Nota de fundamentare
la proiectul hotărârii Guvernului cu privire la modul de realizare a obligațiilor de asigurare a 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 proiectului de act normativ este constituit din prevederile art. 11 alin. (4), art. 12 alin. (9) și art. 14 alin. (2) din Legea nr. 48/2023 privind securitatea cibernetică (în continuare – Legea nr. 48/2023). Aceste norme stabilesc corespunzător în competența Guvernului reglementarea următoarelor aspecte:

- aprobarea standardelor naționale în domeniul securității informației și al securității cibernetice în baza standardelor și a specificațiilor tehnice europene și celor internaționale relevante pentru securitatea rețelelor și a sistemelor informatice
- aprobarea cerințelor specifice de securitate privind rețelele și sistemele informatice în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.
- stabilirea procedurii de notificare a incidentelor cibernetice, inclusiv a interacțiunii dintre furnizorul de servicii și autoritatea competentă, a modul de stabilire a impactului unui incident cibernetic și formatul informațiilor, evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic;
- aprobarea măsurilor de securitate minime obligatorii pentru persoanele juridice de drept public.

Proiectul de act normativ propus spre examinare concentrează aceste aspecte într-o singură inițiativă de intervenție normativă, pe de o parte, din motivul multiplelor interconexiuni dintre cele două componente a obligațiilor de asigurare a securității cibernetice: măsurile de gestionare a riscurilor și notificarea incidentelor cibernetice semnificative și, în acest context, evitarea eventualelor dublări în cazul divizării reglementărilor în diferite acte, iar, pe de altă parte, unificarea abordării în ce privește sectorul public și sectorul privat pentru a evita potențialele conflicte în interpretarea de către entitățile din sectorul public a aplicabilității unor reglementări ce vizează măsurile de gestionare a riscurilor și obligațiile de notificare.

De asemenea proiectul are ca sursă:

- Regulamentul de punere în aplicare (UE) 2024/2690[1] al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere, și

[1] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R2690

- Comunicarea Comisiei Orientările[2] Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555 (Directiva NIS 2) 2023/C 328/02.

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

Similar cum este prezentat în analizele de impact asociate proiectului de Lege privind securitatea cibernetică și legilor conexe, inclusiv proiectul de hotărâre de Guvern referitoare la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică, potrivit datelor actualizate, în perioada 2018-2023, statele membre ale Uniunii Europene au înregistrat un total de 3251 incidente cibernetice cu impact semnificativ, conform criteriilor stabilite de Directiva NIS1, Codul european al comunicațiilor electronice și Regulamentul eIDAS. Din acest număr, 26% au fost considerate acțiuni rău intenționate. Sectorul cel mai afectate a fost cel privat, în special domeniile comunicațiilor, bancar, sănătate, servicii de încredere, transport și energie. Deși numărul incidentelor a înregistrat o scădere în 2023 comparativ cu 2022, tendința generală este de creștere a incidentelor cu impact semnificativ, conform *Figurii 1*. Din cele 847 de incidente rău intenționate raportate, majoritatea au fost clasificate ca infracțiuni cibernetice, conform graficului de cauzalitate tehnică prezentat în *Figura 2*. Aceste date subliniază necesitatea unei abordări riguroase, comprehensive și bine coordonate pentru prevenirea și gestionarea incidentelor cibernetice cu impact semnificativ.

Fig.1 Numărul de incidente (anual)

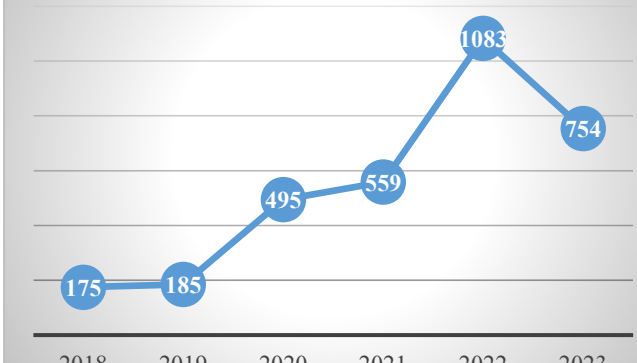
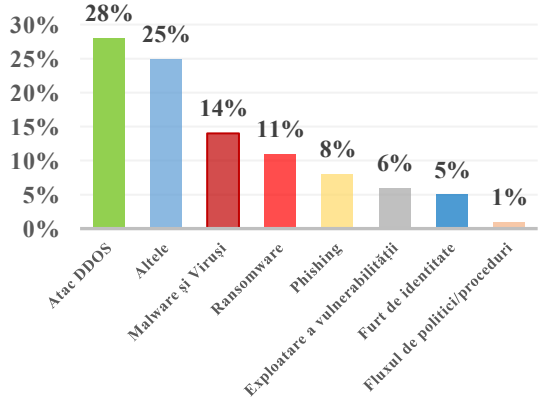


Fig. 2 Cauzalitatea tehnică

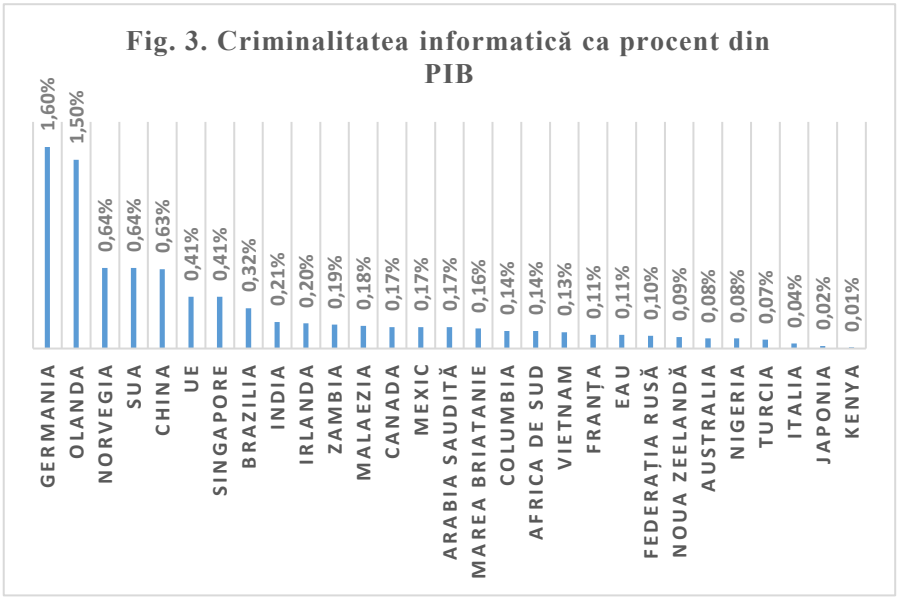


Conform raportului IBM *Cost of a Data Breach*[3] actualizat pentru anul 2023, impactul financiar al încălcării datelor este și mai mare pentru entitățile critice. Raportul arată că în 2023, costul mediu global al unei încălcări de date a atins un nivel record de 4,45 milioane de dolari americani, înregistrând o creștere cu 2,3% față de anul 2022 și o creștere cu 15,3% față de 2020. Comparând aceste date cu cele prezentate în analizele de impact anterioare, putem constata că de la instituirea cadrului normativ primar în domeniul securității cibernetice în Republica Moldova, impactul incidentelor cibernetice a devenit și mai pronunțat.

[2] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918(01)
[3] https://www.ibm.com/reports/data-breach

În plus, relevăm studiul global realizat de compania McAfee[4], care a evaluat pierderile economice cauzate de criminalitatea cibernetică. Acest studiu, intitulat *Net Losses: Estimating the Global Cost of Cybercrime*, furnizează o estimare a impactului economic al infracțiunilor informatice pentru diferite țări, exprimate ca procent din PIB. Graficul prezentat în *Figura 3* evidențiază țările cel mai grav afectate în funcție de proporția prejudiciului monetizat în raport cu PIB-ul lor. În medie, pierderile cauzate de infracțiunile cibernetice reprezintă aproximativ 0,3% din PIB. Extrapolând aceste date pentru Republica Moldova, având în vedere că Produsul Intern Brut al acesteia a fost de aproximativ 16,5 miliarde de dolari SUA în 2023, se poate estima un prejudiciu potențial anual de aproximativ 49 de milioane de dolari, bazat pe media de 0,3% din PIB.

Fig. 3. Criminalitatea informatică ca procent din PIB



Potrivit Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030[5], sectorul TIC a devenit principalul motor al digitalizării și inovării în Republica Moldova și este în creștere rapidă. În 2021, industria IT a atins o pondere de peste 4,2% din produsul intern brut (PIB), depășind 10 mlrd. lei vânzări, ponderea sectorului TIC fiind de peste 7,6 % din PIB, cu peste 18 mlrd. lei vânzări în anul 2021, realizate de circa 2000 de companii cu peste 30 000 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.

Prin urmare, deși Legea nr. 48/2023 privind securitatea cibernetică stabilește un cadru normativ de bază în domeniul securității cibernetice, absența unor reglementări complete la nivel sectorial pune în pericol funcționarea economiei Republicii Moldova, în special a celei digitale. În acest context, reziliența cibernetică a persoanelor juridice (atât publice, cât și private), care sunt furnizori de servicii esențiale și critice pentru funcționarea economiei naționale și a statului în ansamblu, devine un aspect de importanță majoră.

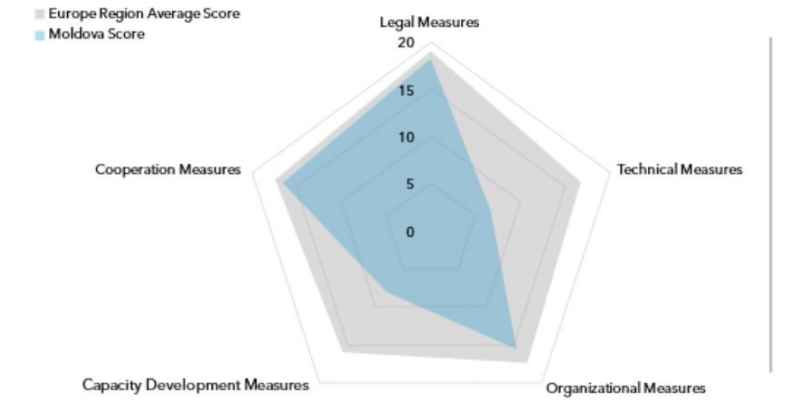
[4] https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis

[5] https://www.legis.md/cautare/getResults?doc_id=139408&lang=ro

Conform Indicelui Global de Securitate Cibernetică (GCI) al Uniunii Internaționale a Telecomunicațiilor (ITU) pentru anul 2024, scorul general al Republicii Moldova este de 65,09, iar performanța țării este descrisă ca fiind de nivel 3 - „Stabilire". Acest nivel reprezintă țările care au obținut un scor general de cel puțin 55/100, demonstrând un angajament de bază în materie de securitate cibernetică prin acțiuni guvernamentale care includ evaluarea, stabilirea sau implementarea anumitor măsuri de securitate cibernetică general acceptate într-un număr moderat de piloni sau indicatori. Acest indice evaluează angajamentul a 172 de țări în domeniul securității cibernetice, analizând gradul de conștientizare a importanței și dimensiunilor problemelor de securitate cibernetică, precum și rezistența și fiabilitatea sectorului TIC din fiecare țară.

