernetice cu impact semnificativ[1], conform criteriilor stabilite de Directiva NIS1[2], Codul[3] european al comunicațiilor electronice și Regulamentul eIDAS[4] . Dintre acestea, 29 % au fost considerate acțiuni rău intenționate. Cel mai afectat sector a fost sectorul privat, în special domeniile comunicațiilor, bancar, sănătate, servicii de încredere, transporturi și energie.

Datele indică o tendință generală de creștere a numărului de incidente cu impact semnificativ (figura 1). Din cele 1402 de incidente rău intenționate raportate, majoritatea au fost clasificate ca infracțiuni cibernetice, conform graficului de cauzalitate tehnică prezentat în figura 2.





Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

Conform *raportului actualizat al IBM privind costul unei încălcări a securității datelor în 2024*[5] , impactul financiar al încălcărilor securității datelor este și mai mare pentru entitățile critice. Raportul indică faptul că, în 2024, costul mediu global al unei încălcări a securității datelor a atins un nivel record de 4,88 milioane de dolari SUA, înregistrând o creștere de 10% față de 2023

Studiul global realizat de compania McAfee[6] , care a evaluat pierderile economice cauzate de criminalitatea informatică, intitulat "Pierderi nete: estimarea costului global al criminalității informatice", oferă o estimare a impactului economic al criminalității informatice pentru diferite țări, exprimat ca procent din PIB. Graficul prezentat în figura 3 evidențiază țările cele mai grav afectate în funcție de proporția daunelor monetizate în raport cu PIB-ul lor. În medie, pierderile cauzate de criminalitatea cibernetică reprezintă aproximativ 0,3% din PIB. Extrapolând aceste date pentru Republica Moldova, având în vedere că produsul intern brut al țării a fost de aproximativ 16,5 miliarde de dolari americani în 2023, se poate estima un prejudiciu anual potențial de aproximativ 49 de milioane de dolari, pe baza mediei de 0,3% din PIB.

---

[1] https://ciras.enisa.europa.eu/ciras-consolidated-reporting

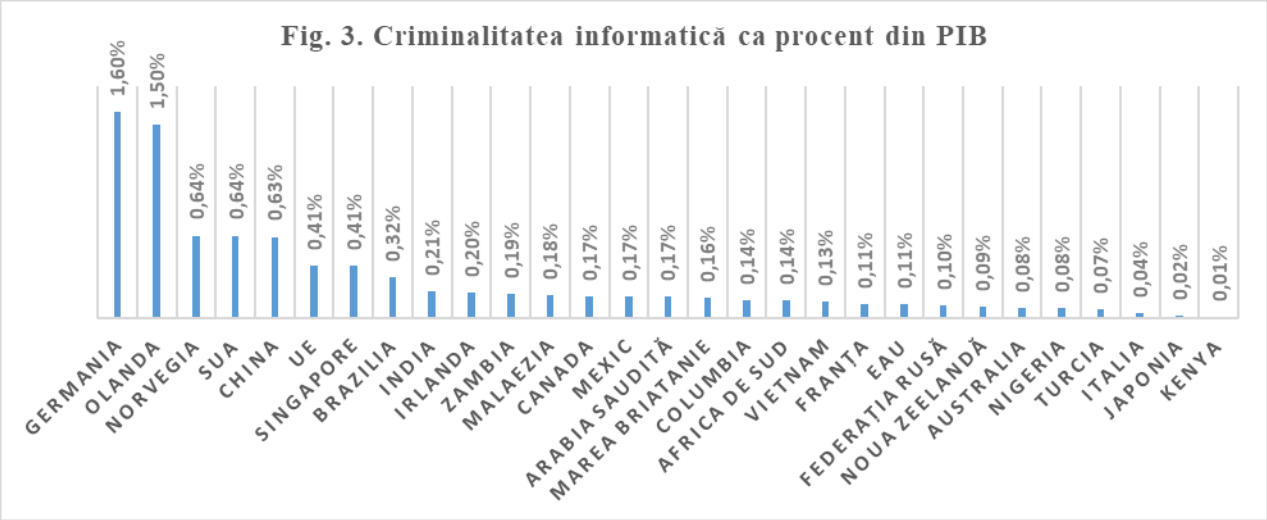
[2] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32016L1148

