

LEGE
pentru modificarea unor acte normative
(armonizarea legislației naționale cu Directiva NIS2)

Parlamentul adoptă prezenta lege organică.

Prezenta lege transpune Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr.910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), publicată în Jurnalul Oficial al Uniunii Europene seria L nr.333 din 27 decembrie 2022.

Art. I – Codul Contravențional nr. 218/2008 (Republicat: Monitorul Oficial al Republicii Moldova, 2017, nr.78-84, art.100), cu modificările ulterioare, se modifică după cum urmează:

1. Se completează cu articolele 259³ și 259⁴, cu următorul cuprins:

„Articolul 259³. Încălcarea legislației în domeniul securității cibernetice

(1) Încălcarea cerințelor stabilite de art. 11 alin. (1), (2), (2²), (2³) sau (3) ori de art. 12 alin. (1), (3), (3¹), (4), (6), (7¹), (8) sau (8¹) din Legea nr. 48/2023 privind securitatea cibernetică de către furnizorul esențial de servicii,

se sancționează cu amendă de la 100 la 1000 de unități convenționale aplicată persoanei fizice, cu amendă de la 500 la 1500 de unități convenționale aplicată persoanei cu funcție de răspundere.

(2) Încălcarea cerințelor stabilite de art. 11 alin. (1), (2), (2²), (2³) sau (3) ori de art. 12 alin. (1), (3), (3¹), (4), (6), (7¹), (8) sau (8¹) din Legea nr. 48/2023 privind securitatea cibernetică de către furnizorul important de servicii,

se sancționează cu amendă de la 50 la 500 de unități convenționale aplicată persoanei fizice, cu amendă de la 100 la 1000 de unități convenționale aplicată persoanei cu funcție de răspundere.

(3) Neexecutarea obligației prevăzute de articolul 17 alin. (4) din Legea nr. 48/2023 privind securitatea cibernetică,

se sancționează cu amendă de la 50 la 150 de unități convenționale aplicată persoanei cu funcție de răspundere, cu amendă de la 100 la 500 de unități convenționale aplicată persoanei juridice.

Articolul 259⁴. Împiedicarea activității Agenției pentru Securitate Cibernetică

Refuzul neîntemeiat de a prezenta informațiile sau documentele solicitate de Agenția pentru Securitate Cibernetică în procesul exercitării atribuțiilor sau prezentarea informației neautentice sau incomplete sau împiedicarea accesului pentru personalul abilitat cu funcții de control al Agenției pentru Securitate Cibernetică în locurile unde sunt amplasate obiectele controlului,

se sancționează cu amendă de la 50 la 150 de unități convenționale aplicată persoanei fizice, cu amendă de la 100 la 300 de unități convenționale aplicată persoanei cu funcție de răspundere, cu amendă de la 500 la 1500 de unități convenționale aplicată persoanei juridice.”.

2. Se completează cu articolul 410¹ cu următorul cuprins:

„Articolul 410¹. Agenția pentru Securitate Cibernetică

(1) Contravențiile prevăzute la articolele 259³ și 259⁴ se constată și se examinează de către Agenția pentru Securitate Cibernetică.

(2) Sunt în drept să constate contravenții și să încheie procese-verbale șefii subdiviziunilor și funcționarii din cadrul Agenției pentru Securitate Cibernetică, împuterniciți de către directorul sau directorul adjunct al Agenției.

(3) Sunt în drept să examineze cauzele contravenționale și să aplice sancțiuni directorul sau directorul adjunct ai Agenției pentru Securitate Cibernetică.”.

Art. II - Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr.151–153, art.225), se modifică după cum urmează:

1. Clauza de armonizare va avea următorul cuprins:

„Prezenta lege transpune Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr.910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), publicată în Jurnalul Oficial al Uniunii Europene seria L nr.333 din 27 decembrie 2022.”;

2. Articolul 1 va avea următorul cuprins:

„Articolul 1. Obiectul de reglementare

Prezenta lege are ca obiect de reglementare:

- a) cadrul instituțional, de coordonare și de cooperare la nivel național în domeniul securității cibernetică, inclusiv de gestionare a crizelor în domeniul securității cibernetică;
- b) statutul juridic al autorității competente în domeniul securității cibernetică;
- c) obligațiile privind asigurarea securității cibernetică, inclusiv cu privire la măsurile de gestionare a riscurilor de securitate cibernetică și la notificarea incidentelor cibernetică semnificative, precum și supravegherea și controlul de stat al modului în care aceste obligații sunt respectate;

d) cerințele de bază în ce privește schimbul de informații în materie de securitate cibernetică.”

3. Articolul 2:

1) la noțiunea **amenințare cibernetică semnificativă**, după cuvântul „persoane” se introduc cuvintele „fizice sau”;

2) noțiunea **„furnizor de servicii”** va avea următorul cuprins:

„furnizor de servicii – persoană juridică de drept privat sau persoană fizică care practică activitate de întreprinzător (în continuare - întreprinderi), înregistrată în Republica Moldova, care este de tipul stabilit de Guvern în sectoarele și subsectoarele critice, sau persoană juridică de drept public, care este identificată de autoritatea competentă în conformitate cu prevederile prezentei legi și ale actelor normative de punere a acestora în aplicare;”;

3) după noțiunea de **„furnizor de servicii”** se completează cu noțiunile *„furnizor de servicii DNS”, „furnizor de servicii gestionate” și „furnizor de servicii de securitate gestionate” cu următorul cuprins:*

furnizor de servicii DNS - o persoană fizică sau juridică care furnizează:

a) servicii de rezoluție a numelor de domenii recursive accesibile publicului pentru utilizatorii finali de internet; sau

b) servicii de rezoluție a numelor de domenii cu autoritate pentru utilizarea de către terți, cu excepția serverelor pentru nume primare;

furnizor de servicii gestionate – persoană fizică sau juridică care furnizează servicii (business-to-business) legate de instalarea, gestionarea, funcționarea sau întreținerea produselor, a rețelelor, a infrastructurii, a aplicațiilor de tehnologie a informației și comunicațiilor (TIC) sau a oricăror alte rețele și sisteme informatice, prin intermediul asistenței sau administrării active, efectuate fie la sediul clienților, fie la distanță;

furnizor de servicii de înregistrare a numelor de domenii - operator de registru sau un agent care acționează în numele operatorilor de registru, cum ar fi un furnizor sau un revânzător de servicii de protecție a confidențialității sau servicii de proxy;

furnizor de servicii de securitate gestionate – furnizor de servicii gestionate (business-to-business) care efectuează sau furnizează asistență pentru activitățile legate de gestionarea riscurilor în materie de securitate cibernetică;”;

4) după noțiunea de **„incident cibernetic”** se completează cu noțiunea *„incident cibernetic de mare amploare” cu următorul cuprins:*

„incident cibernetic de mare amploare - incident cibernetic care provoacă un nivel de perturbare care depășește capacitatea Republicii Moldova de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două state membre ale Uniunii Europene;”;

5) la noțiunea „**incident cibernetic evitat la limită**”, după cuvintele „care a fost împiedicat” se completează cu cuvintele „cu succes”;

6) după noțiunea de „**măsuri de securitate**” se completează cu noțiunile „motor de căutare online”, „piață online” și „platformă de servicii de socializare în rețea”, cu următorul cuprins:

motor de căutare online – serviciu digital care permite utilizatorilor să introducă interogări pentru a căuta, în principiu, în toate site-urile internet sau site-urile internet într-o anumită limbă, în baza unei interogări privind orice subiect sub forma unui cuvânt, a unei solicitări vocale, a unei fraze sau a unui alt element introdus și care revine cu rezultate în orice format în care se pot găsi informații legate de conținutul căutat;

piață online – serviciu care utilizează software, inclusiv o pagină de internet sau o parte a unei pagini de internet sau o aplicație gestionată de către comerciant sau în numele acestuia, care le permite consumatorilor să încheie contracte la distanță cu alți comercianți sau consumatori;

platformă de servicii de socializare în rețea – platformă care permite utilizatorilor finali să se conecteze, să partajeze, să descopere și să comunice între ei prin intermediul a mai multe dispozitive, în special prin intermediul chatului, al postărilor, al materialelor video și al recomandărilor;”;

7) la noțiunea de „**proces al tehnologiei informației și comunicațiilor (proces TIC)**”, textul „și/sau a întreține produse TIC sau servicii TIC” se substituie cu textul „sau a întreține un produs TIC sau un serviciu TIC”;

8) la noțiunea de „**produs al tehnologiei informației și comunicațiilor (produs TIC)**” textul „ale rețelelor și/sau sistemelor informatice” se substituie cu textul „al unei rețele sau al unui sistem informatic”;

9) după noțiunea de „**produs al tehnologiei informației și comunicațiilor (produs TIC)**” se completează cu noțiunile „punct de schimb de internet (internet exchange point sau IXP)”, „registru de nume de domenii de prim nivel sau „registru de nume TLD” (top-level domain – TLD)”, „reprezentant” și „rețea de furnizare de conținut”, cu următorul cuprins:

„punct de schimb de internet (internet exchange point) – infrastructură de rețea care permite interconectarea a mai mult de două rețele autonome independente (sisteme autonome), în special în scopul facilitării schimbului de trafic de internet, care furnizează interconectare doar pentru sisteme autonome și care nu necesită trecerea printr-un al treilea sistem autonom al traficului de internet dintre orice pereche de sisteme autonome participante și nici nu modifică sau nu interacționează într-un alt mod cu acest trafic;

registru de nume de domenii de prim nivel sau „registru de nume TLD” (top-level domain – TLD) - o persoană fizică sau juridică căreia i s-a delegat un anumit TLD și care este responsabilă cu administrarea TLD-ului, inclusiv cu înregistrarea numelor de domenii în cadrul TLD-ului și cu exploatarea tehnică a TLD-ului, inclusiv exploatarea serverelor sale

de nume, întreținerea bazelor sale de date și distribuirea fișierelor zonale TLD între serverele de nume, indiferent dacă oricare dintre aceste operațiuni este efectuată de persoana însăși sau este externalizată, dar excluzând situațiile în care numele TLD sunt utilizate de un registru numai pentru uzul propriu;

reprezentant - o persoană fizică sau juridică stabilită în Uniunea Europeană care este desemnată în mod explicit să acționeze în numele unui furnizor de servicii DNS, al unui registru de nume TLD, al unei entități care furnizează servicii de înregistrare a numelor de domenii, al unui furnizor de servicii de cloud computing, al unui furnizor de servicii de centre de date, al unui furnizor de rețele de furnizare de conținut, al unui furnizor de servicii gestionate, al unui furnizor de servicii de securitate gestionate sau al unui furnizor al unei piețe online, al unui motor de căutare online sau al unei platforme de servicii de socializare în rețea, care nu este stabilit în Uniunea Europeană, căreia autoritatea competentă i se poate adresa în locul furnizorului de servicii în cauză în ceea ce privește obligațiile ce îi revin acestuia conform prezentei legi;

rețea de furnizare de conținut – rețea de servere distribuite geografic cu scopul de a asigura o disponibilitate ridicată, o accesibilitate sau o furnizare rapidă de conținut digital și servicii către utilizatorii de internet, în numele furnizorilor de conținut și de servicii;”;

10) la noțiunea „**rețea și sistem informatic**”, litera a), textul „Legii comunicațiilor electronice nr. 241/2007” se substituie cu textul „legislației privind comunicațiile electronice”;

11) la noțiunea „**securitatea rețelelor și sistemelor informatice**” cuvintele „oricărei acțiuni” se substituie cu cuvintele „oricărui eveniment”;

12) după noțiunea de „**serviciu al tehnologiei informației și comunicațiilor (serviciu TIC)**” se completează cu noțiunile „**serviciu de centre de date**”, „**serviciu de cloud computing**”, „**serviciu de securitate gestionat**”, „**serviciu digital**” și „**sistem de nume de domenii sau DNS**” cu următorul cuprins:

„**serviciu de centre de date** – serviciu care cuprinde structuri sau grupuri de structuri dedicate găzduirii, interconectării și exploatării centralizate a tehnologiei informației și a echipamentelor de rețea, care furnizează servicii de stocare, prelucrare și transport de date, împreună cu toate instalațiile și infrastructura de distribuție a energiei electrice și de control al mediului;

„**serviciu de cloud computing** – serviciu digital care permite administrarea la cerere și accesul amplu la distanță la un bazin redimensionabil și elastic de resurse informatice, care pot fi puse în comun, inclusiv în cazul în care aceste resurse sunt distribuite în mai multe locații;

„**serviciu de securitate gestionat** – serviciu furnizat unei părți terțe care constă în desfășurarea sau furnizarea de asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică, cum ar fi gestionarea incidentelor, testele de rezistență la

intruziuni, auditurile de securitate și consultanța, inclusiv consultanța de specialitate, în legătură cu asistența tehnică;

serviciu digital – serviciu al societății informaționale, astfel cum este definit de Legea nr.284/2004 privind serviciile societății informaționale;

sistem de nume de domenii sau DNS - un sistem ierarhic și distribuit de atribuire de nume care face posibilă identificarea serviciilor și a resurselor de pe internet, permițând dispozitivelor utilizatorilor finali să utilizeze serviciile de rutare și conectivitate pe internet pentru a accesa serviciile și resursele respective.