Conform raportului ITU privind echipa de răspuns la incidente de securitate cibernetică la nivel național, performanța Republicii Moldova în cadrul GCI pentru 2024, în comparație cu anul 2020 a înregistrat o creștere a măsurilor juridice, organizatorice și de cooperare. Cu toate acestea, însă se remarcă o scădere notabilă a măsurilor tehnice și de dezvoltare a capacităților, însă acest lucru poate fi atribuit parțial ajustărilor metodologice și a ponderărilor GCI, precum și modificărilor aduse întrebărilor. Cu toate acestea, acest indice poate fi îmbunătățit prin armonizarea legislației naționale cu cea a UE și prin implementarea corespunzătoare a legislației naționale, inclusiv prin stabilirea unei autorități competente responsabile de gestionarea acestui sector.

Graficul de mai jos (*Figura 4*) evidențiază performanța Republicii Moldova în cadrul GCI pentru anul 2020, subliniind că măsurile organizaționale și consolidarea capacităților sunt punctele cele mai slabe ale Republicii Moldova în acest domeniu.



Domenii relativ consolidate:
Măsurile legale, de cooperare și organizaționale

Domenii cu potențial de creștere:
Măsurile tehnice și dezvoltarea capacităților

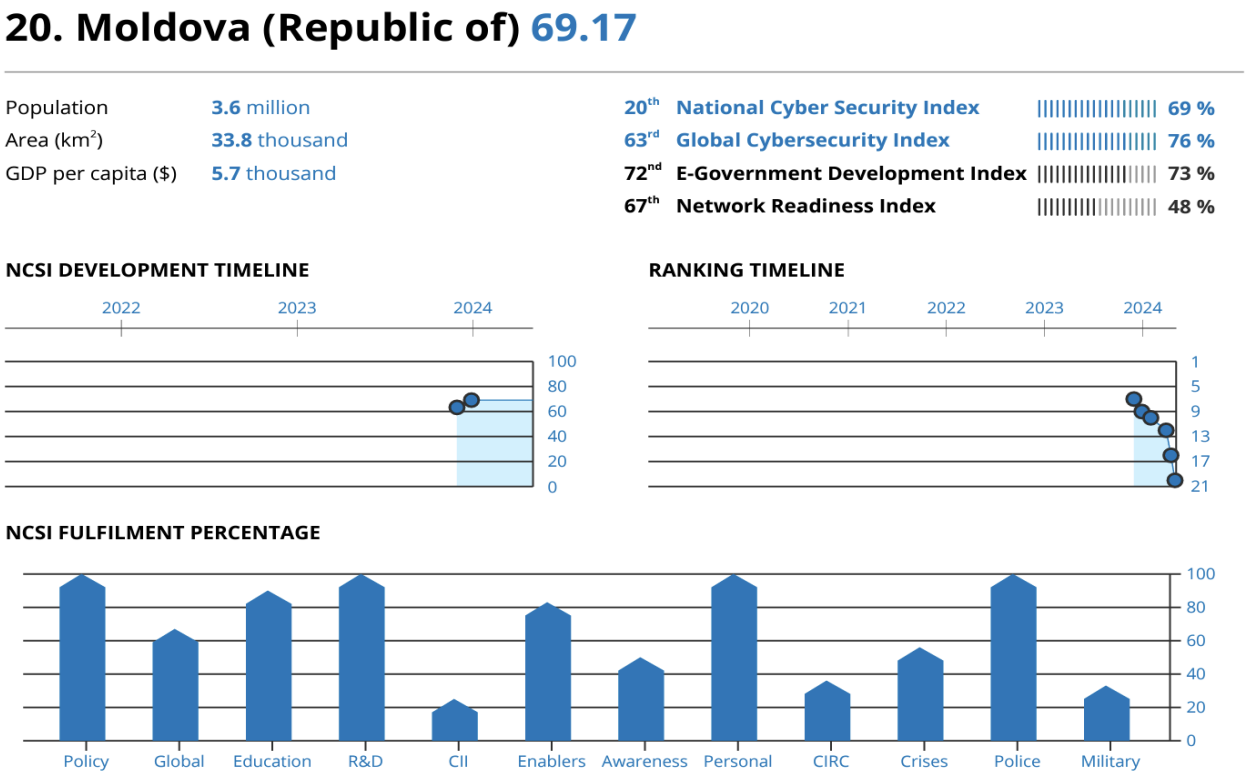
Scorul total	Măsurile legale	Măsurile tehnice	Măsurile organizaționale	Dezvoltarea capacităților	Măsuri de cooperare
65,09	18,28	6,68	15,51	8,04	16,58

De asemenea, trebuie să evidențiem că Republica Moldova este evaluată și în ceea ce privește maturitatea în domeniul securității cibernetice prin intermediul Indicelui Național de Securitate Cibernetică (NCSI)[6]. Acesta este un indice global în timp real, care măsoară gradul de pregătire a țărilor pentru a preveni amenințările cibernetice și a gestiona incidentele cibernetice. NCSI este, de asemenea, o bază de date cu materiale de evidență disponibile publicului și un instrument pentru consolidarea capacităților naționale în domeniul securității cibernetice.

[6] https://ncsi.ega.ee/

În figura de mai jos (Fig. 5.) este reflectată poziția Republicii Moldova și principalii indicatori care reflectă maturitatea țării în materie de securitate cibernetică. Potrivit NCSI, există restanțe semnificative în ceea ce privește protecția infrastructurilor critice (care constituie 25%), răspunsul la incidente cibernetice și asigurarea apărării cibernetice (ambii indicatori situându-se sub 40%)[7].

Fig. 5. Gradul de maturitate a Republicii Moldova în domeniul securității cibernetice conform NCSI



Astfel, la data de 16 martie 2023, Parlamentul a adoptat Legea nr. 48/2023 privind securitatea cibernetică, care urmează să intre 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 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[8] și, implicit, a unor elemente esențiale ale Directivei NIS1[9].

[7] https://ncsi.ega.ee/country/md/

[8] ***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;

[9] ***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;

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.

Potrivit prevederilor Legii privind securitatea cibernetică, Guvernul este învestit cu competență de intervenție, de diferită natură (normativă, organizatorică și tehnică), pe un șir de chestiuni în vederea punerii în aplicare a prevederilor acesteia, dintre care în mod special ținem să le evidențiem pe cele care sunt pertinente obiectului de reglementare a proiectului propus spre avizare și anume punerea în aplicare a cadrului legal primar în ce privește obligațiile de asigurare a securității cibernetice de către persoanele juridice de drept public și 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 cu impact semnificativ.

Cadrul de politici de securitate cibernetică este oferit de un set de documente de politici publice adoptate de Parlament sau Guvern și care oferă viziunea strategică pentru țară cu privire la modul de înființare, consolidare și asigurare a rezilienței sistemului de securitate cibernetică pentru spațiul informațional al Republicii Moldova.

Din perspectiva **cadrului strategic** următoarele documente de politici cuprind obiective ce condiționează intervenția statului:

Concepția securității informaționale[10], aprobată prin Legea nr. 299/2017

Concepția reprezintă o viziune de ansamblu asupra scopului, obiectivelor, principiilor și direcțiilor de bază ale activității de asigurare a unui nivel înalt al securității informaționale a Republicii Moldova, securitatea informațională fiind parte componentă a sistemului național de securitate. Potrivit acestei concepții măsurile de prevenire, depistare și contracarare a amenințărilor complexe și persistente la adresa securității informaționale pot fi întreprinse doar cu condiția existenței și funcționării unui cadru normativ corespunzător în domeniu, a unor instrumente și metode bine definite, a unor mecanisme de colaborare la nivel național și internațional. Concepția

[10] https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro

securității informaționale a Republicii Moldova este determinată de necesitatea protejării intereselor statului, ale societății și ale persoanei, a obiectivelor vitale și de importanță strategică pentru securitatea națională, de necesitatea asigurării protecției informației atribuite la secret de stat, precum și de necesitatea prevenirii și combaterii criminalității informatice.

Concepția constituie baza pentru elaborarea Strategiei securității informaționale a Republicii Moldova și a Planului de acțiuni pentru implementarea strategiei respective. În primul capitol Concepția descrie situația în domeniu și definește problemele din acest sector, stabilește obiectivele de bază, amenințările la adresa securității informaționale, realizarea cărora are ca scop asigurarea protecției, în spațiul informațional, a drepturilor și libertăților fundamentale, a democrației și a statului de drept. În partea a doua Concepția descrie instrumentele și căile de soluționare a problemelor identificate, inclusiv direcțiile strategice și tactice de asigurare a securității informaționale, principiile și principalele sarcini ale autorităților competente, metodele de asigurare a securității informaționale (juridice, tehnico-organizatorice, economice, contrainformative și de securitate), cooperarea internațională în acest domeniu și organizarea sistemului de asigurare a securității informaționale. În ce privește aspectul organizării sistemului respectiv, concepția desemnează Serviciul de Informații și Securitate ca fiind, în limitele competenței atribuite prin lege, autoritatea națională de coordonare a activității autorităților publice desfășurate în domeniul securității informaționale.

Strategia securității informaționale[11] a Republicii Moldova pentru anii 2019-2024 și Planul de acțiuni pentru implementarea acesteia, aprobate prin Hotărârea Parlamentului nr. 257/2018

După cum s-a menționat mai sus, Concepția securității informaționale reprezintă documentul de bază pentru elaborarea acestei Strategii și documentul de politici ce integrează domeniile centrale și asociate spațiului informațional, ce oferă noțiuni, definește principiile de organizare la nivel de stat, societate și persoană, precum și detaliază metodele juridice, tehnico-organizatorice, economice și contrainformative pentru asigurarea securității informaționale a Republicii Moldova. În acest context, **scopul principal** al Strategiei de securitate informațională este de a lega și integra din punct de vedere juridic domeniile prioritare cu responsabilități și competențe de asigurare a securității informațiilor la nivel național, bazată inclusiv pe reziliența cibernetică. Scopul și obiectivele acestei Strategii se realizează în baza Planului de acțiuni pentru implementarea acesteia. Astfel, în contextul definirii problemelor și al descrierii situației la momentul adoptării strategiei, acest document evidențiază un spectru larg de probleme cu care se confruntă până acum Republica Moldova. Problemele abordate de Strategie se referă la cinci componente de bază ale securității cibernetice și investigației criminalității cibernetice, securitatea spațiului media, componenta de contrainformații și securitate, aspectele juridice și, în final, problemele de conștientizare a maselor. Dintre acestea, Strategia evidențiază problemele cele mai proeminente cum ar fi lipsa unui CERT național (Centrul de răspuns la incidente de securitate cibernetică), responsabil de prevenirea și răspunsul la incidente din domeniul securității cibernetice la scară largă la nivel național, lipsa unui sistem integrat de management al securității cibernetice și un mecanism viabil de audit al securității cibernetice, precum și lipsa de specialiști calificați, programe de formare specializată adresate angajaților organelor de drept, dotarea insuficientă cu echipamente și software, finanțare redusă pentru participarea specialiștilor la proiecte internaționale și evenimente pentru consolidarea capacităților și schimbul de bune practici etc. Strategia include mai multe cerințe fundamentale pentru a obține o

[11] https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro

mai bună guvernare a securității cibernetice la nivel național, precum și o listă de acțiuni propuse și indicatori de progres.

Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030, aprobată prin Hotărârea Guvernului nr. 650/2023[12]

Unul dintre obiectivele Strategiei de transformare digitală 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. Astfel, 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.

Diverse aspecte ale securității cibernetice sunt abordate și în Strategia securității naționale a Republicii Moldova, aprobată prin Hotărârea Parlamentului nr. 391/2023[13].

Din perspectiva cadrului normativ privind măsurile de securitate a rețelelor și sistemelor informatice, ***Legea nr. 48/2023 privind securitatea cibernetică*** reprezintă cadrul normativ general primar în domeniul securității cibernetice. Implementarea cerințelor, măsurilor și mecanismelor instituite în această lege are ca obiectiv să garanteze un nivel înalt de securitate a rețelelor și sistemelor informatice din Republica Moldova, oferind protecție pentru interesele vitale ale persoanelor fizice și juridice, ale societății și ale statului, precum și ale intereselor naționale ale Republicii Moldova.

Pentru punerea în aplicare a acestei legi au fost adoptate deja un set de acte normative după cum urmează:

Legea nr.58/2024 pentru modificarea unor acte normative, care are ca obiectiv aducerea în concordanță a cadrului normativ primar cu Legea nr. 48/2023;

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.

Legea nr. 467/2003[14] cu privire la informatizare si resursele informaționale de stat (art.23) și **Legea nr. 71/2007[15] cu privire la registre** (art.24) reglementează, pe de o parte, responsabilitățile autorităților publice în asigurarea securității cibernetice a sistemelor și resurselor informaționale ale statului, iar pe de altă parte, responsabilitățile entităților, inclusiv private, în protecția informațiilor conținute de resursele și prelucrate de sistemele informaționale pe care le creează.

În același timp, cerințele de securitate pentru rețelele publice de comunicații electronice și serviciile de comunicații electronice accesibile publicului sunt prevăzute în ***Legea comunicațiilor electronice nr. 241/2007***[16]. Această lege reglementează activitatea în domeniul comunicațiilor electronice civile a tuturor furnizorilor de rețele sau servicii de comunicații electronice, fie din sectorul public sau privat, și stabilește drepturile și obligațiile utilizatorilor. Legea nu se extinde la rețelele de comunicații speciale. Din punct de vedere al securității rețelelor și serviciilor de comunicații electronice, Agenția Națională pentru Reglementare în Comunicațiile Electronice și

[12] https://www.legis.md/cautare/getResults?doc_id=139408&lang=ro
[13] https://www.legis.md/cautare/getResults?doc_id=141253&lang=ro
[14] https://www.legis.md/cautare/getResults?doc_id=132933&lang=ro
[15] https://www.legis.md/cautare/getResults?doc_id=131038&lang=ro
[16] https://www.legis.md/cautare/getResults?doc_id=133262&lang=ro

Tehnologia Informației este responsabilă de verificarea conformității din perspectiva autorizării a modului de implementare a măsurilor minime de securitate.

De asemenea, **Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate** are ca scop să faciliteze și să eficientizeze schimbul de date și interoperabilitatea în cadrul sectorului public, precum și între sectorul public și cel privat, în vederea creșterii calității serviciilor publice prestate, a creării noilor servicii publice electronice și a asigurării securității informaționale.

Pentru punerea în aplicare a acestor legi, Guvernul a aprobat:

– **Hotărârea Guvernului nr. 201/2017**[17] privind aprobarea cerințelor minime obligatorii de securitate cibernetică, care se adresează atât autorităților guvernamentale, cât și autorităților care nu intră în structura administrativă a Guvernului;

– **Hotărârea Guvernului nr. 482/2020**[18] privind aprobarea măsurilor necesare asigurării securității cibernetice la nivel guvernamental, care completează, în special, cu măsuri organizatorice decizia sus-menționată, dar numai pentru autoritățile și instituțiile publice care fac parte din structura administrativă guvernamentală;

– **Hotărârea Guvernului nr. 388/2022** [19] privind aprobarea Concepției Sistemului Informațional „Registrul de Stat al Incidentelor de Securitate Cibernetică", care este una dintre măsurile preliminare pentru stabilirea unei platforme informaționale pentru comunicarea strategică cu entitățile publice, precum și pentru asigurarea evidenței amenințărilor, vulnerabilităților în spațiul cibernetic și a incidentelor de securitate cibernetică identificate sau raportate.

Cercul de subiecți interesați în intervenția propusă poate fi grupat în următoarele categorii:

1. ***Guvernul și autoritatea 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 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.

Prezentul proiect de hotărâre de Guvern este parte indispensabilă a setului de acte care stau la soluționarea problemei definite la pct. 1 a) din prezenta analiză de impact. Astfel, problematica enunțată și descrisă în subcompartimentele anterioare, rezumată la reziliența cibernetică scăzută a actorilor esențiali, perturbarea activității cărora ar putea prejudicia considerabil viața economică și socială caracterizată în mod special printr-un nivel insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor la securitatea rețelelor și a sistemelor informatice ale acestora are la bază o serie de **cauze**, principalele dintre care constau în următoarele:

1. lipsa unui cadru normativ complet, de gestionare a crizelor la nivel național, inclusiv în caz de incidente cibernetice de mare amploare sau care ar putea sau au impact semnificativ asupra sectoarelor critice sau societății;

[17] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro
[18] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro
[19] https://www.legis.md/cautare/getResults?doc_id=132011&lang=ro

2. măsuri implementate insuficiente de securitate a rețelelor și sistemelor informatice sau chiar lipsa acestora, ale unor actori din sectorul privat, a căror activitate poate fi calificată ca fiind esențială în prestarea unor servicii;

3. schimbul insuficient de informații cu privire la incidente, riscuri și amenințări de securitate cibernetică în ambele sectoare, public și privat, și lipsa unei platforme digitale pentru schimbul de informații fiabile privind amenințările, riscurile și incidentele de securitate, conform prevederilor Legii nr. 48/2023 privind securitatea cibernetică. Majoritatea breșelor de securitate nu sunt raportate și trec neobservate, în principal din cauza reticenței companiilor de a împărtăși aceste informații, de teama daunelor aduse reputației sau a răspunderii. De cele mai multe ori, persoanele responsabile de securitatea rețelelor și a sistemelor informatice împărtășesc informațiile relevante doar cu grupuri mici pe care le consideră de încredere, mai degrabă decât să treacă prin canalele oficiale.

4. există în prezent un cadru instituțional, procedural și normativ-juridic incomplet pentru schimbul de informații de încredere privind amenințările, riscurile și incidentele de securitate între sectorul public și cel privat.

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 obiectivul 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, ținem să evidențiem următoarele:

– instituirea unei abordări uniforme în gestionarea riscurilor în materie de securitate cibernetică prin elaborarea și adoptarea unui set unic de norme și proceduri aplicabile tuturor entităților vizate de prezenta hotărâre de Guvern;

– reglementarea unor chestiuni generale privind procesul de notificare a incidentelor cibernetice cu impact semnificativ de către furnizorii de servicii către Agenția pentru Securitate Cibernetică

– stabilirea unei bazei juridice clare pentru determinarea sincronizată a impactului semnificativ al unor incidente cibernetice, cu accent pe unele tipuri de furnizori din cadrul sectorului infrastructurii digitale, gestionarea serviciilor TIC și cel al furnizorilor digitali;

– clarificarea și aplicarea principiului proporționalității în implementarea măsurilor de securitate cibernetică prin dezvoltarea unui cadru metodologic care să asigure corelarea măsurilor respective cu riscurile identificate, precum și echivalența dintre legislația sectorială și cea privind securitatea cibernetică.

Proiectul de act normativ propus spre examinare are ca **obiect de reglementare**:

a) cerințele privind măsurile de gestionare a riscurilor la adresa securității rețelelor și sistemelor informatice pe care le utilizează furnizorii de servicii la prestarea serviciilor esențiale;

b) aspecte generale privind procedura de notificare a incidentelor cibernetice cu impact semnificativ, precum și condiții specifice pentru unele tipuri de furnizori de servicii în care un incident cibernetic urmează a fi calificat ca fiind semnificativ;

c) modul de evaluare a echivalenței efectelor legislației sectoriale în raport cu cele ale Legii nr. 48/2023 privind securitatea cibernetică, prevăzut în art. 3 alineatele (5) și (6) din Legea nr.48/2023 privind securitatea cibernetică.

Art. 23 alin. (2) lit. c) din Legea nr. 48/2023 stabilește în sarcina Guvernului obligația de a asigura elaborarea și adoptarea actelor normative necesare punerii în aplicare a prevederilor acestei legi. Articolul 11 din legea respectivă prevede obligațiile furnizorilor de servicii în contextul asigurării securității cibernetice prin implementarea măsurilor de securitate ale rețelelor și sistemelor informatice pe care le utilizează la prestarea serviciilor esențiale, adecvate și proporționale riscurilor identificate și evaluate. Alineatul (2) din același articol la pct. 2 enumeră tematicile care trebuie abordate atunci când furnizorul de servicii își evaluează riscurile și implementează astfel de măsuri. Tematicile respective sunt preluate din art. 21 alin. (2) din Directiva NIS2 în contextul armonizării legislației naționale la cea a UE. În temeiul alin. (5) din art. 21 al Directivei NIS2 Comisia Europeană a fost împuternicită să adopte un act de punere în aplicare în ce privește cerințe de gestionare a riscurilor în materie de securitate cibernetică pentru furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere. În consecință Comisia a adoptat Regulamentul de punere în aplicare (UE) 2024/2690. Analiza prevederilor Regulamentului respectiv, efectuată de către experți internaționali și naționali a relevat pertinența și concludența aplicării prevederilor acestuia în raport cu toate persoanele juridice care vor fi identificate de către Agenția pentru Securitate Cibernetică în calitate de furnizori de servicii în sensul Legii nr. 48/2023. În consecință **domeniul de aplicare al proiectului** propus spre examinare se extinde asupra tuturor furnizorilor de servicii, esențiali sau importanți, care vor fi identificați de Agenția pentru Securitate Cibernetică în conformitate cu prevederile Hotărârii Guvernului nr. 860/2024. Totuși, trebuie relevat faptul că această extindere nu este una arbitrară, ci este susținută de reglementări privind aplicarea principiului proporționalității, inclusiv a unei marje discreționare motivate și limitate a furnizorului de servicii în aplicarea măsurilor respective, precum și de reglementări de punere în aplicare treptată a prevederilor acestui act normativ, prevăzute de partea dispozitivă a proiectului de hotărâre a Guvernului.