[3] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02018L1972-20241018

[4] Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02014R0910-20241018

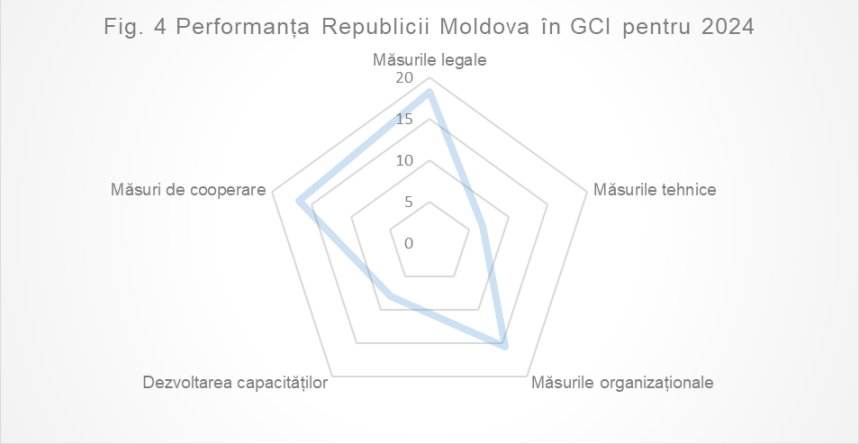
[5] https://www.ibm.com/reports/data-breach

[6] https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis



Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

Conform Indicelui Global de Securitate Cibernetică (GCI) al UIT pentru 2024, Republica Moldova are un scor general de 65,09, iar performanța țării este descrisă ca fiind de nivel 3 (nivelul 3 reprezintă țările care au obținut un scor general de cel puțin 55/100), demonstrând un angajament de bază în materie de securitate cibernetică, care include evaluarea, stabilirea sau implementarea anumitor măsuri de securitate cibernetică general acceptate, pe un număr moderat de piloni sau indicatori. Conform raportului UIT privind echipa națională de răspuns la incidente de securitate cibernetică, performanța Republicii Moldova pentru 2024, comparativ cu 2020, a înregistrat o creștere a măsurilor legale, organizaționale și de cooperare, însă o scădere notabilă a măsurilor tehnice și de dezvoltare a capacităților, dar acest lucru poate fi atribuit parțial ajustărilor metodologice și ponderilor GCI, precum și modificărilor aduse întrebărilor. Graficul de mai jos (Figura 4) evidențiază performanța Republicii Moldova în GCI pentru 2024, subliniind că măsurile tehnice și consolidarea capacităților sunt punctele slabe ale Republicii Moldova în acest domeniu. Cu toate acestea, acest indice poate fi îmbunătățit prin implementarea corespunzătoare a legislației naționale armonizate cu legislația UE.



Industria IT în Republica Moldova se dezvoltă rapid. În 2023, industria IT a atins o pondere de peste 5,3% din produsul intern brut, depășind 15 miliarde de lei în vânzări, ponderea sectorului TIC este de peste 8,3% din PIB, cu peste 25 de miliarde de lei în vânzări în 2023, realizate de aproximativ 3 200 de companii cu peste 35 000 de angajați. Creșterea în sectorul IT a fost generată de avantajele pe care Moldova le oferă ca destinație pentru externalizarea serviciilor IT, beneficiind de costuri competitive, amplasare geografică favorabilă și calificări ale forței de muncă, alături de un cadru fiscal și

administrativ facil pentru rezidenții Parcului IT Virtual Moldova. Rapoartele globale referitoare la digitalizare (cum ar fi Indicele UN DESA e-Guvernare, Indicele de Dezvoltare în Rețea NRI, Indicele Țării Digitale etc.), rapoartele emise de ANRCETI și sondajele anuale efectuate de Agenția de Guvernare Electronică (AGE) confirmă progresele semnificative ale Republicii Moldova în privința accesului la internet și utilizarea dispozitivelor IT, precum și dezvoltarea platformelor de e-guvernare.
Cu toate acestea, avansul rapid al tehnologiei informației și comunicațiilor electronice și al proceselor de transformare digitală, deși aduce beneficii incontestabile în diverse domenii, este însoțit de o creștere semnificativă și continuă a amenințărilor la adresa securității cibernetice. Reieșind din acestea, securitatea cibernetică a fost declarată ca fiind o prioritate la nivel național, acest aspect fiind reflectat într-un set de documente de politici, cum ar fi:

- ***Programul național de aderare a Republicii Moldova la Uniunea Europeană*** **pentru perioada 2025-2029**[7] acordă prioritate punerii în aplicare a Legii 48/2023 privind securitatea cibernetică, în special identificării furnizorilor de servicii critice și punerii în aplicare a cerințelor de securitate pentru rețele și sisteme informatice, precum și operaționalizării complete a Agenției pentru Securitate Cibernetică. Hotărârea Guvernului nr. 562/2025 „Cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice", care include în obiectul său de reglementare și cerințele de securitate pentru rețele și sisteme informatice, este în proces de promovare, urmând în timpul apropiat să fie supus examinării de către Guvern. Aceasta determină necesitatea consolidării capacităților furnizorilor de servicii din sectoarele critice, deoarece aceștia au nevoie de formare în ceea ce privește modul de punere în aplicare a cerințelor de securitate cibernetică și de respectare a cadrului normativ în domeniu.
- ***Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030***[8]***:*** unul dintre obiectivele acesteia este crearea unui mediu digital accesibil, sigur și incluziv, având ca scop asigurarea unei creșteri a nivelului de reziliență cibernetică a entităților-cheie din Republica Moldova. Aceste entități urmează fi gestionate mult mai eficient și transparent, iar incidentele cibernetice, precum și eventualele prejudicii materiale și reputaționale asociate acestora, vor fi evitate. În același timp, se urmărește implementarea unei abordări multidisciplinare, iar toate părțile interesate, inclusiv Guvernul, sectorul privat și societatea civilă, își vor asuma responsabilitatea și angajamentul comun pentru susținerea și cooperarea în asigurarea securității cibernetice.
- ***Strategia securității naționale a Republicii Moldova***[9], care evidențiază riscurile cibernetice la care este expusă Republica Moldova, subliniind în principal atacurile cinetice sau cibernetice lansate de actori statali externi asupra infrastructurii critice naționale și regionale, atacurile cibernetice lansate asupra instituțiilor publice sau private de către structuri specializate în criminalitatea cibernetică, precum și riscurile asociate evoluțiilor din domeniul tehnologiilor precum blockchain și criptomonede, inteligența artificială, învățarea automată, internetul obiectelor, tehnologia 5G, big data, tehnologiile cuantice, internetul ascuns.

La data de 16 martie 2023, Parlamentul a adoptat Legea nr. 48/2023 privind securitatea cibernetică, care a intrat în vigoare la data de 1 ianuarie 2025. Legea are ca obiectiv general să asigure legalitatea în spațiul cibernetic prin 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. Un

[7] https://www.legis.md/cautare/getResults?doc_id=148720&lang=ro
[8] https://www.legis.md/cautare/getResults?doc_id=139408&lang=ro
[9] https://www.legis.md/cautare/getResults?doc_id=141253&lang=ro

instrument juridic esențial asumat în procesul reglementării acestui domeniu a constituit legislația Uniunii Europene, inclusiv în contextul obținerii de către Republica Moldova a statutului de țară candidat la aderarea la Uniunea Europeană, prin Legea respectivă asigurându-se, deși doar parțial, armonizarea cadrului normativ național la prevederile Directivei NIS2[10] și, implicit, a unor elemente esențiale ale Directivei NIS1[11].

Astfel, Legea privind securitatea cibernetică cuprinde un set de reglementări care au ca scop în principal:

a) stabilirea cadrului general privind cooperarea și coordonarea strategică la nivel național și internațional, prin reglementarea expresă a constituirii unui consiliul coordonator cu rol consultativ al Guvernului, dedicat exclusiv domeniului securității cibernetice și stabilirea obligativității adoptării unei strategii naționale în acest domeniu;

b) desemnarea/instituirea de către Guvern a unei autorități competente în domeniul securității cibernetice la nivel național, care să includă în competența sa, de rând cu funcțiile de coordonare, cooperare internă, supraveghere și control de stat, și pe cele de echipă națională de răspuns la incidentele cibernetice și de punct unic de contact la nivel național;

c) reglementarea legală primară a procesului de coordonare și gestionare a crizelor în domeniul securității cibernetice și atribuirea competenței legale în această materie viitoarei autorități responsabile;

d) stabilirea cadrului legal primar în ce privește obligațiile de asigurare a securității cibernetice nu doar de către persoanele juridice de drept public, ci și de către cele de drept privat, în mod special în ceea ce privește obligațiile de implementare a măsurilor de securitate și în ceea ce privește obligațiile de notificare a incidentelor cibernetice semnificative, și împuternicirea autorității competente la nivel național în acest domeniu cu exercitarea funcțiilor de supraveghere și control de stat al modului în care persoanele vizate îndeplinesc aceste obligații;

e) determinarea cadrului normativ primar pentru identificarea persoanelor juridice ca fiind furnizori de servicii esențiale, împuternicire atribuită, de asemenea, autorității respective, ca parte componentă a funcției de supraveghere etc.

Totuși, Legea nr. 48/2023 privind securitatea cibernetică stabilește doar cadrul normativ primar în domeniul securității cibernetice, pentru punerea în aplicare a acesteia fiind necesară aprobarea unor acte normative, în mod specific, la nivelul Guvernului. O parte importantă a chestiunilor abordate în lege, reglementarea cărora a fost dată în competența Guvernului, a fost deja soluționată prin aprobarea următoarelor acte normative:

- ***Hotărârea Guvernului nr. 1028/2023*** cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică;
- ***Hotărârea Guvernului nr. 333/2024*** cu privire la instituirea, organizarea și funcționarea Consiliului coordonator în domeniul securității cibernetice;
- ***Hotărârea Guvernului nr. 860/2024*** cu privire la identificarea furnizorilor de servicii;
- ***Hotărârea Guvernului nr. 112/2025*** pentru modificarea unor hotărâri ale Guvernului (*modificarea actelor normative subsidiare în conformitate cu Legea nr.48/2023 privind securitatea cibernetică și legile conexe*)
- ***Hotărârea Guvernului nr. 562/2025*** cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice.