4. Articolul 3 și articolul 4 vor avea următorul cuprins:

„Articolul 3. Domeniul de aplicare

(1) Prezenta lege se aplică persoanelor juridice de drept public, precum și întreprinderilor care îndeplinesc cumulativ următoarele condiții:

1) se califică drept întreprinderi mijlocii, potrivit clasificării prevăzute de legislația cu privire la întreprinderile mici și mijlocii, sau depășesc criteriile pentru întreprinderile mijlocii;

2) furnizează servicii în cel puțin unul dintre următoarele sectoare sau subsectoare critice:

a) sectoare și subsectoare de importanță critică ridicată:

1. sectorul energetică, care include subsectoarele energie electrică, încălzire centralizată și răcire centralizată, piața produselor petroliere, gaze naturale, hidrogen;

2. sectorul transport, care include subsectoarele transport aerian; transport feroviar, transport pe apă și transport rutier;

3. sectorul bancar;

4. sectorul infrastructuri ale pieței financiare;

5. sectorul sănătate;

6. sectorul alimentare cu apă și canalizare;

7. infrastructură digitală;

8. gestionare a serviciilor TIC (business-to-business);

9. spațiu;

b) sectoare de importanță critică:

1. sectorul servicii poștale și de curierat;

2. sectorul gestionarea deșeurilor;

3. sectorul fabricarea, producția și distribuția de substanțe chimice;

4. sectorul producția, prelucrarea și distribuția de alimente;

5. sectorul fabricare, care include, în conformitate cu clasificatorul activităților economice din Republica Moldova următoarele subsectoare: fabricarea dispozitivelor medicale și a dispozitivelor medicale pentru diagnostic in vitro; fabricarea calculatoarelor și

a produselor electronice și optice, fabricarea echipamentelor electrice, fabricarea altor mașini și echipamente neclasificate altundeva; fabricarea autovehiculelor, remorcilor și semiremorcilor; fabricarea altor echipamente de transport;

6. sectorul furnizori digitali;

7. sectorul cercetare;

3) sunt de cel puțin de un tip stabilit de Guvern.

(2) Prevederile art. 5² alin. (3) din Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii nu se aplică în sensul prezentei legi.

(3) Indiferent de dimensiunea acesteia, prezenta lege se aplică și întreprinderii, de tipul stabilit de Guvern, dacă aceasta îndeplinește cel puțin una dintre următoarele condiții:

a) este furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, în sensul legislației privind comunicațiile electronice;

b) este prestator de servicii de încredere, în sensul legislației privind identificarea electronică și serviciile de încredere;

c) este Registrator național al domeniului de nivel superior .md;

d) este furnizor de servicii DNS;

e) furnizează servicii de înregistrare a numelor de domenii;

f) este singurul furnizor în Republica Moldova al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice;

g) furnizează un serviciu, dependent de o rețea și/sau de un sistem informatic, perturbarea căruia ar putea avea un impact semnificativ asupra ordinii publice, a securității publice sau a sănătății publice

h) furnizează un serviciu, dependent de o rețea și/sau de un sistem informatic, perturbarea căruia ar putea genera un risc sistemic semnificativ, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier;

i) este critică din cauza importanței sale specifice la nivel național sau regional pentru sectorul ori tipul de servicii respective sau pentru alte sectoare interdependente;

j) este gestionar de infrastructură critică națională, identificată conform legislației privind identificarea, desemnarea și protecția infrastructurii critice naționale sau operator al obiectivului de infrastructură critică, identificat conform legislației privind prevenirea și combaterea terorismului;

(4) În sensul prezentei legi, în categoria furnizorilor esențiali de servicii intră:

1) furnizorii de servicii de tipurile stabilite de Guvern care îndeplinesc cumulativ următoarele condiții:

a) furnizează servicii în cel puțin un sector sau subsector de importanță critică ridicată;

b) depășesc criteriile pentru întreprinderile mijlocii, stabilite de legislația privind întreprinderile mici și mijlocii;

2) prestatorii de servicii de încredere calificați, Registratorul național al domeniului de nivel superior .md și furnizorii de servicii DNS, indiferent de dimensiunea lor;

3) furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului care se califică drept întreprinderi mijlocii sau depășesc criteriile pentru întreprinderile mijlocii, stabilite de legislația privind întreprinderile mici și mijlocii;

4) persoanele juridice de drept public, cu excepția autorităților administrației publice locale și a instituțiilor publice și serviciilor publice de interes raional sau local înființate de acestea;

5) întreprinderile care îndeplinesc cel puțin una din condițiile stabilite la alineatul (3) literele f)-i);

6) întreprinderile care îndeplinesc condiția stabilită la alineatul (3) litera j).

(5) Din categoria furnizorilor importanți de servicii fac parte întreprinderile și persoanele juridice de drept public care intră în domeniul de aplicare al prezentei legi în conformitate cu alineatele (1) și (2), dar nu cad sub incidența alineatului (3).

(6) Prezenta lege nu se aplică, cu excepția prestatorilor de servicii de încredere:

a) activităților desfășurate de către autoritățile publice în domeniul protecției secretului de stat, în legătură cu mentenanța rețelelor și sistemelor informatice care sunt destinate prelucrării unor astfel de informații;

b) activităților desfășurate de către autoritățile publice în domeniul securității naționale, al apărării naționale, al activității speciale de investigații și al urmăririi penale, în legătură cu mentenanța rețelelor și sistemelor informatice destinate prelucrării informațiilor din domeniile respective.

c) rețelelor și sistemelor informatice operate exclusiv de organisme de drept public cu sau fără personalitate juridică, înființate de către Republica Moldova sau de către Republica Moldova și un alt stat membru al Uniunii Europene în comun cu un stat care nu este membru al Uniunii Europene (țară terță) în conformitate cu un acord internațional;

d) rețelelor și sistemelor informatice ale misiunilor diplomatice și consulare Republicii Moldova în țări terțe, în măsura în care aceste sisteme se află la sediul misiunii sau sunt utilizate pentru utilizatori dintr-o țară terță.

(7) În cazul în care tratatele internaționale la care Republica Moldova este parte stabilesc alte norme decât cele prevăzute de prezenta lege, se aplică normele tratatelor internaționale.

(8) În cazul în care legile care reglementează activitatea furnizorilor de servicii sau sectoarele și subsectoarele critice (în continuare - legi sectoriale), prevăd implementarea unor măsuri de securitate sau îndeplinirea obligațiilor de notificare a incidentelor

cibernetice cu impact semnificativ, ale căror efecte sunt cel puțin echivalente cu efectele obligațiilor stabilite de prezenta lege, se consideră că prevederile legilor sectoriale au caracter special în raport cu prevederile prezentei legi.

(9) Legile sectoriale sunt considerate echivalente în privința efectului cu obligațiile prevăzute în prezenta lege dacă:

a) măsurile de gestionare a riscurilor în materie de securitate cibernetică sunt cel puțin echivalente în privința efectului cu cele prevăzute la articolul 11, sau

b) legea sectorială prevede accesul imediat, după caz automat și direct, la notificările incidentelor cibernetice pentru autoritatea competentă în temeiul prezentei legi și dacă cerințele de notificare a incidentelor cibernetice cu impact semnificativ au un efect cel puțin echivalent cu cele prevăzute la articolul 12.

(10) În cazul în care obligațiile, prevăzute la alin.(8), stabilite de legile sectoriale sunt aplicabile unui număr mai restrâns de întreprinderi decât cel prevăzut de prezenta lege prevederile prezentei legi se aplică întreprinderilor care nu cad sub incidența obligațiilor impuse de legile sectoriale.

(11) Prevederile alin.(8) și (10) din prezentul articol se aplică de către autoritatea competentă în modul stabilit de Guvern.

(12) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului intră în domeniul de aplicare al prezentei legi dacă prestează servicii pe teritoriul Republicii Moldova, indiferent de locul de înființare sau de înregistrare.

Articolul 4. Identificarea furnizorilor de servicii în sectoarele și subsectoarele critice

(1) Întreprinderile sunt identificate în calitate de furnizori de servicii în sectoarele și subsectoarele critice de către autoritatea competentă. Modul de identificare a furnizorilor de servicii și tipurile furnizorilor de servicii corespunzătoare sectoarelor și subsectoarelor critice se stabilesc de Guvern.

(2) În procesul identificării furnizorilor de servicii, autoritatea competentă trebuie să determine eligibilitatea întreprinderii în conformitate cu toate temeiurile stabilite la art. 3 alineatele (1) - (4). Dacă întreprinderea este identificată ca furnizor de servicii în baza mai multor temeiuri de la art. 3 alin. (1) - (4) și cel puțin unul dintre aceste temeiuri o califică ca furnizor esențial de servicii, aceasta urmează a fi desemnată ca furnizor esențial de servicii.

(3) Decizia cu privire la desemnarea în calitate de furnizor de servicii se comunică furnizorului de servicii identificat în termen de 5 zile din data emiterii.

(4) Decizia de desemnare în calitate de furnizor de servicii poate fi contestată în instanța de judecată în conformitate cu prevederile cadrului normativ. Acțiunea de contestare a deciziei autorității competente nu are efect suspensiv de executare.

(5) Întreprinderile se pot autoidentifica în mod voluntar în conformitate cu prevederile prezentei legi și cadrul normativ aprobat de Guvern și pot remite în acest sens o înștiințare către autoritatea competentă. Autoritatea competentă asigură implementarea mecanismelor necesare pentru autoidentificare.

(6) Autoidentificarea nu exclude obligația autorității competente de a realiza procesul de identificare în privința respectivei întreprinderi în conformitate cu prezenta lege.

(7) Persoanele juridice de drept public sunt identificate ca furnizori de servicii în sectorul administrație publică și incluși în Lista furnizorilor de servicii prin efectul legii. Sectorul administrație publică este sector de importanță critică ridicată.

(8) La solicitarea autorității competente, Ministerul Afacerilor Interne și Serviciul de Informații și Securitate, în termen de 30 de zile de la data solicitării, furnizează acesteia lista gestionarilor de infrastructură critică națională și, respectiv, lista operatorilor obiectivelor de infrastructură critică, precum și orice modificare a acestor liste, în termen de 15 zile de la data operării modificării respective. Listele respective trebuie să cuprindă cel puțin următoarele informații::

- a) denumirea și numărul de identificare de stat (IDNO)
- b) datele de contact ale conducătorului sau reprezentantului împuternicit (nume, prenume, funcție, număr de telefon, adresă de email);
- c) sectorul critic, după caz subsectorul critic, și tipul gestionarului de infrastructură critică, conform anexei la Legea nr.223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale;
- d) serviciile esențiale prestate de gestionarul infrastructurii critice naționale;
- e) gama de IP-uri utilizate de gestionarul infrastructurii critice;
- f) statele, inclusiv statele membre ale Uniunii Europene, în care gestionarul infrastructurii critice naționale prestează serviciile esențiale.