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, termenul de implementare a cerințelor privind măsurile de gestionare a riscurilor în materie de securitate cibernetică de către furnizorii de servicii și sarcini pentru Agenția pentru Securitate Cibernetică. Termenul de implementare este diferit pentru cele două categorii de furnizori de servicii: pentru cei esențiali – 12 luni, iar pentru cei importanți 18 de luni din data intrării în vigoare a hotărârii. Intrarea în vigoare urmând să aibă loc în baza regulii generale, stabilită de art. 56 alin. (1) din Legea nr. 100/2017 privind actele normative, adică la o lună din data publicării. În partea dispozitivă a proiectului de act normativ, de asemenea sunt stabilite un set de sarcini atât furnizorilor de servicii, cât și Agenției orientate spre inițierea primei iterații de evaluare a maturității furnizorilor de servicii și determinarea inconsistențelor, implementarea îmbunătățirilor, în baza recomandărilor evaluatorilor, inclusiv ale Agenției pentru Securitate Cibernetică.

În anexă este dat Regulamentul cu privire la modul de aplicare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice. Acesta include trei capitole și o anexă.

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 și cercul de subiecți care cad sub incidența prevederilor actului normativ.

Capitolul II „Modul de aplicare a cerințelor privind măsurile de securitate a rețelelor și sistemelor informatice a furnizorilor de servicii în sectoarele critice” stabilește reglementări ale unor aspecte generale privind implementarea cerințelor privind măsurile de securitate stabilite în anexa la proiectul de Regulament. În mod specific este acordată o marjă discreționară largă furnizorilor de servicii în utilizarea standardelor naționale și internaționale, atunci când un nivel de detaliere mai înaltă este necesar pentru implementarea adecvată a anumitor cerințe. De asemenea Agenția pentru Securitate Cibernetică urmează să vină cu orientări metodologice și explicații furnizorilor de servicii atunci când aceștia au nevoie în procesul de aplicare a cerințelor respective, inclusiv în ce privește aplicarea principiului proporționalității. De asemenea, în acest capitol este reglementat și modul de aplicare a principiului proporționalității de către furnizorii de servicii atunci când determină relevanța unei anumite cerințe de securitate pentru tratarea riscurilor identificate și condițiile când cerința aplicată este considerată ca fiind proporțională (dacă este adecvată, dacă este aplicabilă și în măsura în care este fezabilă.) Atunci când identifică și prioritizează măsurile adecvate pentru abordarea riscurilor, furnizorii de servicii trebuie să ia în considerare rezultatele evaluării riscurilor, eficacitatea măsurilor și costul punerii în aplicare în raport cu beneficiile preconizate. Dacă un furnizor de servicii consideră că nu este adecvat, nu este aplicabil sau nu este fezabil ca acesta să aplice anumite cerințe din anexa la proiectul regulamentului, furnizorul respectiv de servicii trebuie să motiveze documentat această neaplicare. În context trebuie menționat că acest principiu al proporționalității va constitui și un instrument pentru Agenția pentru Securitate Cibernetică atunci când își exercită atribuțiile de supraveghere. Aceasta va trebui să țină cont de raționamentele de neaplicare ale furnizorului de servicii și de timpul rezonabil care este necesar pentru punerea în aplicare a unei anumite cerințe.

Acest capitol cuprinde și reglementări care stabilesc în sarcina furnizorilor de servicii efectuarea, o dată la 3 ani, a unor audituri externe de securitate cibernetică în vederea determinării nivelului de conformitate cu cerințele privind măsurile de securitate a rețelelor și sistemelor informatice. Totodată, în acest capitol este propusă o prevedere care exonerează furnizorii de servicii, care sunt conformi cu standardul național de securitate a informației și cele internaționale corespunzătoare, de la aplicarea cerințelor de securitate stabilite de proiect. Totuși aceasta nu exclude competența Agenției de a verifica conformitate cu aceste cerințe în totalitate sau în parte în contextul exercitării de către aceasta a funcției de supraveghere și control de stat.

Capitolul III „Modul de evaluare a echivalenței efectelor obligațiilor de asigurare a securității cibernetice” din proiectul Regulamentului cuprinde prevederi care stabilesc condițiile privind dispozițiile minime pe care trebuie să le includă legislația sectorială din punctul de vedere al reglementării aspectelor ce țin de măsurile de gestionare a riscurilor și obligațiile de raportare a incidentelor cibernetice cu impact semnificativ, în raport cu Legea nr. 48/2023, pentru a fi aplicabilă furnizorilor de servicii în materie de gestionare a riscurilor și raportare a incidentelor. Acest capitol vine cu un set de clarificări necesare atât pentru furnizorii de servicii, cât și pentru Agenția pentru Securitate Cibernetică în procesul de determinare a cerințelor de securitate aplicabile. Reglementările propuse în acest capitol sunt bazate pe Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555 (Directiva NIS 2)[20].

Capitolul IV Procedura de notificare a incidentelor cibernetice cu impact semnificativ din proiectul Regulamentului include prevederi, întemeiate pe art. 12 din Legea nr. 48/2023, și reglementează aspecte generale privind procedura de notificare incidentelor cibernetice cu impact semnificativ, inclusiv, interacțiunea dintre subiecții acestui proces. Este important de menționat că

[20] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918(01)

aspectul general al acestor prevederi este datorat faptului că acestea vor fi completate de prevederi ale actelor interne ale furnizorilor de servicii și ale Agenției pentru Securitate Cibernetică aprobate în legătură cu necesitatea implementării cerințelor privind măsurile de securitate ce vizează gestionarea incidentelor.

În acest capitol este stabilit și conținutul notificărilor privind incidentele cibernetice cu impact semnificativ transmise de către furnizorii de servicii către Agenția pentru Securitate Cibernetică. Astfel raportarea incidentelor semnificative către Agenție urmează a fi realizată în trei etape:

- prin transmiterea unei notificări care să includă în cazul în care există, informații privind suspiciunile că incidentul semnificativ este cauzat de acte ilegale sau răuvoitoare sau dacă există probabilitatea că acest incident ar putea avea un impact transfrontalier;

- printr-o actualizare a notificării incidentului, care să cuprindă o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, precum și, dacă există, a indicatorilor de compromitere. Suplimentar actualizarea notificării incidentului, atunci când există, trebuie să conțină o actualizare a informațiilor transmise în cadrul notificării.

- printr-un raport final care să includă o descriere detaliată a incidentului, inclusiv a gravității și a impactului acestuia; tipul de amenințare sau de cauză principală care este probabil să fi declanșat incidentul; măsurile de atenuare aplicate și în curs de aplicare și, dacă este cazul, o descriere a impactului transfrontalier al incidentului.

Agenția potrivit prevederilor părții dispozitive a proiectului de hotărâre urmează să implementeze, în termen de 6 luni, mecanisme, inclusiv prin utilizarea mijloacelor tehnice, care să asigure un schimb direct, sistematic și imediat de informații în contextul realizării de către furnizorii de servicii a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ. Această sarcină a Agenției decurge din prevederile art. 7 alin. (4) punctele 5) și 7) ale Legii nr. 48/2023, conform cărora Agenția acordă asistență furnizorilor de servicii în procesul de răspuns la incidentele cibernetice, precum și creează platforme de management al incidentelor cibernetice și pentru schimbul de informații. De asemenea, în procesul de implementarea a prevederilor proiectului de act normativ, Agenția trebuie să țină cont și să faciliteze și schimbul voluntar de informații în contextul punerii în aplicare a prevederilor art. 17 din Legea nr. 48/2023.

Prevederile cuprinse de **Capitolul V „Condiții specifice pentru determinarea impactului semnificativ al incidentelor cibernetice pentru unele tipuri de furnizori de servicii”** vizează condiții de determinare a impactului semnificativ al unui incident cibernetic și au ca obiectiv punerea în aplicare a art. 12 alin. (5) din Legea nr. 48/2023, în ce privește furnizorii de servicii DNS, Registratorul național al domeniului de nivel superior .md, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate, furnizorii de piețe online, furnizorii de motoare de căutare online, furnizorii de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere, în vederea clarificării unor aspecte ce vizează modul de determinare a unui incident cibernetic pentru. Astfel, art. 12 alin. (5) din Legea nr. 48/2023 stabilește condițiile când un incident cibernetic se consideră că are un impact semnificativ, și anume atunci când:

a) gravitatea consecințelor incidentului cibernetic este determinată ca fiind cel puțin înaltă în raportul de evaluare a riscurilor de securitate a rețelelor și sistemelor informatice, întocmit în conformitate cu prevederile art.11 alin.(2) pct.1) din lege sau cu cerințele prevăzute de actele aprobate potrivit art.11 alin.(4) din Legea nr. 8/2023;

b) din cauza incidentului cibernetic, prestarea serviciului nu poate fi continuată după expirarea perioadei maxime admise prevăzute în acordul privind nivelul agreat al serviciilor, încheiat în cadrul

relațiilor contractuale ale furnizorului de servicii cu alte persoane, sau prevăzute de cerințele privind continuitatea serviciului stabilite în documentația indicată la art.11 alin.(2) pct.1)–3);

c) continuitatea serviciului altui furnizor de servicii este perturbată de incidentul cibernetic;

d) furnizorului de servicii care notifică incidentul cibernetic, altui furnizor de servicii sau utilizatorilor serviciilor le-au fost cauzate sau le-ar putea fi cauzate prejudicii materiale sau nonmateriale considerabile din cauza incidentului cibernetic.

Punctulv25 din acest capitol asigură transpunerea art. 3 din Regulamentul de punere în aplicare (UE) 2024/2690, prin prisma prevederilor art. 12 alin. (5) lit. d) din Legea nr.48/2023, stabilind cerințe pentru toți furnizorii de servicii în determinarea caracterului considerabil al prejudiciilor materiale și non-materiale la determinarea caracterului semnificativ al unui incident cibernetic. În continuare punctele 26-35 asigură transpunerea prevederilor art. 5-14 din Regulamentul de punere în aplicare (UE) 2024/2690 prin prisma prevederilor art. 12 alin. (5) literele a) și b) din Legea securității cibernetice, stabilind cerințe pentru anumite categorii de furnizori de servicii, atunci când determină caracterul semnificativ al unui incident cibernetic, în ce privește gradul de indisponibilitate a serviciului, gradul de compromitere a integrității, confidențialității sau autenticității informațiilor sau datelor, nivelul de compromitere a accesului fizic sau protecția fizică a unor anumite infrastructuri critice.