[10] ***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;

[11] ***Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului*** din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;

Proiectul de act normativ propus nu este generat ca urmare a identificării unei probleme noi, ci este o măsură care asigură implementarea prevederilor Legii nr. 48/2023 privind securitatea cibernetică și actele normative aprobate pentru punerea acesteia în aplicare. **Problema principală** care urmează a fi soluționată prin inițiativa propusă, astfel cum a fost identificată în analiza de impact aferentă proiectului de lege, ulterior aprobat prin Legea nr. 48/2023 privind securitatea cibernetică, constă în nivelul general insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor ce vizează securitatea rețelelor și a sistemelor informatice. Această deficiență poate compromite buna funcționare a administrației publice centrale și locale, în special în ceea ce privește prestarea serviciilor publice, precum și activitatea economică a întreprinderilor din sectorul privat, afectând în consecință întreaga economie națională și, implicit, viața socială.

Categoria de subiecți interesați în intervenția propusă poate fi grupată în următoarele categorii:

1. ***Guvernul și Ministerul Dezvoltării Economice și Digitalizării, în calitatea sa de autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice*** – din perspectiva, pe de o parte, a necesității instituirii unui mecanism instituțional și organizațional viabil de implementare a politicii de stat în domeniul securității cibernetice, în vederea asigurării rezilienței cibernetice a cercului de subiecți care cad sub incidența actului normativ, iar, pe de altă parte – necesitatea armonizării cadrului normativ național;
2. ***Persoanele juridice de drept public***, inclusiv ***autoritățile administrației publice locale*** – categorie care prin efectul legii sunt identificate ca furnizori esențiali sau importanți de servicii;
3. ***Persoanele juridice de drept privat, inclusiv întreprinderile de stat,*** care cad sub incidența prevederilor proiectului de act normativ;
4. ***Utilizatorii finali ai serviciilor*** prestate de furnizorii de servicii, esențiali sau importanți, din perspectiva interesului pe care îl au în creșterea calității serviciilor de care beneficiază, în mod special din punctul de vedere al securității și protecției datelor cu caracter personal.

Problematica descrisă mai sus are la bază o serie de cauze:

1. măsuri de securitate a rețelelor și sistemelor informatice implementate fragmentar sau chiar lipsa acestora;
2. schimbul insuficient de informații cu privire la incidente, riscuri și amenințări de securitate cibernetică în ambele sectoare, public și privat. Vulnerabilitățile și incidentele cibernetice nu sunt raportate, în principal din cauza reticenței companiilor de a dezvălui aceste informații, din temerea prejudiciilor aduse reputației sau a posibilei răspunderi.
3. cadrul instituțional, procedural și normativ-juridic incomplet.

3. Obiectivele urmărite şi soluţiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Prezentul proiect de hotărâre de Guvern va contribui la realizarea **obiectivului general al întregului cadru normativ în domeniul securității cibernetice** și anume de creștere a nivelului de reziliență cibernetică a furnizorilor de servicii, privați sau publici, asigurând un nivel ridicat de protecție a rețelelor și sistemelor informatice ale acestor furnizori utilizate în procesul de prestare de către aceștia a serviciilor esențiale.

Ca **obiective specifice** ale prezentului proiect de hotărâre de Guvern, care odată realizate vor contribui la atingerea obiectivului general enunțat mai sus, trebuie relevate următoarele:

– stabilirea unor mecanisme de evaluare a implementării cerințelor de securitate a rețelelor și sistemelor informatice pe care le dețin și le utilizează furnizorii de servicii din sectoarele critice;

– stabilirea procedurilor privind modul de exercitare de către Agenția pentru Securitate Cibernetică a funcțiilor de supraveghere și control de stat.

Proiectul de act normativ propus spre examinare are ca **obiect de reglementare** stabilirea cadrului juridic, organizatoric și procedural de exercitare de către Agenția pentru Securitate Cibernetică a

funcției de supraveghere și control de stat al modului în care furnizorii de servicii în sectoarele critice asigură conformarea cu prevederile cadrului normativ în domeniul securității cibernetice.

Domeniul de aplicare al proiectului propus spre examinare se extinde asupra tuturor furnizorilor de servicii, esențiali și importanți, care sunt sau urmează să fie identificați de Agenția pentru Securitate Cibernetică în conformitate cu prevederile Hotărârii Guvernului nr. 860/2024.

Din punct de vedere structural, proiectul include partea dispozitivă a hotărârii de Guvern și anexa.

Partea dispozitivă cuprinde decizia Guvernului de adoptare a regulamentului în speță și sarcina Ministerului Dezvoltării Economice și Digitalizării de elaborare, în comun cu Agenția pentru Securitate Cibernetică, a Metodologiei privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică.