(9) În scopurile identificării, autoritatea competentă utilizează informațiile conținute în resursele informaționale de stat. Autoritățile și instituțiile publice, deținători ai resurselor informaționale de stat, oferă autorității competente acces la datele și informațiile relevante, conform solicitării acesteia.

(10) Atunci când este necesară verificarea veridicității informației disponibile în resursele informaționale de stat, la solicitarea autorității competente, întreprinderile prezintă în termen de 14 zile, informațiile necesare identificării acestora în calitate de furnizori de servicii, inclusiv cele menționate la art. 4² alin. (3).

(11) Autoritățile publice responsabile de realizarea politicii de stat în sectoarele sau subsectoarele critice, stabilite de către Guvern, instituțiile publice responsabile de gestionarea unor domenii conexe sectoarelor și subsectoarelor respective, precum și, după caz, autoritățile publice de reglementare a activității în aceste sectoare sau subsectoare

asigură acordarea suportului necesar autorității competente, la solicitarea acesteia, în procesul de identificare a furnizorilor de servicii.

(12) Întreprinderile identificate în calitate de furnizor de servicii și persoanele juridice de drept public sunt înregistrate în Lista furnizorilor de servicii.”

5. Se completează cu articolele 4¹, 4² și 4³ cu următorul cuprins:

„Articolul 4¹. Încetarea calității de furnizor de servicii

(1) Autoritatea competentă decide încetarea calității de furnizor de servicii:

a) dacă întreprinderea nu mai corespunde condițiilor stabilite de articolul 3 alineatele (1)-(4);

b) dacă întreprinderea sau persoana juridică de drept public a încetat activitatea.

(2) Procedura de încetare a calității de furnizor de servicii se inițiază de autoritatea competentă la sesizare sau din oficiu.

(4) În cazul prevăzut la alin. (1) lit.a), autoritatea competentă remite decizia de încetare a calității de furnizor de servicii, întreprinderii vizate în termen de 5 zile de la data emiterii.

Articolul 4². Lista furnizorilor de servicii

(1) Autoritatea competentă întocmește și ține Lista furnizorilor de servicii, inclusiv a furnizorilor de servicii de înregistrare a numelor de domenii.

(2) Lista constituie principala resursă informațională de stat de evidență a furnizorilor de servicii și reprezintă sursa primară de informație oficială privind statutul de furnizor de servicii în sensul prezentei legi.

(3) Lista furnizorilor de servicii cuprinde cel puțin următoarele informații:

a) datele generale privind furnizorul de servicii: denumirea, forma de organizare juridică, adresa juridică, numărul de identificare de stat (IDNO), datele de contact (telefon, email, fax), și gama de IP-uri,

b) datele de contact (nume, prenume, telefon, email) ale administratorului și ale angajatului responsabil pentru interacțiunea cu autoritatea competentă;

c) sectorul critic și, după caz, subsectorul critic, tipul și categoria furnizorului de servicii;

e) statele în care furnizorul de servicii prestează servicii corespunzătoare tipului stabilit de Guvern, conform căruia a fost identificat în calitate de furnizori de servicii.

(4) Autoritatea competentă actualizează Lista furnizorilor de servicii, ori de câte ori este necesar, însă nu mai rar decât o dată la doi ani.

(5) În scopul întocmirii Listei furnizorilor de servicii la solicitarea autorității competente, furnizorii de servicii prezintă acesteia în termen de 30 de zile de la solicitare

informațiile prevăzute la alineatul (3), precum și notifică fără întârziere orice modificare a informațiilor respective însă nu mai târziu de 14 zile de la data modificării.

(6) Furnizorul de servicii este radiat din Lista furnizorilor de servicii în temeiul deciziei autorității competente de încetare a calității de furnizor de servicii.

(7) Modul de întocmire, ținere și actualizare a Listei furnizorilor de servicii se stabilește de Guvern.

Articolul 4³. Cerințe specifice față de unele tipuri de furnizori de servicii

(1) Furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de înregistrare a numelor de domenii, 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, precum și furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, prezintă autorității competente următoarele informații:

- a) denumirea furnizorului de servicii;
- b) sectorul, subsectorul relevant și tipul stabilit de Guvern;
- c) adresa sediului principal al furnizorului de servicii și a celorlalte sedii legale ale sale din Uniunea Europeană sau, dacă nu este stabilită sau nu are un sediu legal în Uniunea Europeană, adresa reprezentantului său desemnat în Uniunea Europeană;
- d) datele de contact actualizate, inclusiv adresele de e-mail și numerele de telefon ale furnizorului de servicii și, după caz, ale reprezentantului său desemnat în Uniunea Europeană;
- e) statele membre ale Uniunii Europene în care entitatea furnizează servicii; și
- f) gamele de adrese IP ale furnizorului de servicii.

(2) Furnizorii de servicii menționați la alin. (1) informează autoritatea competentă fără întârziere și, în orice caz, în termen de trei luni de la data modificării, orice modificare a informațiilor pe care le-au transmis în temeiul alin. (1).

(3) Autoritatea competentă transmite, fără întârzieri justificate, informațiile prevăzute la alin. (1), cu excepția celor de la lit. f), către Agenția Uniunii Europene pentru Securitate Cibernetică.

(4) Furnizorii de servicii, de tipul celor menționați la alin. (1) intră sub jurisdicția Republicii Moldova dacă au sediul principal din Uniunea Europeană în Republica Moldova sau, dacă nu sunt stabiliți în Uniunea Europeană, au stabilit un reprezentant în Republica Moldova.

(5) Se consideră că furnizorii de servicii de tipul celor menționați la alin. (1) au sediul principal în Republica Moldova în cazul în care deciziile privind măsurile de securitate ale furnizorului de servicii sunt luate în mod predominant în Republica Moldova.

(6) Dacă nu este posibilă determinarea sediului principal conform alin. (5) sau nu poate fi determinat un alt stat membru al UE în care furnizorul de servicii, de tipul celor menționați la alin. (1), își are sediul principal sau dacă deciziile furnizorului respectiv de servicii privind măsurile de securitate nu sunt luate în Uniunea Europeană, se consideră că sediul principal al furnizorului de servicii este Republica Moldova dacă activitățile sau operațiunile de realizare a obligațiilor de asigurare a securității cibernetice se desfășoară în Republica Moldova.

(7) Dacă sediul principal al furnizorului de servicii, de tipul celor menționați la alin. (1), nu poate fi determinat în conformitate cu alin. (5) și (6), se consideră că sediul principal al furnizorului respectiv de servicii este în Republica Moldova dacă furnizorul respectiv de servicii își are sediul cu cel mai mare număr de angajați din Uniunea Europeană în Republica Moldova.

(8) În cazul în care un furnizor de servicii de tipul menționat la alin (1) nu este stabilit în Uniunea Europeană, dar prestează servicii în Republica Moldova, acesta trebuie să desemneze un reprezentant în Republica Moldova sau într-un alt stat membru al Uniunii Europene în care își prestează serviciile și să prezinte autorității competente informațiile de contact ale reprezentantului său, precum și să le facă publice. Dacă furnizorul respectiv de servicii nu desemnează un reprezentant în Uniunea Europeană, autoritățile și instituțiile publice pot iniția acțiuni în justiție sau activități de control sau aplica măsurilor de asigurare a respectării legii împotriva acestui furnizor de servicii, dacă acesta prestează servicii pe teritoriul Republicii Moldova.

(9) Desemnarea unui reprezentant de către un furnizor de servicii de tipul menționat la alin (1), nu împiedică inițierea unor acțiuni în justiție sau a activităților de control sau a aplicării măsurilor de asigurare a respectării legii împotriva entității înseși.”

6. La articolul 6:

alineatul (1) cuvintele „politicii de stat” de substituie cu cuvintele „politicii publice a Guvernului”;

la alineatul (2), după cuvântul „politicilor” se completează cu cuvintele „publice a Guvernului”.

7. Articolul 7:

în **titlu**, după cuvântul „competentă” se completează cu textul „în domeniul securității cibernetice”;

la **alineatul (2)**, după cuvântul echipă se completează cu „națională”, iar cuvintele „la nivel național” se exclud;

la **alineatul (3)**:

litera a), după cuvintele „furnizorilor de servicii” se completează cu textul „în sectoarele și subsectoarele critice”;

se completează cu **literale c¹**) și c²) cu următorul cuprins:

„c¹) reprezintă Republica Moldova în Grupul de cooperare privind rețelele și sistemele informatice al Uniunii Europene (în continuare – Grupul de cooperare) și asigură participarea și cooperarea în cadrul acestuia;

c²) în conformitate cu art. 7² participă la evaluările inter pares în condițiile legislației relevante a Uniunii Europene și în conformitate cu metodologia stabilită de Grupul de cooperare;”;

la **alineatul (4)**:

după cuvântul „echipă” se completează cu „națională”, iar cuvintele „la nivel național” se exclud;

se completează cu **punctul 1¹)** cu următorul cuprins:

„1¹) monitorizează numele de domenii din spațiul de adrese în Internet al Republicii Moldova și legate de domeniul de nivel superior .md, analizează riscurile, precum și impactul potențial al acestora asupra statului, societății și securității rețelelor și sistemelor informatice;”;

punctul 2), după cuvintele „monitorizare de către aceștia” se completează cu textul „, în timp real sau aproape real;”;

punctul 3) va avea următorul cuprins:

„3) emite avertizări timpurii, alerte, anunțuri și diseminează informații către părți interesate relevante, inclusiv și în mod prioritar către furnizorii de servicii vizați, privind amenințările cibernetice, vulnerabilitățile și incidentele cibernetice, dacă este posibil, în timp aproape real;”;

se completează cu **punctul 3¹)** cu următorul cuprins:

„3¹) efectuează scanări proactive și neintrusive ale rețelelor și sistemelor informatice accesibile publicului ale furnizorilor de servicii pentru a detecta rețelele și sistemele informatice vulnerabile sau configurate în mod nesigur și pentru a informa furnizorii de servicii respectivi, fără a afecta continuitatea prestării serviciilor și activitatea acestora;”;

se completează cu **punctele 7¹) și 7²)** cu următorul cuprins:

„7¹) cooperează și, după caz, face schimb de informații în materie de securitate cibernetică cu furnizorii de servicii și cu alte părți interesate din sectorul privat, precum și facilitează instituirea unor comunități ale furnizorilor de servicii la nivelul unuia sau mai multor sectoare sau subsectoare critice;

7²) asigură calitatea de membru în rețeaua Echipelor de intervenție în caz de incidente de securitate informatică a Uniunii Europene (rețeaua CSIRT) și furnizează, la

solicitarea altor membri ai rețelei CSIRT asistență în funcție de capacitățile și competențele de care dispune;”;

punctul 8), textul „ , în conformitate cu actul normativ aprobat de Guvern potrivit art.12 alin.(9)” se exclude;

se completează cu **punctul 9¹)** cu următorul cuprins:

„9¹) pentru facilitarea cooperării cu sectorul privat, asigură promovarea, acceptarea și utilizarea unor practici, sisteme de clasificare și taxonomii comune sau standardizate în legătură cu procedurile de gestionare a incidentelor cibernetice, de gestionare a crizelor și cele de divulgare a coordonată a vulnerabilităților;”;

punctul 10) se completează cu litera e¹) cu următorul cuprins:

„e¹) în cazul în care o vulnerabilitate raportată ar putea avea un impact semnificativ asupra persoanelor din mai multe state membre ale Uniunii Europene, asigură cooperarea în cadrul Rețelei CSIRT cu alți coordonatori ai procesului de divulgare coordonată a vulnerabilităților în statele membre respective.”.

se completează cu **alineatul (4¹) cu următorul cuprins:**

„(4¹) Pentru realizarea eficientă a funcției de echipă națională de răspuns la incidente cibernetice, autoritatea competentă asigură în mod continuu corespunderea subdiviziunilor interne și a personalului implicat în exercitarea acestei funcții cu următoarele cerințe:

- a) disponibilitate înaltă, publicitate și diversitate a canalelor de comunicare în mod special cu furnizorii de servicii;
- b) localuri și sistemele informatice de suport situate în amplasamente securizate;
- (c) sistem adecvat de gestionare și redirectionare a solicitărilor, în special pentru a facilita transferurile eficiente și eficace ale acestora;
- (d) confidențialitate și credibilitate a operațiunilor sale;
- (e) personal calificat pentru a asigura disponibilitatea permanentă a serviciilor;
- (f) continuitate a activității, inclusiv prin echiparea cu sisteme redundante și spațiu de lucru de rezervă.”.