În **Anexa la proiectul Regulamentului** sunt prevăzute **Cerințele privind măsurile de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii în sectoarele critice.** Scopul acestor cerințe este să asigure un nivel uniform și suficient de maturitate a furnizorilor de servicii în procesul de asigurare a securității rețelelor și sistemelor informatice pe are aceștia le dețin. Cerințele transpun practic în totalitate prevederile anexei la Regulamentul de punere în aplicare (UE) 2024/2690 cu limitările ce țin de terminologia legislației moldovenești și de extinderea domeniului de aplicare a cerințelor la toți furnizorii de servicii. Problematicile abordate în cele 13 capitole ale anexei se fundamentează pe prevederile art. 11 alin. (2) pct. 2) și vizează:

1. ***Politica privind securitatea rețelelor și a sistemelor informatice*****,** inclusiv rolurile, responsabilitățile și autoritățile în cadrul furnizorului de servicii;
2. ***Politica de gestionare a riscurilor*** la adresa securității rețelelor și sistemelor informatice: cadrul de gestionare a riscurilor; monitorizarea conformității și examinarea independentă a securității informațiilor și rețelelor;
3. ***Gestionarea incidentelor:*** politica de gestionare a incidentelor, monitorizare și jurnalizare a activităților în rețelele și sistemele informatice, raportarea evenimentelor, evaluarea și clasificarea evenimentelor, răspunsul la incidente, analizele post-incident;
4. ***Continuitatea activității și gestionarea crizelor:*** planurile de continuitate a activității și de recuperare în caz de dezastru, gestionarea copiilor de rezervă și a redundanței, procesul de gestionare a crizelor;
5. ***Securitatea lanțului de aprovizionare:*** politica de securitate a lanțului de aprovizionare și registrul furnizorilor și al prestatorilor de servicii direcți ai furnizorului de servicii;
6. ***Securitatea în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice:*** securitatea în achiziționarea de servicii TIC sau de produse TIC; ciclul de viață al dezvoltării securizate; gestionarea configurației; gestionarea modificărilor, reparații și întreținere; testele de securitate; gestionarea corecțiilor de securitate; securitatea rețelelor; segmentarea rețelei; protecția împotriva software-ului rău-intenționat și neautorizat, gestionarea și divulgarea vulnerabilităților;
7. ***Politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor în materie de securitate cibernetică;***

8. ***Practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice:*** sensibilizare și practici de bază în materie de igienă cibernetică; formare în domeniul securității;
9. ***Criptografie:*** politica și procedurile legate de criptografie cu scopul de a asigura utilizarea adecvată și eficace a criptografiei pentru a proteja confidențialitatea, autenticitatea și integritatea datelor în conformitate cu clasificarea activelor;
10. ***Securitatea resurselor umane,*** inclusiv verificarea antecedentelor, procedura în caz de încetare sau modificare a raporturilor de muncă și procesul disciplinar;
11. ***Controlul accesului,*** inclusiv politica de control al accesului, gestionarea drepturilor de acces, conturile privilegiate și conturile de administrare a sistemului, sisteme de administrare, identificarea, autentificarea, inclusiv multifactor,
12. ***Gestionarea activelor*****,** inclusiv clasificarea acestora, politica privind suporturile amovibile, inventarul activelor;
13. ***Securitatea mediului și fizică,*** inclusiv utilități de sprijin, protecția împotriva amenințărilor fizice și de mediu, controlul perimetrului și al accesului fizic.

Astfel, art. 11 alin. (1) din Legea nr. 48/2023 stabilește că aceste cerințe ale măsurilor de securitate urmează a fi implementate în mod continuu de către furnizorii de servicii în scopul prevenirii incidentelor cibernetice, soluționării incidentelor cibernetice, prevenirii și atenuării impactului asupra continuității serviciului ori asupra securității rețelei și/sau sistemului informatic, cauzat de un incident cibernetic, precum și prevenirii și atenuării impactului potențial asupra continuității serviciilor ori asupra securității rețelelor și sistemelor informatice dependente de cele ale furnizorului de servicii. Abordarea bazată pe risc reflectată de alineatul (2) al aceluiași articol impune furnizorilor de servicii să efectueze și să documenteze o evaluare a riscurilor de securitate a rețelelor și sistemelor informatice și să descrie măsurile pentru soluționarea unui potențial incident cibernetic, precum și să implementeze măsuri de securitate corespunzătoare și proporționale pentru a gestiona riscurile de securitate a rețelelor și a sistemelor informatice.

Din punctul de vedere al elementelor noi care vor fi introduse în legislația națională prin adoptarea proiectului respectiv de act normativ relevăm în mod special unificarea într-un singur act a reglementărilor privind gestionarea riscurilor în materie de securitatea cibernetică atât sub aspectul relației domeniul public - domeniul privat, cât și din perspectiva sectoarelor critice în care sunt prestate servicii esențiale pentru funcționarea activităților societale și economice critice. Cu toate acestea, această unificare este una care decurge din necesitatea asigurării punerii în aplicare a prevederilor Legii nr. 48/2023, măsurile de securitate în sine nefiind un element de o noutate absolută pentru o bună parte a potențialilor furnizori de servicii. Spre exemplu, majoritatea cerințelor din anexa la proiectul Regulamentului sunt deja obiectul reglementării Hotărârii Guvernului nr. 201/2017, care are ca subiecți toate personale juridice de drept public cu competență la nivel național. De asemenea, unor categorii distincte de furnizori de servicii, cum sunt, spre exemplu, furnizorii de rețele publice de comunicații electronice și/sau de servicii de comunicații electronice accesibile publicului, le sunt în prezent aplicabile cerințe, într-o anumită măsură similare, prin Hotărârea ANRCETI nr. 60/2019 pentru aprobarea Modalității de implementare a măsurilor minime de securitate și integritate a rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului.

Totodată, propunerea privind modificarea Hotărârii Guvernului 860/2024 cu privire la identificarea furnizorilor de servicii derivă în general din necesitatea eficientizării procesului de identificare a furnizorilor de servicii , precum și din cea de protejare a siguranței publice prin

restricționarea accesului la actele administrative emise de către Agenția pentru Securitate Cibernetică în raport cu furnizorii de servicii.

Astfel, în particular, se propune completarea Anexei 1 cu un punct nou ce urmează să restricționeze accesul la notificarea prealabilă și la actul administrativ emis de către Agenție în cadrul procedurii administrative cu potențialii furnizori de servicii pentru a nu prejudicia procedura administrativă și nemijlocit siguranța națională.

În altă ordine de idei, modificarea anexei 3 la Hotărârea Guvernului nr. 860/2024 este necesară deoarece, în urma aplicării acesteia, s-a constatat că formularea actuală a punctului 10 din anexa 3 permite interpretări duale, generând dificultăți în întocmirea Listei furnizorilor de servicii care este esențială în contextul asigurării securității cibernetice a furnizorilor de servicii esențiali și importanți. Mai mult, includerea listei la informație atribuită la secret de stat creează blocaje în activitatea Agenției, din perspectiva identificării și urmării amenințărilor și vulnerabilităților cibernetice asupra entităților esențiale și importante. Totodată, atribuirea la secret de stat a listei este lipsită de sens deoarece această listă poate fi dedusă din criteriile ce sunt stabilite de către Guvern care sunt stipulate într-un act normativ public.

Pentru a evita blocajele de întocmire și menținere a listei, se propune revizuirea punctului 10, oferindu-i o formulare mai clară. Conform articolului 34 din Constituție, dreptul la informație de interes public nu poate fi îngrădit, însă acesta trebuie să fie exercitat fără a compromite siguranța națională sau protecția cetățenilor.

Totodată, având în vedere caracterul sensibil al listei furnizorilor de servicii, aceasta nu poate fi pusă la dispoziția publicului fără restricții. Se propune, așadar, ca accesul la listă să fie limitat, iar modul de gestionare și utilizare a acestor informații să fie stabilit prin Ordinul Directorului Agenției pentru Securitate Cibernetică.

Această modificare este în concordanță cu practicile europene, unde, deși accesul la astfel de liste este restricționat, acestea nu sunt clasificate drept secret de stat. Regimuri similare se regăsesc în Germania, Belgia, Estonia, Spania și alte state europene.

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

Determinarea unei valori absolute a **impactului financiar asupra mediului de afaceri** nu poate fi determinată în prealabil. Numărul mare de indicatori necunoscuți sau variabili nu permite o evaluare a distribuției costurilor de securitate cibernetică. Dintre acești indicatori ar putea fi relevați cel puțin următorii: starea actuală de securitate a fiecărei organizații în parte; numărul exact de furnizori de servicii care vor cădea sub incidența prevederilor Legii nr. 48/2023 și implicit a obligațiilor privind implementarea măsurilor de securitate a rețelelor și sistemelor lor informatice; variabilitatea mare a domeniului de aplicare a măsurilor de securitate cibernetică, care poate fi foarte diferit de la o organizație la alta, inclusiv în funcție de tipul acesteia, dimensiunea acestea, sectorul și subsectorul în care activează; ponderea cheltuielilor destinate asigurării securității cibernetice în totalul cheltuielilor destinate dezvoltării tehnologiei informației și comunicațiilor în cadrul

organizației; variabilitatea costurilor în timp legată de aspecte macroeconomice și de evoluția tehnologiei, etc.

Totuși unele puncte de referință sunt oferite de studiile și rapoartele realizate la nivel european și internațional care permit având anumite date la nivel național determinarea estimativă a impactului financiar asupra mediului de afaceri. Astfel, potrivit Raportului [21] de evaluare a impactului la propunerea de Directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de abrogare a Directivei (UE) 2016/1148 (Directiva NIS2): „Pe baza previziunilor periodice ale Gartner din 2012 până în 2020 privind procentajul cheltuielilor globale cu securitatea TIC din cheltuielile TIC și din veniturile totale, precum și ținând seama de cele mai recente date sectoriale ale Gartner disponibile Comisiei, în scopul evaluării impactului s-a presupus că media cheltuielilor pentru securitatea TIC pe sector în 2020 este de aproximativ **9,14%** din cheltuielile totale TIC. În funcție de nivelul de maturitate și de capacitățile de securitate cibernetică ale sectorului, precum și de nivelul de digitalizare, această medie ar putea fi ajustată cu +/-3%. În plus, cheltuielile medii TIC pe sector sunt estimate la aproximativ **5,69% din cifra de afaceri** totală și, prin urmare, cheltuielile medii cu securitatea TIC din cifra de afaceri totală pe sector în 2020 sunt estimate la **aprox. 0.52%**.„

Cu toate acestea aceste estimări au fost considerate ca fiind destul de prudente. „Un studiu privind investițiile NIS comandat de ENISA și realizat de Gartner indică un nivel mai scăzut al cheltuielilor pentru securitatea TIC în Europa, de aproximativ 6 % din bugetul TIC începând cu 2016, organizațiile din sectorul bancar, al serviciilor financiare și al produselor farmaceutice având un raport mai mare de 5 %, în timp ce sectoare precum transporturile, educația și comerțul cu amănuntul ar avea cele mai mici astfel de raporturi, sub 2,5 %."