Anexa cuprinde Regulamentul cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice. Acesta include patru capitole.

Capitolul I – Dispoziții generale – cuprinde prevederi care determină obiectul de reglementare al proiectului, actele legislative relevante care cuprind definițiile unor noțiuni utilizate în textul proiectului de act normativ, precum și categoria de subiecți care cad sub incidența prevederilor actului normativ. Totodată, capitolul enunță principiile specifice exercitării funcției de supraveghere și control de către Agenția pentru Securitate Cibernetică, dintre care se remarcă principiile proporționalității, eficacității și efectului de descurajare, principii expres prevăzute atât în Directiva NIS2, cât și în legislația națională în domeniul securității cibernetice.

Conform art. 25 alin. (2) lit. c) din Legea nr.98/2012 privind administrația publică centrală de specialitate, una din funcțiile de bază ale unui minister este ***funcția de supraveghere și control de stat***. Această funcție este constituită din ***două părți componente***: ***supravegherea***, definită ca fiind totalitatea acțiunilor întreprinse prin analiza continuă sau periodică a unor informații ce țin de persoanele fizice și juridice, fără a interveni în activitatea acestora, și ***controlul de stat***, definită ca verificarea respectării de către persoanele fizice și juridice a prevederilor legislației, realizate în limitele și în conformitate cu legea. Unul dintre principiile fundamentale de organizare și funcționare a administrației publice centrale de specialitate este ***delimitarea funcțiilor de elaborare și de promovare a politicilor de funcțiile de implementare a acestora,*** prevăzut la art. 4 pct. 1) lit. c) din nr.98/2012. În baza acestui principiu, pus în aplicare și prin prevederile art. 14 din Legea nr. 98/2012, funcția de supraveghere și control de stat a fost atribuită prin Legea nr. 48/2023 cu privire la securitatea cibernetică Agenției pentru Securitate Cibernetică. ***Conceptul propus în proiect*** urmează această abordare, delimitând reglementările care vizează supravegherea și controlul de stat în capitole separate. Aceasta este motivat de faptul că supravegherea este diferită de controlul de stat atât prin compoziția sa materială, cât și din punct de vedere a problematicii procedurale pe care o implică. De asemenea, supravegherea diferă de controlul de stat atât prin obiectivele pe care le urmărește și mijloacele pe care le folosește, cât și prin intensitatea și consistența intervenției autorității publice în exercitarea acestei subfuncții. Un alt aspect important al conceptului propus în proiect derivă din prevederile art. 19 alin. (5) din Legea nr. 48/2023, care deleagă Guvernului reglementarea modului de efectuare a controlului de stat de către ASC, însă separat pentru persoanele juridice de drept public și, respectiv, pentru persoanele juridice de drept privat. Această separare este determinată de domeniul de aplicare a Legii nr. 131/2012 privind controlul de stat. Potrivit art. 1 controlul se extinde doar asupra controlului de stat al activității de întreprinzător. Acțiunea legii respective poate fi extinsă și asupra controlului persoanelor care nu practică activitatea de întreprinzător doar dacă legile speciale fac referință la Legea nr. 131/2012. Potrivit prevederilor art. 19 alin. (1) din Legea nr. 48/2023, Agenția pentru Securitate Cibernetică exercită controlul de stat asupra respectării legii de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr.131/2012 privind controlul de stat.

Prevederea punctului 5 este determinată de necesitatea asigurării complementarității dintre cadrul strategic și operațional din domeniul securității cibernetice cu cel din domeniul protecției fizice a infrastructurii critice din perspectiva exercitării funcției de supraveghere și control de stat. Cadrul strategic și operațional în domeniul protecției fizice a infrastructurii critice este reglementat prin Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale. Legea nr. 48/2023 privind securitatea cibernetică și Legea nr. 223/2025 sunt acte ce asigură armonizarea cadrului normativ național la Directiva (UE) 2022/2555 [12] și, respectiv, la Directiva (UE) 2022/2557 [13]. Complementaritatea acestor două directive și, implicit, a legilor naționale menționate mai sus, constă în necesitatea asigurării unei cooperări și unui schimb de informații între autoritățile competente în temeiul acestor cadre legislative, *„în special în ceea ce privește identificarea entităților critice, a riscurilor, a amenințărilor cibernetice și a incidentelor, precum și în legătură cu riscurile, amenințările și incidentele de altă natură decât cibernetică ce afectează entitățile critice, inclusiv măsurile în materie de securitate cibernetică și măsurile fizice adoptate de entitățile critice precum și* ***rezultatele activităților de supraveghere*** *desfășurate în legătură cu astfel de entități. În plus, pentru a raționaliza activitățile de supraveghere între autoritățile competente (n.n. – din ambele domenii de activitate) ... și pentru a reduce la minimum sarcina administrativă pentru entitățile în cauză, autoritățile competente ar trebui să depună eforturi pentru a armoniza modelele de notificare a incidentelor și* ***procesele de supraveghere****. După caz, autoritățile competente în temeiul Directivei (UE) 2022/2557 ar trebui să poată solicita autorităților competente în temeiul prezentei directive să își exercite competențele de supraveghere și de asigurare a respectării legii în legătură cu o entitate care este identificată drept o entitate critică în temeiul Directivei (UE) 2022/2557. Autoritățile competente în temeiul prezentei directive și cele competente în temeiul Directivei (UE) 2022/2557 ar trebui, atunci când este posibil în timp real, să coopereze și să facă schimb de informații în acest scop."*[14]