8. Se completează cu **articolele 7¹ , 7² și 7³**, cu următorul cuprins:

„Articolul 7¹. Cooperarea și schimbul de informații cu autoritățile și instituțiile Uniunii Europene

(1) În scopul îndeplinirii obligațiilor de informare în relația cu autoritățile și instituțiile Uniunii Europene, autoritatea competentă:

- (a) prezintă, o dată la doi ani, Comisiei Europene și Grupului de cooperare o informație privind numărul furnizorilor esențiali de servicii și numărul furnizorilor importanți de servicii pentru fiecare sector și subsector critic;

(b) prezintă, o dată la doi ani, Comisiei Europene o informație privind numărul de furnizori de servicii identificați în temeiul articolului 3 alineatul (3) literele (f)-(i), sectorul și subsectorul critic din care acestea fac parte, tipul de servicii pe care le furnizează și dispozițiile legale, dintre cele de la articolul 3 alineatul (3) literele (f)-(i), în temeiul cărora furnizorii de servicii respectivi au fost identificați;

c) la cererea Comisiei Europene, furnizează informații privind denumirile furnizorilor de servicii menționați la litera b), dacă aceasta nu prejudiciază securitatea națională, ordinea sau securitatea publică;

d) în termen de 3 luni de la adoptare, notifică Comisiei Europene strategia națională de securitate cibernetică;

e) notifică Comisiei Europene identitatea autorității competente în domeniul securității cibernetice, inclusiv calitatea acesteia de autoritate de gestionare a crizelor cibernetice, precum și, fără întârzieri nejustificate, orice modificare în datele de identificare sau în competența acesteia în ce privește exercitarea atribuțiilor sale de punct național unic de contact pentru asigurarea cooperării transfrontaliere în domeniul securității cibernetice la nivelul Uniunii Europene, de autoritate responsabilă de gestionarea crizelor cibernetice, de echipă națională de răspuns la incidentele cibernetice sau de coordonator al procesului de divulgare coordonată a vulnerabilităților.

f) în termen de 3 luni de la data adoptării planului național de răspuns la incidente cibernetice și crize cibernetice, prezintă Comisiei și Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) informații relevante, solicitate de aceste organizații referitoare la cerințele de la articolul 9 alineatul (3) cu privire la planul respectiv, cu excepția informațiilor care ar putea prejudicia securitatea națională;

g) o dată la trei luni, transmite Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) un raport de sinteză care include date anonimizate și agregate privind incidentele cibernetice cu impact semnificativ, incidentele, amenințările cibernetice semnificative și incidentele evitate la limită notificate în conformitate cu articolele 12 și 13.

h) furnizează, în caz de necesitate sau la solicitare autorităților și instituțiilor Uniunii Europene informații suplimentare și asigură cooperarea necesară;

i) furnizează Comisiei Europene și Agenției Uniunii Europene pentru Securitate Cibernetică alte informații a căror furnizare decurge din prevederile Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022.

(2) În cadrul schimbului de informații cu autoritățile Uniunii Europene autoritatea competentă nu poate furniza informații a căror divulgare ar contraveni intereselor esențiale ale statelor membre ale Uniunii Europene în materie de securitate națională, siguranță și ordine publică sau apărare.

(3) Autoritatea competentă poate face schimb de informații, considerate confidențiale în conformitate cu normele Uniunii Europene sau cu cele naționale, precum

și informații care constituie secret comercial, cu Comisia Europeană și cu alte autorități relevante ale Uniunii Europene, numai dacă acest schimb de informații este necesar pentru aplicarea prezentei legi, conform scopului urmărit prin schimbul de informații și proporțional acestui scop.

(4) Autoritatea competentă limitează schimbul de informații la informațiile relevante scopului urmărit și proporționale cu acest scop, asigurând păstrarea confidențialității informațiilor și protecția securității și intereselor comerciale ale furnizorilor de servicii sau ale altor persoane vizate de schimbul de informații.

Articolul 7². Participarea Republicii Moldova în evaluările inter pares

(1) Autoritatea competentă decide participarea la evaluările inter pares în conformitate cu actele normative relevante ale Uniunii Europene.

(2) Atunci când participă în cadrul evaluărilor inter pares, autoritatea competentă:

a) poate identifica și propune pentru o evaluare inter pares aspecte specifice de natură transfrontalieră sau transsectorială în materie de securitate cibernetică;

b) informează statele membre ale Uniunii Europene care participă la evaluarea inter pares cu privire la domeniul de aplicare al acesteia, inclusiv aspectele specifice identificate în temeiul literei a);

c) poate efectua o autoevaluare, în conformitate cu metodologia stabilită de Grupul de cooperare, a aspectelor ce urmează a fi supuse evaluării și furniza autoevaluarea respectivă experților în materie de securitate cibernetică desemnați;

e) furnizează experților în materie de securitate cibernetică desemnați informațiile necesare pentru evaluare, fără a aduce atingere dreptului Uniunii Europene privind protecția informațiilor confidențiale sau clasificate sau cadrului normativ național privind protecția secretului de stat și asigurarea securității naționale.

f) decide publicarea raportului de evaluare inter pares în privința sa sau a unei versiuni redactate a acestuia;

g) înainte de începerea evaluării inter pares, informează celelalte state membre ale Uniunii Europene, Grupul de cooperare, Comisia și ENISA cu privire la orice risc de conflict de interese în ceea ce privește experții în materie de securitate cibernetică pe care îi desemnează;

h) poate formula obiecții motivate cu privire la desemnarea anumitor experți în securitate cibernetică și le comunica statului membru al Uniunii Europene care a desemnat experții respectivi;

i) prezintă observații cu privire la proiectele de rapoarte care o privesc;

j) exercită alte atribuții care derivă din participarea sa în evaluări inter pares în conformitate cu legislația relevantă.

Articolul 7³. Cooperarea la nivel național și internațional în materie de securitate cibernetică

(1) Autoritatea competentă, autoritățile publice responsabile în temeiul legislației privind identificarea, desemnarea și protecția infrastructurilor naționale critice și Ministerul Afacerilor Interne cooperează și fac schimb reciproc de informații ori de câte ori este necesar pentru identificarea infrastructurilor critice naționale, cu privire la riscurile, amenințările cibernetică și incidentele cibernetică, precum și la riscurile, amenințările și incidentele de altă natură decât cibernetică care afectează furnizorii esențiali de servicii, identificați ca fiind critici în temeiul legislației privind identificarea, desemnarea și protecția infrastructurilor naționale critice, precum și cu privire la măsurile luate ca răspuns la astfel de riscuri, amenințări și incidente.

(2) Autoritatea competentă în temeiul prezentei legi și autoritățile de supraveghere și reglementare a domeniului identificării electronice și serviciilor de încredere, a domeniului comunicațiilor electronice și al domeniilor bancar și pieței financiare fac schimb de informații relevante în mod periodic, inclusiv în ceea ce privește incidentele și amenințările cibernetică relevante.

(3) În scopul realizării eficiente a prevederilor prezentului articol autoritățile publice menționate în alineatele (1) și (2) pot adopta acte administrative comune în vederea reglementării procedurilor operaționale de cooperare și de schimb reciproc de informații în materie de securitate cibernetică.”.

(4) În contextul realizării atribuțiilor prevăzute de prezenta lege sau în temeiul obligațiilor care decurg dintr-un tratat internațional, autoritatea competentă este în drept să transmită altui stat sau organizații internaționale informații privind prevenirea și soluționarea incidentelor cibernetică în cazul în care nu există riscul ca informațiile transmise să prejudicieze securitatea națională sau desfășurarea procedurilor de urmărire penală. Schimbul de informații în sensul prezentului alineat se efectuează cu respectarea condițiilor stabilite la art. 7¹ alin. (2) – alin. (4).

9. La articolul 9:

în titlu și în tot textul cuvintele „în domeniul securității” se exclud;

alineatul (1) va avea următorul cuprins:

„(1) Autoritatea competentă este autoritatea publică națională responsabilă cu gestionarea incidentelor cibernetică de mare amploare și a crizelor cibernetică.”;

la alineatul (2) sintagma „În acest scop, autoritatea” se substituie cu cuvântul „Autoritatea”;

alineatul (3) litera f), textul „gestionarea incidentelor cibernetice și a crizelor în domeniul securității cibernetice de mare amploare” se substituie cu textul „gestionarea incidentelor cibernetice de mare amploare și a crizelor în domeniul securității cibernetice”
alineatul (4) cuvântul „metodologic” se exclude.

10. La articolul 11:

alineatul (2) punctul 2)

textul „să implementeze măsuri tehnice și organizatorice corespunzătoare și proporționale, în conformitate cu standardele aprobate potrivit alin.(4) lit. a),” se substituie cu textul „să implementeze, în mod corespunzător și proporțional, măsuri de securitate tehnice, operaționale și organizatorice”;

a doua propoziție după cuvântul „trebuie” se completează cu textul „să se bazeze pe o abordare multirisc, care vizează protecția rețelelor și a sistemelor informatice și a mediului fizic al acestor sisteme împotriva incidentelor cibernetice, și”

se completează cu **alineatele (2¹), (2²) și (2³)** cu următorul cuprins:

„(2¹) Administratorul furnizorului de servicii este obligat:

a) să urmeze cursuri de formare pentru a dobândi suficiente cunoștințe și competențe pentru a putea identifica riscurile și a evalua practicile de gestionare a riscurilor de securitate cibernetică și impactul acestora asupra serviciilor pe care le prestează furnizorul de servicii;

b) să aprobe măsurile de securitate a rețelelor și a sistemelor informatice;

c) să supravegheze modul în care aceste măsuri sunt implementate.

Atunci când administrarea furnizorului de servicii este realizată de un organ colegial, acesta desemnează un membru al organului colegial responsabil de realizarea obligațiilor de asigurare a securității cibernetice, care este obligat să urmeze cursurile de formare prevăzute la lit. a). La cererea autorității competente, furnizorul de servicii comunică numele și datele de contact ale membrului sau membrilor relevanți ai organului colegial desemnat. Autoritatea competentă oferă orientări metodologice furnizorilor de servicii în vederea realizării obligațiilor prevăzute de prezentul alineat.

(2²) Furnizorul de servicii trebuie să asigure un nivel de securitate a rețelelor și sistemelor sale informatice proporțional riscurilor la adresa acestor rețele și sisteme informatice. La determinarea proporționalității dintre măsurile de securitate și riscuri, furnizorul de servicii, în procesul de implementare a acestor măsuri, și autoritatea competentă, în exercitarea controlului de stat, trebuie să țină cont în mod corespunzător de gradul de expunere a furnizorului de servicii la riscuri, de dimensiunea acestuia, de probabilitatea producerii incidentelor cibernetice și de gravitatea acestora, inclusiv de impactul lor societal și economic, precum și de costul punerii în aplicare a măsurii de

securitate. La aplicarea măsurilor de securitate, furnizorul de servicii ia în considerare cele mai avansate standarde naționale, europene și internaționale în domeniu.