Din perspectiva rezultatelor celor două analize efectuate de către Comisia Europeană și ENISA, odată cu finalizarea procesului de identificare a furnizorilor de servicii de către Agenția pentru Securitate Cibernetică conform Hotărârii Guvernului nr. 860/2024 „Cu privire la identificarea furnizorilor de servicii", va fi cunoscută lista furnizorilor de servicii și fiecare caz aparte, cunoscând cifra de afaceri al acestor entități prin aplicarea procentului de 0,52% va fi posibil de determinat costurile aproximative ale implementării măsurilor de securitate. Cu toate aceste, chiar și valorile respective vor fi destul de aproximative nefiind cunoscut nivelul actual de maturitate al fiecărui furnizori în parte.

Suplimentar considerăm relevant să menționăm că în 2024 ENISA a produs cel de-al cincilea Raport privind investițiile în securitatea rețelelor și informațiilor (NIS Investments 2024Report)[22] oferind un set de concluzii relevante pentru estimarea globală a impactului asupra sectorului privat, bazate pe procesare datelor de la „1 350 de organizații din toate cele 27 de state membre ale UE, acoperind toate sectoarele NIS 2 de mare importanță, precum și sectorul de producție". Raportul oferă o „perspectivă asupra pregătirii entităților de a se conforma noilor cerințe, precum și asupra provocărilor cu care se confruntă acestea". Principalele concluzii relevante ale raportului care pot oferi furnizorilor de servicii o suficientă bază pentru a-și estima costurile de implementare sunt următoarele:

„a) Organizațiile alocă 9,0% din investițiile lor IT pentru securitatea informațiilor, o creștere semnificativă de 1,9 puncte procentuale față de anul trecut.

b) Organizațiile alocă 11,1 % din ENI (echivalent normă întreagă) pentru securitatea informațiilor, ceea ce reprezintă o scădere de 0,8 % față de anul trecut, în ciuda creșterii generale a

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020SC0345, pag. 71

[22] https://www.enisa.europa.eu/publications/nis-investments-2024

cheltuielilor cu securitatea cibernetică și al patrulea an consecutiv în care se observă o scădere a acestui indicator.

c) 89% dintre organizații vor avea nevoie de mai mult personal în domeniul securității cibernetice pentru a se conforma NIS 2, în special în domeniile arhitecturii și ingineriei securității cibernetice (46%) și operațiunilor de securitate cibernetică (40%).

d) Organizațiile vor avea nevoie, de asemenea, de ENI suplimentare pentru a se conforma altor acte legislative orizontale (CRA - 85%) sau verticale (DORA - 84%; NCCS - 81%) privind securitatea cibernetică.

e) Majoritatea organizațiilor anticipează o creștere punctuală sau permanentă a bugetelor de securitate cibernetică pentru conformitatea cu NIS 2, deși un număr substanțial de entități nu vor putea solicita bugetul suplimentar necesar, un procent care este deosebit de ridicat pentru IMM-uri (34%)...".

De asemenea, din perspectiva impactului financiar asupra sectorului privat trebuie să relevăm și informațiile aduse în analiza de impact la proiectul de Lege privind securitatea cibernetică la orientările pe această dimensiune oferite de Comisia Europeană în procesul de evaluare a costurilor de conformare pentru mediul privat în procesul de pregătire a propunerii de Directivă NIS1: „Pornind de la costurile totale de conformare pentru sectorul privat, care variază între 360 și 720 de milioane de euro, costul de conformare pentru fiecare întreprindere mică și mijlocie s-ar situa între 2 500 și 5 000 de euro. La efectuarea calculului, s-a presupus că întreprinderile mici și mijlocii reprezintă 20% din cifra de afaceri a întreprinderilor private vizate de regulament și reprezintă 68% din toate întreprinderile afectate, adică puțin peste 28 000 de întreprinderi. Acesta este costul mediu estimat pentru fiecare IMM pentru atingerea nivelului actual de "cel mai bun din clasă" în ceea ce privește protecția NIS. Pe măsură ce tehnologiile evoluează, riscurile, pe de o parte, și măsurile de protecție, pe de altă parte, vor continua să evolueze și ele. Astfel, vor fi necesare investiții continue pentru a ține pasul cu stadiul actual al tehnologiei, dar este foarte dificil, în acest stadiu, să se prevadă care vor fi costurile pe care le implică menținerea pasului cu evoluțiile tehnologice. Cu toate acestea, aceste investiții vor garanta că atât întreprinderile mari și mici, cât și economia europeană vor fi bine poziționate pentru a profita de avantajele pieței globale a securității cibernetice, care, potrivit estimărilor, se va număra printre segmentele cu cea mai rapidă creștere din sectorul tehnologiei informației (IT) în următorii 3-5 ani; în 2011, piața securității cibernetice valora 63,7 miliarde de dolari și se preconizează că va crește între 80 și 120,1 miliarde de dolari până în 2017."

În ce privește costurile pentru entitățile administrației publice și furnizorii de servicii asociați cu raportarea obligatorie a unui incident semnificativ, Comisia Europeană a estimat în aceeași analiză de impact următoarele:

„Pentru a evalua costurile de raportare a incidentelor grave din NIS, a fost extrapolată o estimare a notificărilor care ar trebui efectuate pe parcursul unui an, pe baza datelor existente privind punerea în aplicare a articolului 13a din directiva-cadru privind comunicațiile electronice. Pe această bază, numărul de notificări de incidente NIS preconizate s-ar ridica la aproximativ 1 700 pe an. Presupunând că un angajat ar trebui să aloce 0,5 zile lucrătoare pentru notificare și că notificarea ca atare ar avea costuri neglijabile (de exemplu, ar fi efectuată prin intermediul unui e-mail), costul preconizat pentru fiecare notificare de încălcare ar fi de 125 EUR, ceea ce ar duce la un cost total pentru notificarea încălcărilor pe bază anuală de 212 500 EUR la nivelul UE. În ceea ce privește posibilele investigații care pot fi inițiate de către autoritățile competente din NIS cu privire la respectarea obligațiilor de gestionare a riscurilor și de notificare a incidentelor NIS, nu este posibil în acest stadiu să se estimeze dacă și câte investigații ar putea fi inițiate. Cu toate acestea, se poate presupune în mod rezonabil că între 10 și 20% din notificările de incidente NIS ar putea fi urmate

de o investigație, ceea ce corespunde unei valori absolute de 170-340 de investigații preconizate pe an. Ținând cont de costul salarial standard, costul maxim pentru entitatea afectată ar fi de maximum 25 000 EUR pe investigație…".

Cu toate acestea, trebuie remarcat că acestea nu sunt cheltuieli care ar trebui efectuate într-un interval scurt de timp. Având în vedere prevederile punctelor 6 și 7 ale proiectului de Regulament costurile necesare pentru implementarea cerințelor de securitatea pot fi eșalonate de-a lungul anilor, în funcție de prioritizarea activelor critice vizate și de capacitatea financiară a furnizorului de servicii. În plus, trebuie să se țină cont de faptul că punerea în aplicare a măsurilor de securitate nu este un proiect unic cu costuri introductive, ci un proces continuu în cadrul fiecărei entități, având în vedere că multe măsuri de securitate necesită actualizări regulate, monitorizare și îmbunătățire continuă.

Sub aspectul **impactului financiar asupra sectorului public** acesta trebuie examinat din perspectiva a două componente: costurile de implementare ce urmează a fi suportate de către Agenția pentru Securitatea Cibernetică din punctul de vedere al măsurilor de implementare descrise în punctul 9 din prezenta notă și costurile și cheltuielile ce urmează a fi suportate de către furnizorii de servicii – persoane juridice de drept public pentru implementarea cerințelor privind măsurile de gestionare a riscurilor în materie de securitate cibernetică și a celor de raportare a incidentelor cibernetice cu impact semnificativ.

Astfel, în ce privește prima componentă, realizarea de către Agenție a activităților de implementare nu implică cheltuieli suplimentare la cele care sunt deja prevăzute în bugetul de stat. Astfel, în Legea bugetului de stat pentru anul 2025, Ministerului Dezvoltării Economice și Digitalizării în subprogramul bugetar 1504 "Tehnologii informaționale" îi sunt prevăzute cheltuieli în valoare de 20416,5 mii lei. Aceste cheltuieli sunt asociate realizării de către Agenție a competenței sale în ce privește implementarea politicii de stat în domeniul securității cibernetice, inclusiv exercitarea funcției de supraveghere și control al modului în care sunt respectate prevederile cadrului normativ în acest domeniul, oferirea de asistență, inclusiv metodologică furnizorilor de servicii în sectoarele critice în vederea implementării măsurilor de securitate.

În ceea ce privește cea de-a doua componentă costurile de implementare a măsurilor de securitate pentru furnizorii de servicii din sectorul public, relevăm următoarele. În prezent o parte dintre aceste entități publice sunt obligate să implementeze măsurile de securitate stabilite de Hotărârea Guvernului nr. 201/2017 „Cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică", și anume Cancelaria de Stat, ministerele, alte autorități administrative centrale subordonate Guvernului, inclusiv al structurilor organizaționale din sfera lor de competență (autoritățile administrative din subordine, serviciile publice desconcentrate și cele aflate în subordine, instituțiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator), al autorităților administrative autonome și unităților cu autonomie financiară. Se presupune că toate aceste autorități și instituții publice au deja prevăzute anumite mijloace financiare în bugetul de stat pentru realizarea obligațiilor prevăzute de Hotărârea Guvernului nr. 201/2023. Având în vedere că obligațiile impuse de această hotărâre de Guvern și cele propuse în proiectul de hotărâre propus spre examinare nu diferă fundamental sub aspectul conceptului și obiectivelor urmărite prin implementarea măsurilor de securitate, dar și într-o anumită măsură a conținutului acestor măsuri, este de presupus să nu fie necesară o creștere substanțială a cuantumului mijloacelor financiare la cele deja planificate în bugetul de stat pentru asigurarea conformității cu cerințe privind măsurile de gestionare a riscurilor în materie de securitate cibernetică. În principiu, putem conchide că implementarea măsurilor de securitate cibernetică

pentru furnizorii de servicii din sectorul public urmează să se asigure din contul și în limita mijloacelor financiare alocate în legile bugetare anuale.