În **Capitolul II –** ***Supravegherea respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice*** **–** sunt reglementate aspecte privind modul de supraveghere asupra respectării cadrului normativ în domeniul securității cibernetice de către toți furnizorii de servicii în sectoarele critice: atât de către cei care sunt persoane juridice de drept public, cât și de către cei care sunt persoane juridice de drept privat. În capitol sunt enumerate măsurile de supraveghere pe care ASC urmează să le realizeze în exercitarea acestei funcții și limitele și principalele caracteristici ale acestora. Conform proiectului, măsurile de supraveghere urmează a fi aplicate în baza rezultatelor evaluării riscurilor în domeniul securității cibernetice la nivel național, intersectorial, sectorial, subsectorial, precum și atunci când este relevant, în baza evaluărilor de riscuri în alte domenii, iar scopul acestora este să asigure facilitarea conformării, consolidarea capacităților și creșterea nivelului de reziliență cibernetică a furnizorilor de servicii.

Capitolul III - ***Controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept privat, identificate ca furnizori de servicii în sectoarele critice*** – reglementează procedura controlului de stat în privința furnizorilor de servicii în sectoarele critice, care sunt persoane juridice de drept privat, principiile și procedura stabilită de prevederile Legii nr. 131/2012 privind controlul de stat fiind aplicate corespunzător.

[12] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555

[13] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557

[14] Recitalul 33 din 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).

În **Capitolul IV -** ***Controlul de stat al respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept public, identificate ca furnizori de servicii în sectoarele critice*** **–** sunt reglementate aspecte privind activitatea desfășurată de către ASC în exercitarea funcției de control de stat asupra furnizorilor de servicii din sectorul public. Capitolul cuprinde prevederi privind planificarea controlului, pregătirea și realizarea controlului, etapa finalizării acestuia și monitorizarea măsurilor stabilite. Având în vedere faptul că prevederile Legii 131/2012 privind controlul de stat nu se răsfrâng asupra entităților din sectorul public, capitolul descrie o procedură separată pentru aceste entități și simplificată, într-o anumită măsură, din perspectiva faptului că entitățile din sectorul public, nepracticând activitate de întreprinzător nu pot beneficia de întregul spectru de garanții oferite de Legea respectivă mediului privat. Din contra aceste entități poartă o responsabilitate sporită dat fiind interesul public pe care îl protejează și în realizarea căruia își desfășoară activitatea administrativă. Cu toate acestea, procedura propusă păstrează garanții legate de continuitatea activității furnizorului de servicii, documentarea procesului, planificarea activității de control, etc.

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

Opțiunile alternative nu au fost luate în considerare deoarece la nivel de lege este stabilită obligația Guvernului de a aproba cerințe privind măsurile de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Proiectul de act normativ nu implică impacturi structurale și instituționale asupra sistemului administrației publice, inclusiv acțiuni de reformă structurală sau instituțională.

4.2. Impactul financiar și argumentarea costurilor estimative

Impactul financiar direct al proiectului asupra mediului de afaceri este reprezentat de costurile administrative ce urmează a fi suportate de către agenții economici. În vederea estimării costurilor administrative pe care agenții economici trebuie să le suporte pentru a se conforma obligațiilor informaționale impuse prin prezentul proiect de hotărâre de Guvern este utilizată Metodologia de estimare a costurilor administrative prin aplicarea Modelului Costului Standard aprobată prin Hotărârea Guvernului nr. 307/2016.

Astfel, în sensul Metodologiei menționate supra, obligația informațională generată pentru agenții economici de noile prevederi normative, în calitatea lor de furnizorii de servicii, este participarea la realizarea controlului de către Agenția pentru Securitate Cibernetică.