(2³) Atunci când analizează ce măsuri de securitate de la alin. (2) pct.2 lit. h), sunt corespunzătoare riscurilor, furnizorii de servicii trebuie să ia în considerare:

a) vulnerabilitățile specifice fiecărui prestator și furnizor direct de servicii, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale prestatorilor și furnizorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare;

b) rezultatele evaluărilor coordonate, la nivelul Uniunii Europene, ale riscurilor de securitate a lanțurilor de aprovizionare critice efectuate de Grupul de cooperare. ”;

La **alineatul (4) litera b)** textul „specifice de securitate privind rețelele și sistemele informatice în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii” se substituie cu textul „privind măsurile de securitate a rețelelor și a sistemelor informatice ale furnizorilor de servicii în sectoarele critice”.

11. La articolul 12:

titlul va avea următorul cuprins:

„Articolul 12. Obligații de notificare a incidentelor cibernetice semnificative”;

alineatul (1):

cuvântul „informează” se substituie cu cuvântul „notifică”;

se completează în final cu o propoziție cu următorul cuprins:

„În scopul notificării conform prezentului alineat furnizorii de servicii transmit autorității competente o avertizare timpurie care trebuie să cuprindă cel puțin informațiile disponibile la momentul notificării despre incidentul cibernetic, inclusiv informații privind existența suspiciunilor că incidentul cibernetic cu impact semnificativ este cauzat de acțiuni ilegale sau răuvoitoare și informații dacă acesta ar putea avea un impact transfrontalier.”.

la alineatul (2):

după cuvintele „fără întârzieri nejustificate” se completează cu sintagma „ , atunci când este posibil,”;

cuvântul „informației” se substituie cu cuvintele „avertizării timpurii”;

textul „recomandări și instrucțiuni operaționale” se substituie cu textul „recomandări, instrucțiuni operaționale și suportul tehnic necesar”;

după cuvintele „continuitate a activității” se completează cu textul „ , precum și orientări privind raportarea incidentului către autoritățile de aplicare a legi, dacă există suspiciuni că incidentul cibernetic ar putea constitui o infracțiune sau o contravenție”;

alineatul (3), după cuvintele „despre incidentul cibernetic” se completează cu cuvintele „o notificare a incidentului cibernetic care trebuie să conțină”;

se completează cu **alineatul (3')** cu următorul cuprins:

„(3¹) Prestatorul de servicii de încredere prezintă autorității competente notificarea menționată la alineatul (3), în ceea ce privește incidentele cibernetice cu impact semnificativ care afectează prestarea serviciilor sale de încredere, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care au luat cunoștință de incidentul cibernetic cu impact semnificativ.”;

alineatul (6), ultima propoziție, se completează în final cu textul „și, dacă e cazul, despre incidentul semnificativ”.

Se completează cu **alineatul (6¹)** cu următorul cuprins:

„(6¹) În cazul în care informarea publicului este necesară pentru a preveni un incident cibernetic cu impact semnificativ sau pentru a gestiona un astfel de incident în curs sau în cazul în care divulgarea informațiilor despre incidentul respectiv este în alt mod în interesul public, autoritatea competentă poate, după consultarea furnizorului de servicii în cauză, să informeze publicul cu privire la incidentul cibernetic cu impact semnificativ sau să solicite furnizorului de servicii să facă acest lucru. Autoritatea competentă poate informa publicul cu privire la incidentele cibernetice cu impact transfrontalier produse în alte state membre ale Uniunii Europene care au afectat Republica Moldova în condițiile prezentului alineat.”;

la **alineatul (7)**, propoziția a doua se exclude.

se completează cu **alineatul (7¹)**, cu următorul cuprins:

„(7¹) La solicitarea autorității competente, furnizorul de servicii este obligat să prezinte un raport intermediar care trebuie să conțină actualizări ale informațiilor deja prezentate în alerta timpurie și în notificare, precum și orice alte informații despre evoluția situației în procesul de gestionare a incidentului cibernetic cu impact semnificativ.”;

alineatul (8) va avea următorul cuprins:

„(8) Furnizorul de servicii este obligat, în termen de o lună de la transmiterea notificării conform alin.(3), să transmită autorității competente un raport final care să includă cel puțin următoarele informații:

a) descrierea detaliată a incidentului cibernetic, inclusiv a gravității și a impactului acestuia;

b) tipul de amenințare cibernetică sau cauza principală care ar fi putut declanșa incidentul cibernetic;

c) măsurile de atenuare aplicate și în proces de aplicare;

d) dacă este cazul, impactul transfrontalier al incidentului cibernetic.

Dacă la expirarea termenului de o lună menționat în prezentul alineat incidentul cibernetic este în desfășurare, furnizorul de servicii prezintă autorității competente un raport de progres privind soluționarea incidentului cibernetic și un raport final în termen de o lună de la finalizarea soluționării incidentului cibernetic.”;

se completează cu **alineatele (8¹), (8²) și (8³)** cu următorul cuprins:

„(8¹) Furnizorii de servicii în realizarea obligațiilor de notificare prevăzute de prezentul articol, sunt obligați să informeze autoritatea competentă despre orice informație care îi permite acestuia să constate impactul transfrontalier al incidentului cibernetic. Simpla notificare nu constituie temei juridic pentru inițierea de către autoritatea competentă a unor acțiuni care ar supune furnizorul de servicii care notifică unei răspunderi sporite.

(8²) Atunci când incidentul cibernetic cu impact semnificativ afectează două sau mai multe state membre ale Uniunii Europene, autoritatea competentă informează, fără întârzieri nejustificate, statele membre ale Uniunii Europene afectate și Agenția Uniunii Europene pentru Securitate Cibernetică cu privire la incidentul cibernetic cu impact semnificativ. Aceste informații includ tipul de informații primite de către autoritatea competentă de la furnizorii de servicii în conformitate cu alineatele (1), (3), (3¹), (7¹) și (8).

(8³) Autoritatea competentă este responsabilă pentru asigurarea protecției intereselor de securitate și comerciale ale furnizorului de servicii, precum și confidențialitatea informațiilor furnizate de aceștia în realizarea obligațiilor de notificare, inclusiv în procesul de schimb transfrontalier de informații și cooperarea internațională.”;

alineatul 10 se abrogă;

alineatul (11) va avea următorul cuprins:

„(11) Atunci când funcția de centru guvernamental de răspuns la incidentele cibernetic este separat de autoritatea competentă, furnizorii de servicii persoane juridice de drept public notifică persoana juridică de drept public care exercită această funcție cu privire la incidentele cibernetic cu impact semnificativ în vederea îndeplinirii obligațiilor prevăzute de prezentul articol. Persoana juridică de drept public care exercită funcția de centru guvernamental de răspuns la incidentele cibernetic informează autoritatea competentă cu privire la incidentele cibernetic cu impact semnificativ în conformitate cu prevederile prezentului articol.”;

se completează cu **alineatul (11')** cu următorul cuprins:

„(11') Autoritatea competentă informează autoritățile publice competente în temeiul legislației privind protecția infrastructurii naționale critice și a legislației privind protecția antiteroristă a infrastructurii critice cu privire la incidente cibernetic cu impact semnificativ, incidente, amenințări cibernetic și incidente evitate la limită, notificate în conformitate cu prezentul articol și cu articolul 13 de către gestionarii de infrastructură critică națională sau de operatorii unui obiectiv al infrastructurii critice.”.

12. Articolul 13:

Alineatul (1) va avea următorul cuprins:

„(1) Pe lângă obligațiile de notificare prevăzute la articolul 12, în adresa autorității competente pot fi transmise notificări voluntare:

a) de către furnizorii de servicii în ce privește incidentele cibernetice care nu au un impact semnificativ, amenințările cibernetice și incidentele cibernetice evitate la limită;

b) de către alte persoane fizice și juridice, cu privire la incidentele cibernetice cu impact semnificativ, amenințările cibernetice și incidentele cibernetice evitate la limită.”;

la **alineatul (2)** textul „menționate la alin.(1) din prezentul articol și la art.12 alin.(10)” se substituie cu cuvântul „voluntare”, iar textul „de prezenta lege și actului aprobat potrivit art.12 alin.(9)” se substituie cu textul „pentru notificările obligatorii”;

la **alineatul (3)** textul „menționate la alin.(1) din prezentul articol și la art.12 alin.(10)” se substituie cu cuvintele „care o efectuează”.

13. Articolele 14, 15 și 16 se abrogă.

14. La articolul 17 alineatele (2) și (3) vor avea următorul cuprins:

„(2) Schimbul de informații prevăzut la alin. (1) se realizează în cadrul unor comunități ale furnizorilor de servicii și, după caz, ale prestatorilor lor de servicii și se pune în aplicare prin acorduri de schimb de informații în materie de securitate cibernetică, care trebuie să țină cont de caracterul potențial sensibil al informațiilor partajate. Acordurile de schimb de informații în materie de securitate cibernetică pot specifica elemente operaționale, inclusiv utilizarea platformelor TIC dedicate și a instrumentelor de automatizare, precum și conținutul și condițiile acestor acorduri. Autoritatea competentă facilitează instituirea unor astfel de acorduri și oferă suport furnizorilor de servicii în procesul de instituire și punere în aplicare a acestora.

(3) Modul de participare a persoanelor juridice de drept public în cadrul acordurilor de schimb de informații în materie de securitate cibernetică, inclusiv condițiile cu privire la informațiile puse la dispozițiile de către autoritatea competentă se stabilește de Guvern.”.

15. Articolul 19 va avea următorul cuprins:

„Articolul 19. Controlul de stat și asigurarea respectării legii

(1) Controlul de stat privind respectarea de către furnizorii de servicii a prezentei legi și a actelor normative adoptate în temeiul acesteia se exercită de către autoritatea competentă în conformitate cu prezenta lege și Legea nr.131/2012 privind controlul de stat.

(2) Prevederile prezentei legi care reglementează controlul de stat exercitat de autoritatea competentă se completează cu prevederile Legii nr.131/2012 privind controlul de stat. Dacă Legea 131/2012 privind controlul de stat nu conține prevederi aplicabile activităților desfășurate de autoritatea competentă în exercitarea controlului de stat și asigurarea respectării legii sau prevederile acesteia sunt insuficiente, prevederile prezentei legi se completează cu prevederile Codului administrativ.

(3) Prevederile Legii nr.131/2012 privind controlul de stat se aplică în măsura în care nu contravin prevederilor prezentei legi.

(4) Autoritatea competentă prioritizează exercitarea controlului de stat în baza unei abordări bazate pe riscuri, asigurând realizarea controlului de stat și aplicarea măsurilor de asigurare a respectării legii în mod efectiv, proporțional, cu efect de descurajare, precum și ținând cont de circumstanțele fiecărui caz în parte.

(5) În exercitarea funcției de control de stat în privința furnizorilor de servicii, autoritatea competentă este împuternicită:

a) să efectueze controale la fața locului și/sau prin solicitare directă a documentației de la furnizorul de servicii;

b) să dispună efectuarea unor audituri de securitate periodice și specifice în privința furnizorului de servicii de către un organism independent;

c) să efectueze controale inopinate, inclusiv în cazurile justificate de un incident cibernetic cu impact semnificativ sau de o încălcare a prezentei legi de către furnizorul de servicii în cauză;

d) să efectueze scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor, după caz cu cooperarea furnizorului de servicii în cauză;

e) să solicite, precizând scopul și conținutul, acces la date, la documente și la orice informații necesare pentru îndeplinirea atribuțiilor de control de stat, inclusiv la informații necesare pentru a evalua măsurile de gestionare a riscurilor în materie de securitate cibernetică adoptate de furnizorul de servicii în cauză, inclusiv politicile de securitate cibernetică documentate, precum și dovezi privind punerea în aplicare a politicilor de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și mijloacele de probă care stau la baza acestor audituri.