Cu toate acestea considerăm important de relevat unele aspecte abordate de către Comisia Europeană în Analiza [23] de impact la propunerea de Directivă NIS2. Astfel, *Datele pentru administrația publică se referă la costurile de funcționare. Cheltuielile TIC în sectorul public sunt de obicei exprimate ca procent din cheltuielile de funcționare în loc de venituri sau cifra de afaceri. Conform Eurostat , în 2019, cheltuielile totale la nivelul administrației centrale în UE-27 au fost de 22% din PIB, în timp ce veniturile totale au fost de 21,7% din PIB. La nivelul administrației locale, cheltuielile totale au fost la fel ca veniturile totale: 10,9% din PIB. Studiul privind investițiile NIS indică o* ***medie anuală a cheltuielilor pentru securitatea TIC de 4% din bugetul TIC pentru guvernele din Europa****. În conformitate cu estimările menționate anterior privind o creștere cu 22% a cheltuielilor pentru securitatea TIC în cei 3-4 ani care urmează intrării în vigoare a Directivei NIS revizuite ...., cheltuielile pentru securitatea TIC ale guvernelor ar trebui, prin urmare, să crească la* ***4,88%****...."*

De asemenea, considerăm relevante exercițiului nostru constatările analizei de impact[24] efectuate de către Agenția Republicii Cehe pentru Securitate Cibernetică și Informațională (NUKIB) la proiectul de lege privind securitate cibernetică care transpune prevederile Directivei NIS2. Astfel, Agenția respectivă a efectuat o analiză în baza mai multor studii privind investițiile în securitatea cibernetică ale ENISA, în baza estimărilor anterioare în procesul de transpunere a Directivei NIS1 și a unui sondaj a unui grup de entități selectate. Această analiză *a condus la un calcul orientativ al costurilor pentru implementarea și punerea în aplicare ulterioară a principalelor măsuri de securitate* ***pentru un sistem securizat*** *sub forma unor estimări foarte aproximative, cuprinse între 800 000 CZK și 1 500 000 CZK (aproximativ între* ***30000 și 60000 euro****). Schimbările în abordarea reglementării introduse de directivă, variabilele menționate mai sus (în special starea diferită a securității actuale în organizațiile reglementate), distribuția obligațiilor impuse acestor entități, precum și agregarea unui număr de măsuri de securitate în mai multe sisteme din cadrul unei organizații pot influența aceste valori, dar, având în vedere cele de mai sus, este posibil să se aștepte la cerințe bugetare publice în acest interval aproximativ. Prin urmare, variabila esențială va fi numărul de sisteme individuale pentru fiecare organizație în parte și multiplicarea sumei de mai sus care va trebui alocată organizațiilor în bugetele publice."* În aceeași analiză NUKIB însă constată că rezultatele sondajului *demonstrează că, din perspectiva autorității de reglementare, nu este posibil să se cuantifice impactul asupra bugetelor sub forma unui număr absolut care să fie suficient de precis*.

Și în acest caz evidențiem faptul că acestea nu sunt cheltuieli care ar trebui efectuate într-un interval de un an bugetar. Implementarea cerințelor de securitate și în sectorul public ar putea fi eșalonate de-a lungul mai multor ani, în funcție de prioritizarea activelor critice vizate și de disponibilitatea mijloacelor financiare ale furnizorului de servicii.

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 îmbunătăți securitatea cibernetică prin detectarea și blocarea eficientă a atacurilor, protejând datele și informațiile sensibile și asigurând reacții rapide.

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52020SC0345

[24] https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/

- 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.

- Îmbunătățirea încrederii și reputației: O securitate cibernetică mai puternică va crește încrederea utilizatorilor și clienților în mediul privat și stat, consolidând reputația acestora.

- 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.

- Stimularea inovării și cercetării: Implementarea soluției va impulsiona inovația și cercetarea în domeniul securității cibernetice, contribuind la dezvoltarea economică și colaborarea internațională.

4.4. Impactul social

4.4.1. Impactul asupra datelor cu caracter personal

Din perspectiva datelor cu caracter personal prevederile proiectului de act normativ ar trebui să aibă 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. Iar aceste rețele și sisteme informatice în mare partea, mai ales în cazul furnizorilor de servicii mari, procesează date cu caracter personal.

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

Un nivel mai ridicat de securitate ar îmbunătăți încrederea cetățenilor în mediul on-line, care ar putea profita pe deplin de avantajele lumii digitale, în mod special în ce privește serviciile digitale guvernamentale. Aceste servicii esențiale ar deveni mai atractive datorită fiabilității și disponibilității ridicate. Acest lucru le poate conferi cetățenilor din regiunile rurale sau îndepărtate cu acces limitat la serviciile offline o mai mare încredere. În cele din urmă, este foarte probabil ca această opțiune să stimuleze crearea unui corp de profesioniști în domeniul asigurării securității rețelelor și sistemelor informatice și, implicit al ocupării forței de muncă a personalului din acest domeniu, inclusiv datorită cerințelor de a efectua evaluări ale riscurilor de securitate cibernetică și de a adopta măsuri de securitate adecvate.

5. Compatibilitatea proiectului actului normativ cu legislația UE

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

Proiectul de act normativ propus spre examinare transpune parțial prevederile Regulamentului de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024[25], precum

[25] Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de

și ia în considerare dispozițiile Comunicării[26] Comisiei referitoare la Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555[27] (Directiva NIS 2) 2023/C 328/02.

Obiectivul Regulamentului de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 constă în stabilirea cerințelor tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică, menționate la articolul 21 alineatul (2) din Directiva (UE) 2022/2555, și să precizeze mai în detaliu cazurile în care un incident ar trebui considerat semnificativ, astfel cum se menționează la articolul 23 alineatul (3) din Directiva (UE) 2022/2555.

Domeniul de aplicare al actului juridic european este limitat la *furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere.* Actul UE acoperă două sectoare cu o importanță critică ridicată (anexa nr. 1 la Directiva NIS2): infrastructura digitală *(cu excepția furnizorilor de puncte de schimb de internet (IXP - internet exchange point) și furnizorii de rețele publice de comunicații electronice și/sau de servicii de comunicații electronice accesibile publicului)* și gestionarea serviciilor TIC, și un sector de importanță critică (anexa nr. II la Directiva NIS): sectorul furnizori digitali. Proiectul de act normativ însă extinde domeniul de aplicare al prevederilor transpuse la întregul spectru de subiecți ai Legii nr 48/2023 privind securitatea cibernetică. Această extensie este datorată pe de o parte de necesitatea punerii în aplicare a prevederilor art. 11 din Legea nr. 48/2023 care reglementează obligațiile furnizorilor de servicii în ce privește implementarea măsurilor de securitate a rețelelor și sistemelor informatice pe care le dețin și, pe de altă parte, de faptul că cerințele reglementate de actul UE sunt cerințe minime necesare pentru asigurarea unei reziliențe din punct de vedere cibernetic atât a entităților din sectorul public, cât și a entităților din sectorul privat. În acest sens, trebuie evidențiat faptul că actul UE *„se bazează pe standarde europene și internaționale, cum ar fi ISO/IEC 27001, ISO/IEC 27002 și ETSI EN 319401, precum și pe specificații tehnice, cum ar fi CEN/TS 18026:2024, care sunt relevante pentru securitatea rețelelor și a sistemelor informatice*"[28] relevante pentru toate tipurile de entități care activează în sectoarele critice.

Actul UE a cărui transpunere se urmărește prin adoptarea proiectului de act normativ propus spre examinare este unul recent adoptat și nu a constituit anterior obiect al transpunerii în legislația națională.

Referitor la reglementările similare existente în legislația statelor membre ale Uniunii Europene, a fost efectuată o evaluare a legislației a cinci State membre ale UE: Belgia, Cehia, Estonia, Germania și România.

Toate cadrele de securitate cibernetică ce se folosesc, se referă la sau au fost inspirate de cele mai comune standarde internaționale, cum ar fi cele ale familiei ISO 27000 și NIST. Unele țări au optat să emită un standard național autonom, altele stabilesc măsurile de securitate în reglementări de implementare, în timp ce a treia categorie utilizează încă certificarea internațională ca dovadă a conformității.

servicii de socializare în rețea, precum și prestatorii de servicii de încredere: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R2690

[26] Comunicare a Comisiei Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555 (Directiva NIS 2) 2023/C 328/02: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918(01)

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

[28] Considerentul (3) din preambulul la Regulamentul de punere în aplicare UE) 2024/2690 al Comisiei din 17 octombrie 2024;

În Belgia, decretul regal din 9 iunie 2024 de executare a legii de transpunere a Directivei NIS2 introduce două cadre de referință din care să aleagă entitățile reglementate. În primul rând, certificarea ISO 27001 și, în al doilea rând Cyber Fundamentals (CyFun), cadrul dezvoltat de Centrul național de securitate cibernetică belgian. Acesta din urmă combină patru cadre de securitate cibernetică utilizate în mod obișnuit (NIST, CSF, ISO 27001/ISO 27002, CIS Controls și IEC 62443), împreună cu date anonimizate ale atacurilor cibernetice anterioare. Cadrul belgian oferă trei niveluri de asigurare: de bază, importantă și esențială, completate de nivelul de pornire „mic". Cu toate acestea, metodologia care stă la baza diferențierii măsurilor de securitate între cele trei niveluri nu este evidentă.

România, la rândul ei, aplică standarde și/sau specificații europene și internaționale individual sau grupate în funcție de domeniile, subdomeniile, măsurile și cerințele de securitate, stabilite în conformitate cu regulile tehnice privind cerințele minime pentru asigurarea securității rețelelor și sistemelor informatice. Aceste standarde și/sau specificații europene și internaționale se găsesc în Lista standardelor și specificațiilor europene și internaționale, adoptată de Guvern. Proiectul de Ordonanță de urgență de transpunere a Directivei NIS2 nu precizează nicio cerință și lasă la latitudinea Directoratului Național de Securitate Cibernetică (DSNC) stabilirea oricărei legislații secundare corespunzătoare între 15 și 180 de zile de la data publicării ordonanței în Monitorul Oficial, în funcție de subtema corespunzătoare. În timp ce adoptarea respectivei ordonanțe de urgență va abroga actuala Lege privind securitatea cibernetică, măsurile adoptate sau impuse în temeiul prevederilor dispozițiilor acesteia din urmă privind securitatea rețelelor și sistemelor informatice, auditurilor și certificărilor, precum și a legislației secundare corespunzătoare, rămân în vigoare până la revizuirea acestora, în conformitate cu perioada menționată mai sus de la data publicării ordonanței. În plus, proiectul menționează o listă de standarde și specificații europene și internaționale, supuse elaborării și aprobării de către DNSC.