În continuare se prezintă potențialul cost administrativ care l-ar putea suporta un agent economic supus controlului, respectând formula dată de Metodologia de estimare a costurilor administrative prin aplicarea Modelului Costului Standard, aprobată prin Hotărârea Guvernului nr. 307/2016:

Acte normative	Autorități implicate	Descrierea obligației informaționale	Activități administrative	Timp, ore	Tarif, lei/oră	Preț, lei	Achiziții, lei	**Preț total, lei**	Numărul de agenți economici	Frecvența, număr pe an	**Cantitate, număr pe an**	**Costuri administrative totale, lei**
1	2	3	4	5	6	7=5x6	8	**9=7+8**	10	11		
Legea nr. 48/2023 privind securitatea cibernetică (art.4)	Agenția pentru Securitate Cibernetică	Participarea la realizarea controlului de către Agenția pentru Securitate Cibernetică	Familiarizarea cu obligația informațională	6,0	105,1	630,6	0,0	**630,6**			**630,6**	**630,6**
			Asistarea în procesul de efectuare a controlului	64,0	105,1	6726,4	0,0	**6726,4**			**6726.4**	**6726,4**
			Prezentarea informațiilor pe marginea	10,0	105,1	1051	0,0	**1051**			**1051**	**1051**

			procesului verbal de control									
			TOTAL									**8408,0**

Aceleași estimări urmează a fi aplicate și evaluării impactului financiar asupra sectorului public din perspectiva obligațiilor pe care furnizorii de servicii din acest sector urmează să le realizeze.
Totodată, evidențiem că activitatea ASC în exercitarea funcției de supraveghere și control de stat în domeniul securității cibernetice urmează a se efectua în limita mijloacelor financiare aprobate acestei autorități în bugetul de stat.

4.3. Impactul asupra sectorului privat

Sub aspectul impacturilor non-financiare asupra sectorului privat ținem să relevăm în mod special că proiectul de act normativ propus spre examinare va contribui la:
- Consolidarea rezilienței și securității cibernetice: Soluția propusă va contribui la consolidarea securității cibernetice prin detectarea și blocarea eficientă a atacurilor, protejând datele și informațiile sensibile și asigurând reacții rapide;
- Protecția informațiilor și a drepturilor utilizatorilor: Implementarea soluției va spori protecția informațiilor personale și a drepturilor utilizatorilor, prevenind accesul neautorizat și utilizarea abuzivă a datelor;
- Reducerea costurilor asociate incidentelor cibernetice: Soluția va reduce riscurile, impactul și costurile financiare legate de incidentele cibernetice, cum ar fi pierderile de date și daunele reputației sau perturbarea serviciilor, economisind astfel resursele necesare pentru recuperare și remediere;
- Siguranța infrastructurii critice: Soluția va proteja infrastructura critică, cum ar fi rețelele energetice, sistemul bancar și transportul, reducând riscul de întreruperi majore și asigurând continuitatea serviciilor vitale;
- Îmbunătățirea cooperării dintre autoritățile publice responsabile și furnizorii de servicii în sectorul privat în implementarea cerințelor de securitate a rețelelor și sistemelor informatice, aprobate prin Hotărârea Guvernului nr. 562/2025.

4.4. Impactul social

4.4.1. Impactul asupra datelor cu caracter personal

Din perspectiva datelor cu caracter personal, prevederile proiectului de act normativ vor avea un impact pozitiv, având în vedere că acesta are ca obiectiv ridicarea nivelului de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii esențiale.

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

Nu este aplicabil.

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 19.05.2025 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de act normativ 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/anunt-privind-initierea-procesului-de-elaborare-a-proiectului-hotararii-de-guvern-cu-privire-la-supravegherea-si-controlul-de-stat-al-modului-in-care-furnizorii-de-servicii-respecta-prevederile-legii-nr-482023-privind-securitatea-cibernetica/14506)
7. Concluziile expertizelor
Proiectul de act normativ urmează a fi supus expertizei anticorupție și expertizei juridice, conform procedurii stabilite de cadrul normativ.
8. Modul de încorporare a actului în cadrul normativ existent
Adoptarea și intrarea în vigoare a proiectului nu va necesita modificarea cadrului normativ existent. Totuși, după cum este reflectat și în partea dispozitivă a hotărârii Guvernului, pentru punerea în aplicare a acestei hotărâri, Ministerul Dezvoltării Economice și Digitalizării, în comun cu Agenția pentru Securitate Cibernetică, urmează să elaboreze și să prezinte Guvernului spre examinare Metodologia privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică.
9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ
Instituția principală responsabilă de asigurarea implementării proiectului de act normativ este Agenția pentru Securitate Cibernetică. Pentru a asigura punerea în aplicare a prevederilor proiectului propus spre examinare, Agenția urmează: - să finalizeze operaționalizarea în volum deplin a subdiviziunii responsabile de supraveghere și control; - să aprobe ghiduri și orientări metodologice privind implementarea măsurilor de securitate a rețelelor și a sistemelor informatice ale furnizorilor de servicii în sectoarele critice; - să efectueze evaluări ale riscurilor la nivel național, sectorial, subsectorial și în baza rezultatelor acestora să planifice activitățile de supraveghere și control de stat; - să acorde suport consultativ furnizorilor de servicii, precum și să întreprindă alte acțiuni menite să faciliteze conformarea furnizorilor de servicii în sectoarele critice cu prevederile cadrului normativ în materie de securitate cibernetică, în mod special cu cerințele de securitate a rețelelor și sistemelor informatice ale acestora; - să evalueze nivelul de conformare a furnizorilor de servicii în sectoarele critice cu cerințele cadrului normativ în domeniul securității cibernetice.