(6) Auditurile de securitate specifice, menționate la alin. (5) litera b), trebuie să se bazeze pe evaluări ale riscurilor efectuate de autoritatea competentă sau de furnizorul de servicii auditat sau pe alte informații disponibile legate de riscuri. Raportul auditului de securitate specific se remite fără întârzieri nejustificate autorității competente. Costurile auditului de securitate specific sunt suportate de furnizorul de servicii, dacă autoritatea competentă nu decide altfel în cazurile justificate corespunzător. Condițiile și cazurile în care autoritatea competentă poate dispune efectuarea unor audituri de securitate specifice, situațiile în care autoritatea competentă rambursează furnizorului de servicii costurile auditului de securitate specific, precum și modul de rambursare a acestor costuri se stabilesc de Guvern.

(7) În exercitarea competenței de asigurare a respectării legii, autoritatea competentă:

a) emite avertismente cu privire la încălcările prezentei legi și a actelor normative adoptate în temeiul acesteia;

b) înaintează furnizorilor de servicii prescripții:

1) privind remedierea deficiențelor identificate sau încălcărilor prezentei legi, precum și încetarea conduitei ilegale și abținerea de la o astfel de conduită sau de la repetarea acesteia;

2) privind măsurile ce urmează a fi puse în aplicare pentru a preveni sau soluționa un incident cibernetic, precum și termene-limită pentru punerea în aplicare a acestor măsuri și pentru raportarea privind punerea acestora în aplicare;

3) privind modul și perioada în care urmează a fi asigurată respectarea obligațiilor privind implementarea măsurilor de securitate și îndeplinirea obligațiilor de notificare stabilite de prezenta lege;

4) privind informarea persoanelor, cărora le furnizează servicii sau pentru care desfășoară activități, care ar putea fi afectate de o amenințare cibernetică semnificativă, cu privire la natura amenințării și la măsurile de protecție sau de remediere pe care acestea le pot lua ca răspuns la amenințarea respectivă;

5) privind punerea în aplicare, într-un termen rezonabil, a recomandărilor formulate în urma unui audit de securitate;

6) privind modalitățile specifice prin care furnizorul de servicii urmează să facă publice anumite aspecte ale încălcărilor prezentei legi și a actelor normative adoptate în temeiul acesteia;

c) restricționează utilizarea ori accesul la o rețea sau un sistem informatic;

d) desemnează, pe o perioadă determinată, o persoană responsabilă cu sarcini în domeniul executării activităților de control și de inspectare a procesului de implementare a obligațiilor stabilite de prezenta lege;

e) aplică sancțiuni contravenționale potrivit prevederilor Codului contravențional;

f) aplică amenzi pentru încălcările prezentei legi și a actelor normative adoptate în temeiul acesteia;

(8) Pentru contracararea unei amenințări cibernetice semnificative imediate asupra securității rețelelor și sistemelor informatice, pentru eliminarea sau atenuarea consecințelor unui incident cibernetic, autoritatea competentă poate accesa o rețea sau un sistem informatic și restricționa utilizarea ori accesul la rețeaua sau sistemul informatic respectiv dacă sunt îndeplinite cumulativ următoarele condiții:

a) incidentul cibernetic compromite ori dăunează securității altei rețele sau altui sistem informatic;

b) administratorul rețelei sau sistemului informatic nu poate în timp util să contracareze amenințarea cibernetică semnificativă sau să elimine perturbarea gravă provocată de incidentul cibernetic;

c) nu este posibilă contracararea amenințării cibernetice semnificative sau eliminarea perturbării grave provocate de incidentul cibernetic prin aplicarea altei măsuri;

d) prin contracararea amenințării cibernetice semnificative sau prin eliminarea perturbării grave provocate de incidentul cibernetic nu este cauzat un prejudiciu disproportionat.

Autoritatea competentă notifică, fără întârzieri nejustificate și nu mai târziu de 24 de ore, cu privire la aplicarea măsurii prevăzute de prezentul alineat, utilizatorii, autoritatea publică care realizează politica de stat în domeniul în care furnizorul de servicii vizat prestează serviciul respectiv și, după caz, autoritatea cu funcții de reglementare a pieței din domeniul respectiv.

(9) În ce privește furnizorii esențiali de servicii, dacă măsurile prevăzute la alin. (7) lit. a) și lit. b) punctele 1) – 3) și 5) sunt ineficiente, autoritatea competentă stabilește un termen suplimentar în care furnizorul esențial de servicii este obligat să remedieze deficiențele sau să se conformeze cerințelor stabilite în prescripția emisă de autoritatea competentă. Dacă furnizorul esențial de servicii nu remediază deficiențele sau nu se conformează cerințelor în termenul suplimentar stabilit în temeiul prezentului alineat, autoritatea competentă:

a) în cazul încălcărilor foarte grave și de riscuri iminente , poate emite o prescripție în calitate de măsură restrictivă în sensul art. 30 din Legea nr. 131/2012 privind controlul de stat, de suspendare a activității furnizorului respectiv de servicii, în parte sau, dacă nu e posibilă disjungerea activităților respective, în totalitate în conformitate și în condițiile stabilite de Legea nr. 131/2012 privind controlul de stat, până la remedierea deficienței și/sau asigurarea conformității cu cerințele prescrise;

b) în cazul încălcărilor grave și foarte grave, poate solicita organelor de conducere ale furnizorului esențial de servicii suspendarea contractului individual de muncă cu persoana fizică care exercită responsabilități de conducere la nivel de director executiv sau de reprezentant legal al furnizorului de servicii sau impunerea unor interdicții acestor persoane în exercitarea responsabilităților respective, până la remedierea deficienței și/sau asigurarea conformității cu cerințele prescrise.

Măsurile prevăzute la prezentul alineat nu se aplică persoanelor juridice de drept public.

(10) La aplicarea măsurilor de asigurare a respectării prezentei legi, prevăzute la alineatele (7) și (9), autoritatea competentă ia în considerare circumstanțele fiecărui caz în parte, în mod special:

a) gravitatea încălcării și importanța cerințelor legale încălcate;

b) durata încălcării;

c) încălcările anterioare relevante comise de furnizorul de servicii în cauză;

d) prejudiciile materiale sau non-materiale cauzate, inclusiv pierderile financiare sau economice, efectele asupra altor servicii și numărul de utilizatori afectați;

e) intenție sau imprudență din partea autorului încălcării;

f) măsurile luate de furnizorul de servicii pentru a preveni sau a atenua prejudiciile materiale sau non materiale;

g) aderarea furnizorului de servicii la coduri de conduită aprobate sau la mecanisme de certificare aprobate;

h) măsura în care persoanele responsabile cooperează cu autoritatea competentă.

(11) Sunt considerate încălcări grave ale prezentei legi și ale actelor normative adoptate în temeiul acesteia următoarele încălcări:

a) încălcările repetate;

b) neîndeplinirea obligației de notificare a incidentului cibernetic cu impact semnificativ, stabilită la articolul 12 alin. (1) sau neaplicarea măsurilor de securitate necesare pentru răspunsul la incidentul cibernetic cu impact semnificativ;

c) neremedierea deficiențelor în urma instrucțiunilor obligatorii prescrise de autoritatea competentă;

d) obstrucționarea auditurilor sau a activităților de monitorizare dispuse de autoritatea competentă în urma constatării unei încălcări;

e) furnizarea de informații false sau vădit denaturate în ceea ce privește implementarea măsurilor de securitate în conformitate cu articolul 11 sau realizarea obligațiilor de notificare în conformitate cu articolul 12.

Aceleași încălcări sunt considerate foarte grave dacă corespund cerințelor stabilite la art. 5¹ alin. (3) lit. c) din Legea nr. 131/2012 cu privire la controlul de stat.

(12) În privința furnizorilor importanți de servicii, autoritatea competentă exercită împuternicirile prevăzute la alin. (5), cu excepția literei b) în ce privește caracterul periodic al auditurilor de securitate specifice, precum și aplică măsurile de asigurare a respectării legii prevăzute la alin. (7), cu excepția celor de la lit. b) pct. 2) și lit. d), doar atunci când dispune de dovezi, indicii sau informații, inclusiv rezultate din alte activități desfășurate de autoritatea competentă în exercitarea competenței sale, furnizate de alte autorități și instituții publice, de persoane fizice sau juridice ori disponibile în surse publice, care ar sugera potențiale încălcări ale prezentei legi (exercitarea ex-post al controlului de stat).

(13) Autoritatea competentă informează autoritățile publice cu funcții de supraveghere și control în temeiul Legii nr.120/2017 cu privire la prevenirea și combaterea terorismului și a Legii nr.223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale atunci când își exercită competențele de control de stat și aplică măsuri de asigurare a respectării legii în privința unui operator al unui obiectiv al infrastructurii critice sau, respectiv, în privința unui gestionar de infrastructură critică națională. După caz, autoritățile publice menționate la prezentul alineat pot solicita

autorității competente exercitarea competențelor de control de stat și de asigurare a respectării legii în legătură cu un operator al unui obiectiv al infrastructurii critice sau, respectiv, cu un gestionar de infrastructură critică națională.

(14) Autoritatea competentă cooperează cu Banca Națională a Moldovei și cu Comisia Națională a Pieței Financiare în exercitarea competenței sale de control de stat și de aplicare a măsurilor de asigurare a respectării legii în privința furnizorilor de servicii din sectorul bancar și sectorul infrastructurilor pieței financiare.

(15) Autoritatea competentă informează Forumul de supraveghere instituit în temeiul articolului 32 alineatul (1) din Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 atunci când exercită competența de control de stat și de asigurare a respectării legii în privința unui furnizor de servicii, care este desemnat ca fiind un furnizor terț de servicii de tehnologie a informației și comunicații critice în temeiul articolului 31 din Regulamentul respectiv.

(16) Autoritatea competentă asigură o cooperare strânsă cu autoritățile de supraveghere în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, fără a aduce atingere competențelor și sarcinilor autorităților de supraveghere în temeiul regulamentului respectiv.”.

16. Se completează cu articolele 19¹, 19² și 19³ cu următorul cuprins:

„Articolul 19¹. Amenda pentru încălcările prezentei legi

(1) Autoritatea competentă aplică amenzile în completare față de oricare dintre măsurile prevăzute la art. 19 alin. (7) literele (a) și b) și alin. (9).

(2) Atunci când decide aplicarea unei amenzi și quantumul acesteia, în fiecare caz în parte autoritatea competentă ține cont în mod corespunzător cel puțin de elementele prevăzute la art. 19 alin. (10).

(3) Pentru încălcarea de către furnizorul esențial de servicii a cerințelor prevăzute la art. 11 alin. (1), (2), (2²), (2³) sau (3) ori la art. 12 alin. (1), (3), (3¹), (4), (6), (7¹), (8) sau (8¹), autoritatea competentă aplică amendă de până la 2000000 lei sau de până la 2% din cifra totală de afaceri realizată în anul anterior aplicării amenzii, luându-se în considerare valoarea cea mai mare dintre acestea.

(4) Pentru încălcarea de către furnizorul important de servicii a cerințelor prevăzute la art. 11 alin. (1), (2), (2²), (2³) sau (3) ori la art. 12 alin. (1), (3), (3¹), (4), (6), (7¹), (8) sau (8¹),

autoritatea competentă aplică amendă de până la 1400000 lei sau de până la 1,4% din cifra totală de afaceri realizată în anul anterior aplicării amenzii, luându-se în considerare valoarea cea mai mare dintre acestea.

(5) În cazul în care cifra totală de afaceri realizată în anul anterior aplicării amenzii nu este înregistrată, se ia în considerare cea mai recentă cifră de afaceri anuală a întreprinderii, anterioară aplicării amenzii.