În Cehia, Legea securității cibernetice face distincție între cerințele de securitate organizațională și cea tehnică și oferă o listă enumerativă a acelor cerințe sau măsuri. Ca urmare a obligației legale de punere în aplicare a măsurilor de securitate, NUKIB emite și este responsabil de actualizarea decretelor care detaliază măsurile de securitate și modalitățile de punere în aplicare și audit a acestora. NUKIB publică în continuare materiale metodice fără caracter obligatoriu care ajută entitățile reglementate să înțeleagă și să pună în aplicare în mod corect cadrul juridic. Cerințele se bazează pe familia ISO 27k și în special pe standardul ISO 27001. În cazul în care legislația sectorială (națională sau a UE) reglementează gestionarea securității și a incidentelor, legea privind securitatea cibernetică recunoaște aceste norme sectoriale ca lex specialis, cu condiția ca acestea să garanteze un nivel de securitate comparabil cu cel al legii privind securitatea cibernetică. În mod obișnuit, o astfel de legislație se găsește în sectoarele energetice, financiare sau de telecomunicații. Legea de transpunere a Directivei NIS2 adoptă aceeași abordare.

Implementarea de către Germania a Directivei NIS și Directivei NIS2 aderă în general la cadrele internaționale de securitate cibernetică și la cele mai bune practici, cum ar fi ISO 27001, dar cu cerințe suplimentare. De exemplu, măsurile trebuie să fie adaptate pentru a aborda riscurile de mediu, amenințările fizice și tehnologiile de ultimă generație. Țara încorporează în continuare cele mai bune practici internaționale și standarde specifice industriei. Astfel, anumite sectoare urmează linii directoare personalizate care reflectă nevoi operaționale unice, cum ar fi catalogul de securitate BNetzA pentru telecomunicații sau cerințele de infrastructură critică conform BSI- KritisV . Acestea sunt personalizate în funcție de riscurile inerente fiecărei industrii. Anumite industrii precum energia, telecomunicațiile și serviciile financiare sunt reglementate prin instrumente juridice suplimentare, cum ar fi Legea industriei energetice (EnWG) și Legea telecomunicațiilor (TKG), care includ

mandate de securitate cibernetică specifice sectorului, aliniate cu Directiva NIS2. Pentru entitățile care nu sunt acoperite de standarde specifice sectorului, legea pune accent pe alinierea la cadrele internaționale mai largi. ISO 27001 este menționat ca fundație, deși este adesea considerat insuficient fără măsuri suplimentare prescrise de Directiva NIS2. Cadrul juridic general oferit de BSIG asigură, prin urmare, o bază de referință, în timp ce industriile specifice aderă la standarde personalizate pentru a aborda riscurile unice. Alegând această abordare hibridă, Germania depune eforturi pentru o acoperire cuprinzătoare a cerințelor de securitate cibernetică în toate sectoarele.

În Estonia, toate entitățile reglementate intră sub supravegherea autorității competente, Autoritatea Estoniană pentru Sisteme Informaționale sau RIA. Drepturile și obligațiile acestei autorități sunt descrise în capitolele 4 și 5 din actul de securitate cibernetică. Prevederile Standardului Estonian de Securitate a Informațiilor sunt de natură generală și se aplică tuturor entităților obligate. Legea nu face diferențe între sectoare (privat vs public sau altfel). Scopul implementării continue a măsurilor de securitate cibernetică este de a permite și de a contribui la prevenirea incidentelor cibernetice, rezolvarea incidentelor cibernetice, prevenirea și atenuarea impactului unui incident asupra continuității unui serviciu sau securității unui sistem sau a altui serviciu dependent sau securitatea unui sistem. Abordarea bazată pe riscuri impune tuturor entităților reglementate să pregătească o evaluare a riscurilor sistemului și să descrie măsurile de soluționare a unui incident cibernetic, să asigure existența și actualitatea unei evaluări documentate a riscurilor sistemului, a reglementărilor de securitate și a descrierii aplicării măsurilor de securitate, să asigure monitorizarea sistemului pentru detectarea acțiunilor sau a programelor informatice care compromit securitatea acestuia și să comunice RIA informații privind acțiunile sau programele informatice care compromit securitatea sistemului, să ia măsuri pentru reducerea impactului și răspândirii unui incident cibernetic, inclusiv restricționarea utilizării sau a accesului la sistem, dacă este necesar.

În conformitate cu prevederile Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene, aprobat prin Hotărârea Guvernului nr. 1171/2018, a fost elaborat tabelul de concordanță care este parte a dosarului de însoțire a proiectului de act normativ.

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, pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md, la data de 25.09.2024 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de hotărâre de Guvern link, - (https://particip.gov.md/ro/document/stages/*/13240).

Anunț privind consultarea publică a proiectului hotărârii de Guvern a fost plasat la data de 04.02.2025, link - (https://particip.gov.md/ro/document/stages/*/13896)

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

Prin proiectul de act normativ se propune abrogarea Hotărârii Guvernului 201/2017 privind cerințele minime obligatorii de securitate cibernetică. Abrogarea este determinată pe de o parte de faptul că toate persoanele juridice de drept public în temeiul art. 3 alin. (2) lit. i) intră în sfera de

aplicare a Legii nr. 48/2023 și cerințele respective le vor fi aplicabile, iar pe de altă parte cerințele prevăzute în Hotărârea Guvernului nr. 201/2017 sunt cuprinse de cerințele propuse în proiect.

În principiu adoptarea și intrarea în vigoare a proiectului nu va necesita modificarea cadrului normativ existent, dat fiind caracterul de lege specială a legislației sectoriale în raport cu legislația privind securitatea cibernetică, inclusiv prevederile proiectului în speță, dacă legislația sectorială stabilește cerințe cel puți echivalente în efecte cu cele ale actelor normative adoptate pentru punerea în aplicare a Legii nr. 48/2023 și lega propriu-zisă.

Deși proiectul nu implică adoptarea unor acte normative noi, totuși trebuie notat că Agenția pentru Securitate Cibernetică urmează să vină cu modele de notificare a incidentelor de către furnizorii de servicii care să le faciliteze raportarea incidentelor cibernetice cu impact semnificativ.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Autoritatea publică principală responsabilă de asigurarea implementării proiectului de act normativ este Agenția pentru Securitate Cibernetică. Potrivit prevederilor art. 7 alin. (3) lit. e), Agenția exercită supravegherea și controlul respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii nr. 48/2023. Modul de exercitarea a acestor funcții ale Agenției urmează a fi reglementat prin-un act normativ separat aprobat de către Guvern în temeiul prevederilor art. 18 alin. (3) și 19 alin (5). Însă proiectul actului normativ propus spre examinare urmează a fi aplicat de către furnizorii de servicii în mod treptat în termen de 3 ani din data publicării. În această perioadă de timp, Agenția urmează:

- să finalizeze operaționalizarea în volum deplin a subdiviziunii responsabile de identificarea, evidența și relaționarea cu furnizorii de servicii în procesul protecției infrastructurii informaționale critice ale acestora și a subdiviziunii responsabile de supraveghere și controlul executării prevederilor legale de către furnizorii de servicii;
- să aprobe ghiduri și orientări metodologice pentru furnizorii de servicii în vederea sprijinirii acestora în implementarea cerințelor privind măsurile de gestionare a riscurilor care ajută furnizorii de servicii să înțeleagă și să pună în aplicare corect cerințele privind măsurile de securitate;
- să acorde suport furnizorilor de servicii prin evaluarea nivelului de maturitate și conformitate a acestora cu cerințele de asigurare a securității cibernetice;
- În baza constatărilor acestor evaluări acordarea suportului entităților în prioritizarea pentru implementare, în mod special în baza principiului proporționalității, a măsurilor de securitate în funcție de capacitatea furnizorilor de servicii, atingerea obiectivelor de reziliență, raportul cost-beneficiu.
- Să stabilească formate și să instituie mecanisme, inclusiv sprijinite de mijloace digitale, pentru a înlesni îndeplinirea de către furnizorii de servicii a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ;
- Să întreprindă alte acțiuni menite să faciliteze schimbul de informații în timp real cu furnizorii de servicii în vederea creșterii nivelului de reziliență a acestora.

Activitatea de evaluare a nivelului de maturitate a furnizorilor de servicii va permite Agenției agregarea unor informații mai detaliate și mai ample și eventual aprobarea unor orientări suplimentare sau modificarea celor inițiale în vedere ajustării. În acest context este necesar de relevat că în acest scop ar putea fi utilizate instrumentele oferite deja de organismele Uniunii Europene, în

mod special de ENISA[29] și de Grupul de cooperare NIS[30] . Spre exemplu, actualmente ENISA este în proces de consultare publică a Ghidului[31] de implementare a Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei, care a fost elaborat în cooperare cu Grupul de cooperare NIS și cu Comisia Europeană. Ghiduri respectiv cuprinde sfaturi orientative și utile privind parametrii care trebuie luați în considerare la punerea în aplicare a unei cerințe sau explicații suplimentare privind conceptele din textul juridic; exemplele de dovezi (tipuri indicative de dovezi care atestă că o cerință tehnică și metodologică este în vigoare) și, în cazul anumitor cerințe, sugestii generale adiționale pentru a fi luate în considerare suplimentar de către entitățile vizate.

Pentru monitorizarea nivelului de implementare a prezentei inițiative normative se stabilesc următori indicatori de performanță:

- Rata de implementare a măsurilor de securitate;
- Numărul de incidente cibernetice raportate;
- Timpul mediu de răspuns la incidente;
- Gradul de conformitate al furnizorilor de servicii cu cerințele de securitate;
- Numărul de furnizori de servicii care au beneficiat de măsuri de consolidare a capacităților în domeniul securității cibernetice;
- Gradul de utilizare a instrumentelor de monitorizare și raportare a incidentelor cibernetice.

Nivelul de implementare și impactul Hotărârii de Guvern vor fi monitorizate și evaluate printr-un sistem structurat, bazat pe informațiile disponibile în cadrul Agenției pentru Securitate Cibernetică și al altor autorități publice, precum și pe datele colectate în procesul de supraveghere și control. Acest proces va fi realizat în conformitate cu prevederile art. 18 și 19 din Legea nr. 48/2023 privind securitatea cibernetică și cu respectarea cadrului normativ primar și secundar aplicabil în domeniul controalelor de stat.

Secretar general

Digitally signed by Voicu Ina
Date: 2025.06.03 18:01:42 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Ina VOICU

[29] https://www.enisa.europa.eu/

[30] https://digital-strategy.ec.europa.eu/ro/policies/nis-cooperation-group

[31] https://www.enisa.europa.eu/publications/implementation-guidance-on-nis-2-security-measures