Viceprim-ministru,

Ministru al Dezvoltării Economice și Digitalizării **Eugen OSMOCHESCU**

Ministerul Dezvoltării
Economice și Digitalizării
al Republicii Moldova

Nr. 13/2- 3189 din 11.11.2025

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 supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice* pentru a fi inclus în lista proiectelor care urmează a fi examinate în cadrul ședinței secretarilor generali.

Reieșind din faptul că proiectul menționat este inclus în documentele strategice ale Republicii Moldova, și anume *Agenda de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025–2027* (aprobat prin Hotărârea Guvernului nr. 260/2025) și *Foaia de parcurs privind „Statul de drept”*, care constituie un criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană (aprobată prin Hotărârea Guvernului nr. 275/2025), având termen de realizare anul 2025, solicităm respectuos includerea acestuia, în regim de urgență, pe agenda 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 supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice.
2.	Autoritatea care a elaborat proiectul	Proiectul este elaborat de către Ministerul Dezvoltării Economiei și Digitalizării cu suportul partenerului de dezvoltare.
3.	Justificarea depunerii cererii	Proiectul este elaborat în temeiul prevederilor art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023 privind securitatea cibernetică, precum și în scopul asigurării unui nivel sporit de securitate cibernetică a rețelelor și sistemelor informatice.
4.	Referința la documentul de planificare care prevede elaborarea proiectului *(PNA, PND, PNR, alte documente de planificare sectoriale)*	1) Agenda de reforme aferentă Planului de creștere al Republicii Moldova pentru 2025-2027 (Hotărârea Guvernului nr. 260/2025) – măsura 2.3.11, (v) delimitarea clară și transparentă a competențelor instituțiilor de securitate cibernetică ale MD, cu ajustarea mandatelor instituțiilor relevante în urma unei note a unui expert. 2) Foaia de parcurs privind „Statul de drept” (criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană) (Hotărârea Guvernului nr. 275/2025) – acț. 4.1 și 4.3 din Rezultatul

		strategic nr. 4. „Consolidarea capacității de prevenire și combatere a criminalității cibernetice”. 3) Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 (Hotărârea Guvernului nr. 306/2025) – Cap.10, proiectul 38. 4) Planul național de reglementări pentru anul 2025 (Hotărârea Guvernului nr. 841/2024) – acțiunea 18. 5) Strategia de transformare digitală a Republicii Moldova (Hotărârea Guvernului nr. 650/2023) - Obiectivul general nr. 5. „Crearea unui mediu digital accesibil, sigur și incluziv”.
5.	Lista autorităților și instituțiilor a căror avizare este necesară	1. Cancelaria de Stat 2. Aparatul Președintelui Republicii Moldova 3. Ministerul Infrastructurii și Dezvoltării Regionale (inclusiv Agenția Națională Transport Auto, Agenția Navală a Republicii Moldova, Autoritatea Aeronautică Civilă) 4. Ministerul Energiei 5. Ministerul Finanțelor 6. Ministerul Mediului (inclusiv Agenția de Mediu, Agenția Națională de Reglementare a Activităților Nucleare și Radiologice) 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 Siguranța Alimentelor 20. Agenția Medicamentului și Dispozitivelor Medicale 21. Agenția Națională pentru Cercetare și Dezvoltare 22. Agenția Națională pentru Reglementare în Energetică 23. Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației 24. Agenția Proprietății Publice (inclusiv ÎS „Administrația de Stat al Drumurilor”, ÎS „Calea Ferată din Moldova”) 25. Comisia Națională a Pieței Financiare 26. Biroul Național de Statistică 27. Banca Națională a Moldovei 28. Centrul Național pentru Protecția Datelor cu Caracter Personal 29. Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător 30. Centrul de Armonizare a Legislației
6.	Termenul-limită pentru depunerea avizelor/expertizelor	Termen-limită de prezentare a avizelor - 5 zile lucrătoare. Termenul de avizare pentru Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător - 5 zile lucrătoare.

7.	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 Veronica Duda, consultant principal al Secției politici în domeniul securității cibernetice, Direcția politici în domeniul tehnologiei informației și digitalizării tel.: 022 250 557 e-mail: veronica.duda@mded.gov.md
8.	Anexe	1. Proiectul hotărârii Guvernului 2. Nota de fundamentare
9.	Data și ora depunerii cererii	
10.	Semnătura	

Viceprim-ministru,
Ministru al Dezvoltării Economice și Digitalizării **Eugen OSMOCHESCU**