(6) Autoritatea competentă constată încălcările prevăzute de prezentul articol în conformitate cu procedura stabilită de Legea nr. 131/2012 privind controlul de stat și aplică amenzi în cuantumul prevăzut de alineatele (3) sau (4) prin procesul verbal cu privire la efectuarea controlului de stat doar pentru încălcările grave și foarte grave.

(7) Furnizorii de servicii, în privința cărora au fost aplicate amenzi în conformitate cu prevederile prezentei legi pot contesta deciziile autorității competente de aplicare a amenzilor respective în conformitate cu prevederile art. 30 din Legea nr. 131/2012 privind controlul de stat.

(8) Amenzile prevăzute de prezentul articol nu se aplică persoanelor juridice de drept public.

Articolul 19². Încălcări care implică o încălcare a securității datelor cu caracter personal

(1) În cazul în care, în exercitarea controlului de stat sau al aplicării măsurilor de asigurare a respectării legii, autoritatea competentă ia cunoștință de faptul că o încălcare de către furnizorul de servicii a articolelor 11 și 12 poate atrage după sine o încălcare a securității datelor cu caracter personal, astfel cum aceasta este definită la art. 4 din Legea nr. 195/2042 privind protecția datelor cu caracter personal, care trebuie notificată în conformitate cu art. 33 din aceeași lege, aceasta informează fără întârzieri nejustificate Centrul Național pentru Protecția Datelor cu Caracter Personal.

(2) În cazul în care Centrul Național pentru Protecția Datelor cu Caracter Personal aplică o amendă în conformitate cu art. 88 din Legea nr. 195/2025 privind protecția datelor cu caracter personal, autoritatea competentă nu aplică o amendă pentru o încălcare a prezentei legi în conformitate cu art. 19¹ rezultată în urma aceluiași comportament care a făcut obiectul amenzii aplicate de Centrul Național pentru Protecția Datelor cu Caracter Personal. Autoritatea competentă poate aplica măsurile de asigurare a respectării legii prevăzute la art. 19 alin. (7) literele a) și b) și alin. (9) în privința furnizorului de servicii respectiv.

(3) În cazul în care autoritatea de supraveghere competentă în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE

(Regulamentul general privind protecția datelor) este stabilită într-un alt stat membru decât autoritatea competentă, autoritatea competentă informează Centrul Național pentru Protecția Datelor cu Caracter Personal cu privire la potențiala încălcare a securității datelor cu caracter personal menționată la alin. (1).

Articolul 19³. Asistență reciprocă

(1) Dacă un furnizor de servicii , prestează servicii în mai multe state membre ale Uniunii Europene sau prestează servicii în unul sau mai multe state membre ale Uniunii Europene, iar rețeaua și sistemele sale informatice sunt situate în unul sau mai multe alte state membre ale Uniunii Europene, autoritatea competentă cooperează și oferă asistență reciprocă, după necesitate, celorlalte autorități competente, desemnate sau stabilite în statele membre în cauză ale Uniunii Europene în temeiul art. 8 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 .

(2) În exercitarea competenței de cooperare și asistență reciprocă conform alineatului (1), autoritatea competentă:

a) atunci când exercită controlul de stat sau aplică măsuri de asigurare a respectării legii în privința unei persoane menționate la alineatul (1), informează și consultă, prin intermediul punctului unic de contact, autoritățile competente din celelalte state membre ale Uniunii Europene în cauză cu privire la măsurile luate;

(b) poate solicita unei alte autorități competente din statele membre ale Uniunii Europene să ia măsuri de supraveghere sau de asigurare a respectării legii;

(c) la primirea unei cereri motivate din partea unei autorități competente din statele membre ale Uniunii Europene, acordă asistență acesteia proporțional cu resursele de care dispune, astfel încât exercitarea controlului de stat sau măsurile de asigurare a respectării legii să poată fi puse în aplicare într-un mod eficace, eficient și consecvent.

(3) Asistența reciprocă menționată la alin. (2) litera (c) poate acoperi cererile de informații și măsurile de control, inclusiv cererile de efectuare a unor controale la fața locului sau prin solicitare directă a documentației ori a unor audituri de securitate specifice.

(4) Autoritatea competentă nu poate refuza o cerere de asistență, cu excepția următoarelor cazuri:

a) dacă nu are competența legală de a furniza asistența solicitată;

b) asistența solicitată nu este proporțională cu sarcinile de control ale autorității competente;

c) cererea privește informații sau implică activități care, dacă ar fi divulgate sau desfășurate, ar fi contrare intereselor esențiale ale Republicii Moldova de securitate națională, siguranță și ordine publică sau apărare națională.

(5) Înainte de a refuza o cerere de asistență, autoritatea competentă consultă celelalte autorități competente în cauză, precum și, la cererea unuia dintre statele membre ale Uniunii Europene în cauză, Comisia Europeană și Agenția Uniunii Europene pentru Securitate Cibernetică.

(6) Atunci când e necesar, autoritatea competentă poate desfășura activități comune de control cu autoritățile competente din alte state membre ale Uniunii Europene, în conformitate cu procedurile operaționale agreeate de comun acord.

(7) Atunci când primește o cerere de asistență reciprocă referitoare la un furnizor de servicii DNS, un registru de nume TLD, un furnizor de servicii de înregistrare a numelor de domenii, un furnizor de servicii de cloud computing, un furnizor de servicii de centre de date, un furnizor de rețele de furnizare de conținut, un furnizor de servicii gestionate, un furnizor de servicii de securitate gestionate, un furnizor de piețe online, un furnizor de motoare de căutare online sau un furnizor de platforme de servicii de socializare în rețea, autoritatea competentă poate, în limitele acestei cereri, să ia măsurile corespunzătoare de control și de asigurare a respectării legii în privința furnizorului respectiv de servicii, dacă acesta prestează servicii sau deține o rețea sau un sistem informatic pe teritoriul Republicii Moldova.”

17. Articolul 20 va avea următorul cuprins:

„Articolul 20. Protecția datelor cu caracter personal

(1) În executarea prevederilor prezentei legi subiecții acesteia prelucrează datele cu caracter personal în măsura necesară pentru scopurile prezentei legi și în conformitate cu legislația privind protecția datelor cu caracter personal.

(2) Prelucrarea datelor cu caracter personal în temeiul prezentei legi de către furnizorii de rețele publice de comunicații electronice sau de către furnizorii de servicii de comunicații electronice accesibile publicului se efectuează în conformitate cu legislația privind protecția datelor cu caracter personal și cea privind comunicațiile electronice.”.

Art. III – Legea nr. 72/2025 comunicațiilor electronice (Monitorul Oficial al Republicii Moldova, 2025, nr. 226-228 art. 266) se modifică după cum urmează:

1. La articolul 3:

alineatul (4), cuvintele „Registratorul național” se substituie cu textul „Registratorul național al domeniului național de nivel superior ".md (în continuare – Registratorul național)”;

alineatul (5), textul „al domeniului național de nivel superior ".md"" se exclude;

2. Se completează cu alineatele (5¹), (5²), (5³) și (5⁴), cu următorul cuprins:

„(5¹) Pentru a contribui la securitatea, stabilitatea și reziliența sistemului de nume de domenii (DNS), Registratorul național și furnizorii de servicii de înregistrare a numelor de

domenii, astfel cum sunt definiți la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică, sunt obligați să colecteze și să mențină date exacte și complete privind înregistrarea numelor de domenii în Registrul numelor din domeniul național de nivel superior ".md", cu diligența necesară, în conformitate cu cadrul normativ național în materie de protecție a datelor cu caracter personal.

(5²) Registrul numelor din domeniul național de nivel superior ".md" trebuie conțina informațiile necesare pentru identificarea și contactarea titularilor numelor de domenii și a punctelor de contact care administrează numele de domenii în domeniul național de nivel superior ".md". Informațiile respective trebuie să includă cel puțin:

- a) numele de domeniu;
- b) data înregistrării;
- c) numele, adresa de e-mail și numărul de telefon de contact ale solicitantului înregistrării;
- d) adresa de e-mail și numărul de telefon de contact ale punctului de contact care administrează numele de domeniu în cazul în care acestea sunt diferite de cele ale solicitantului înregistrării.

(5³) Registratorul național și furnizorii de servicii de înregistrare a numelor de domenii sunt obligați:

- a) să dispună de politici și proceduri, inclusiv proceduri de verificare, care să asigure că Registrul numelor din domeniul național de nivel superior ".md" conține informații exacte și complete și să le pună la dispoziția publicului;
- b) să pună la dispoziția publicului, fără întârzieri nejustificate după înregistrarea unui nume de domeniu, datele de înregistrare a numelui de domeniu care nu sunt date cu caracter personal;
- c) să ofere acces la anumite date de înregistrare a numelor de domenii în baza unor cereri legale și justificate în mod corespunzător ale solicitanților de acces legitimi, în conformitate cu cadrul normativ în materie de protecție a datelor cu caracter personal;
- d) să răspundă fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la primirea cererilor de acces menționate la lit. c);
- e) să dispună de politici și proceduri de divulgare a datelor cu caracter personal și să le pună la dispoziția publicului.
- f) să asigure o cooperare reciprocă efectivă și eficientă în realizarea obligațiilor prevăzute de prezentul alineat, inclusiv pentru a evita suprapuneri în colectarea datelor de înregistrare a numelor de domenii.”;

3. **La articolul 8 alineatul (2) litera i) se abrogă.**

Art. IV – (1) Prezenta lege intră în vigoare la data publicării, cu excepția prevederilor art. 3 alin. (12), art. 4³, art. 7 alin. (4) punctele 7²) și 7³), art. 7¹, art. 12 alin. (6¹) propoziția a

doua, alin. (8²), art. 19 alin. (15), art. 19¹, art. 19² alin. (3), art. 19³, care intră în vigoare la data intrării în vigoare a tratatului de aderare a Republicii Moldova la Uniunea Europeană.

(2) Obligațiile de notificare stabilite la articolul 7¹ alin. (1) din Legea nr. 48/2023 privind securitatea cibernetică, cu modificările ulterioare, urmează a fi realizate pentru prima dată în termen de o lună de la data intrării în vigoare a tratatului de aderare a Republicii Moldova la Uniunea Europeană și ulterior, conform termenelor stabilite de articolul respectiv. Curgerea termenelor menționate la articolul 7¹ alin.(1) literele a), b) și g) începe după expirarea termenului de o lună prevăzut de prezentul alineat.

(3) Obligația de informare prevăzută la art. 4³ alin. (1) se realizează inițial în termen de 3 luni de la data intrării în vigoare a prevederilor art. 4³ stabilită la alin. (1).

(4) Guvernul, în termen de 12 luni din data publicării prezentei legi va aduce actele sale normative în concordanță cu prezenta lege.

NOTA DE FUNDAMENTARE
la proiectul de lege pentru modificarea unor acte normative
(armonizarea legislației naționale la Directiva NIS2)

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
Proiectul de lege a fost elaborat de Ministerului Dezvoltării Economice și Digitalizării (MDED), cu suportul proiectului „Îmbunătățirea rezilienței cibernetice în țările Parteneriatului estic”
2. Condițiile ce au impus elaborarea proiectului actului normativ
2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ
În mod specific, proiectul de lege este elaborat în vederea realizării pct. 48, Clusterul 3: Competitivitate și Creștere Incluzivă, Capitolul 10: Societatea informațională și mass-media din Programul Național de Aderare al Republicii Moldova la Uniunea Europeană (2025-2029), aprobat prin Hotărârea Guvernului nr. 306/2025¹. Conform punctului respectiv, MDED este responsabil de elaborarea proiectului de lege pentru modificarea Legii nr. 48/2023 privind securitatea cibernetică, având ca obiectiv continuarea armonizării legislației naționale în acest domeniu la Directiva NIS2². Potrivit Programului proiectul de lege urmează a fi aprobat de către Guvern și remis Parlamentului spre examinare către luna septembrie a anului curent. În același timp inițiativa în cauză se înscrie în cadrul general de realizare a obiectivelor generale și/sau specifice, precum și a viziunii strategice de ansamblu a țării în domeniul securității cibernetice, prevăzute în următoarele documente de politici: 1. Concepția securității informaționale, aprobată prin Legea nr. 299/2017³, care oferă 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, ca 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; 2. Programul de activitate al Guvernului “UE, pace, dezvoltare”, aprobat prin Hotărârea Parlamentului nr.269/2025⁴, care în contextul priorității sectoriale Guvernare eficientă are ca prioritate consolidarea securității cibernetice și a infrastructurii IT critice; 3. Strategia securității naționale a Republicii Moldova, aprobată prin Hotărârea Parlamentului nr.391/2023⁵, având ca direcție de acțiune securitatea și reziliența cibernetică, stabilește un set de măsuri, dintre care în mod special menționăm elaborarea cadrului normativ, strategic și de cooperare instituțională care să delimiteze responsabilitățile și contribuția fiecărei instituții; consolidarea dialogului și a cooperării în domeniul cibernetic cu UE și participarea și/sau alinierea la normele UE în domeniul reglementării tehnologiilor transformative;

¹ https://www.legis.md/cautare/getResults?doc_id=152627&lang=ro

² DIRECTIVA (UE) 2022/2555 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555>

³ https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro

⁴ https://www.legis.md/cautare/getResults?doc_id=151470&lang=ro

⁵ https://www.legis.md/cautare/getResults?doc_id=141253&lang=ro

4. **Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030** ⁶, aprobată prin Hotărârea Guvernului 650/2023: unul dintre obiectivele acesteia este crearea unui mediu digital accesibil, sigur și incluziv, având ca scop asigurarea unei creșteri a nivelului de reziliență cibernetică a entităților-cheie din Republica Moldova.

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

La data de 28 aprilie 2023 a fost publicată **Legea nr. 48/2023 privind securitatea cibernetică**, care a intrat în vigoare la data de 1 ianuarie 2025. Legea constituie cadrul normativ general primar în domeniul securității cernetice. 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, determinând cerințele generale necesare pentru asigurarea unei protecții efective a drepturilor și intereselor persoanelor fizice și juridice, activităților critice și a serviciilor esențiale pentru societate și economie, precum și ale intereselor naționale ale Republicii Moldova.

Principalele concepte reglementate de legea respectivă derivă din algoritmul de reglementare a aspectelor instituționale, de coordonare, cooperare, schimb de informații și, nu în ultimul rând, de asigurare a securității cernetice la nivelul infrastructurii informaționale critice oferite de Directiva NIS2 și constau în principal în următoarele:

a) **instituirea și desemnarea unei autorități competente în domeniul securității cernetice**, care include în competența sa și funcția de **echipă națională de răspuns la incidentele de securitate cernetică (CSIRT)** și **cea de punct național unic de contact**, de rând cu alte funcții precum coordonarea interacțiunii la nivel național și internațional, schimbul de informații, stimularea și facilitarea cooperării, monitorizare a spațiului cernetic național, identificare și analiză a amenințărilor cernetice, vulnerabilităților și incidentelor cernetice la nivel național, coordonarea răspunsului la incidentele și crizele cernetice, precum și exercitarea supravegherii și controlului de stat;

b) definirea **cadrului general strategic de coordonare și cooperare**, prin împuternicirea Guvernului să instituie un Consiliu coordonator în domeniul securității cernetice și să prezinte Parlamentului spre aprobare a Strategia națională privind securitatea cernetică;

c) determinarea cadrului general, instituțional și funcțional, în **gestionarea crizelor cernetice**, inclusiv prin atribuirea rolului de autoritate publică responsabilă de gestionarea crizelor cernetice autorității competente în domeniul securității cernetice a aprobarea unui plan național de răspuns la incidentele cernetice și crizele cernetice;

d) **stabilirea obligațiilor de asigurare a securității cernetice** pentru furnizorii de servicii publici și privați, în special în ce privește cerințele privind măsurile de securitate a rețelelor și sistemelor informatice ce urmează a fi implementate de către aceștia, precum și instituirea unui mecanism obligatoriu de notificare a incidentelor cernetice semnificative de către furnizorii de servicii,;

e) crearea condițiilor legale necesare pentru asigurarea implementării mecanismelor de **notificare voluntară a incidentelor** cernetice de orice persoană, precum și crearea și asigurarea funcționării adecvate a **mecanismelor de cooperare eficientă la nivel național și internațional**, inclusiv prin difuzarea de către autoritatea competentă întregii societăți și în mod deosebit furnizorilor de servicii în sectoarele și subsectoarele critice, a informațiilor relevante, a avertizărilor și alertelor, precum și a celor mai bune practici internaționale, etc.

Pe parcursul anilor 2023-2025 au fost elaborate și adoptate actele normative care au avut ca obiectiv general să asigure punerea în aplicare a Legii nr. 48/2023 și, implicit, să continue procesul

de armonizare a legislației naționale la legislația UE, în particular la prevederile Directivei NIS2. Astfel în perioada respectivă au fost adoptate următoarele acte normative:

a) *Legea nr.58/2024 pentru modificarea unor acte normative*, prin care cadrul normativ primar a fost adus în concordanță cu Legea nr. 48/2023, în mod specific, pe de o parte, asigurând interconexiunea dintre normele Legii nr. 48/2023 și cele din legile sectoriale care reglementează activitatea furnizorilor de servicii și eliminarea/revizuirea unor prevederi care ar putea genera interpretări echivoce sau contradictorii în procesul aplicării legii, iar, pe de altă parte, finalizarea instituirii cadrului normativ primar necesar implementării modelului de guvernare în domeniul securității cibernetice la nivel național, prevăzut de Legea nr 48/2023, și anume definirea statutului juridic al autorității competente în domeniul securității cibernetice;

b) *Hotărârea Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică*, care determină statutul juridic al Agenției pentru Securitate Cibernetică (ASC) determinând locul și rolul acestei autorități publice în sistemul administrativ guvernamental. ASC este o autoritate administrativă în subordinea MDED, responsabilă de implementarea politicilor publice ale Guvernului în domeniul securității cibernetice, inclusiv exercitarea supravegherii și controlului de stat în acest domeniu.

c) *Hotărârea Guvernului nr. 333/2024 cu privire la instituirea, organizarea și funcționarea Consiliului coordonator în domeniul securității cibernetice*: Consiliul este un organ consultativ care are misiunea de planificare și coordonare, la nivel strategic și operațional, a politicilor în domeniul securității cibernetice. În fapt Consiliul ar trebui să devină o platformă de coordonare și cooperare dintre principalii actori statali responsabili de realizarea politicii de stat în domenii convergente domeniului securității cibernetice.

d) *Hotărârea Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii* este actul normativ care în principiu finalizează instituirea cadrului normativ necesar pentru determinarea domeniului de aplicare al Legii nr. 48/2023, prin stabilirea procedurii de identificare, a sectoarelor/subsectoarelor critice și a tipurilor de persoane juridice care cad sub incidența prevederilor acestei legi, clarificarea criteriilor specifice de identificare stabilite de lege, precum și a listei serviciilor esențiale, a valorilor de prag și indicatorilor necesari pentru aplicare acestor criterii specifice, reglementarea modului de ținere și actualizare a listei furnizorilor de servicii ca o cvasi etapă care încheie întregul proces de identificare.

e) *Hotărârea Guvernului 112/2025 pentru modificarea unor hotărâri ale Guvernului (modificarea actelor normative subsidiare în conformitate cu Legea nr.48/2023 privind securitatea cibernetică și legile conexe)*;

f) *Hotărârea Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice* este actul normativ fundamental care determină în mod detaliat cerințele privind măsurile de securitate a rețelelor și sistemelor informatice ce urmează a fi implementate de către furnizorii de servicii în vederea realizării obligațiilor prevăzute de art. 11 și art. 12 din Legea nr. 48/2023, precum și reglementează aspectele privind modul în care aceste cerințe urmează a fi puse în aplicare, inclusiv cele privind realizarea obligațiilor de notificare a incidentelor cibernetice. De asemenea, actul include reglementări privind modul de evaluare a echivalenței efectelor obligațiilor de asigurare a securității cibernetice care au ca obiectiv determinarea legii aplicabile furnizorilor de servicii în ce privește implementarea de către aceștia a cerințelor privind măsurile de securitate a rețelelor și sistemelor informatice pe care le deține, precum și reglementări ale procedurii de notificare a incidentelor cibernetice semnificative și condițiile de determinare a impactului semnificativ ale incidentului cibernetic pentru unele tipuri de furnizori de

servicii, în mod specific cei din sectorul de importanță critică ridicată al infrastructurii digitale și sectorul de importanță critică al furnizorilor digitali.

g) Hotărârea Guvernului 821/2025 cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026-2030 stabilește principalele obiective strategice în domeniul securității cibernetică precum sunt: consolidarea capacităților operaționale, inclusiv în caz de crize cibernetică; creșterea capacităților de reacție la crimele cibernetică, dezvoltarea competențelor și a culturii de securitate cibernetică în societate, îmbunătățirea cooperării internaționale.

h) Hotărârea Guvernului 822/2025 privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetică" și a Regulamentului cu privire la modul de ținere a Registrului de stat al incidentelor cibernetică

i) Hotărârea Guvernului 823/2025 pentru aprobarea Regulamentului cu privire la elaborarea, actualizarea și implementarea Planului național de răspuns la incidente cibernetică și crize în domeniul securității cibernetică dezvoltă cadrul normativ primar prevăzut de art. 9 din Legea nr. 48/2023 și stabilește cerințele pentru conținutul planului național de răspuns la incidentele cibernetică și crizele în domeniul securității cibernetică, procesul de elaborare, actualizare și implementare a acestui plan, atribuțiile autorităților și instituțiilor publice în acest proces, drepturile și obligațiile persoanelor juridice implicate în proces, precum și procedurile de interacțiune dintre acestea. Domeniul de aplicare al proiectului propus spre examinare se extinde asupra autorităților și instituțiilor publice cu competențe în gestionarea crizelor de securitate cibernetică, furnizorilor de servicii, esențiali sau importanți, asupra altor persoane juridice de drept privat, care deși nu sunt identificate în calitate de furnizori de servicii, totuși ar putea dispune de resurse pertinente procesului de răspuns la un incident cibernetic semnificativ sau de mare amploare care poate escalada într-o criză cibernetică.

j) Hotărârea Guvernului 824/2025 pentru aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetică stabilește cadrul normativ necesar clarificării rolului ASC în exercitarea funcției sale de coordonator al acestui proces, procedura de realizare a acestui proces precum și principalele cerințe pentru realizarea de către subiecții procesului de divulgare vulnerabilităților a drepturilor și obligațiilor care le revin conform legii, inclusiv cele ce derivă din implementarea cerințelor privind măsurile de securitate a rețelelor și sistemelor informatice.

k) Hotărârea Guvernului 825/2025 pentru aprobarea Regulamentului cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetică de către furnizorii de servicii în sectoarele critice stabilește cadrul normativ subsidiar de exercitare de către ASC a funcției sale legale de supraveghere și control de stat. Regulamentul stabilește două proceduri distincte privind exercitarea funcției de control în privința furnizorilor de servicii privați și în privința furnizorilor de servicii publici, precum și determină măsuri de supraveghere orientate spre evaluarea generală a nivelului de maturitate a furnizorilor de servicii.

Adoptarea Legii nr. 48/2023 a constituit o primă etapă în procesul de armonizare a cadrului normativ național la prevederile Directivei NIS2. Având ca obiectiv specific armonizarea legislației naționale la Legislația UE, procesul de elaborare, promovare și adoptare a Legii nr. 48/2023 privind securitatea cibernetică a avut loc într-o perioadă de tranziție în contextul legislativ al Uniunii Europene marcat de adoptarea Directivei NIS2 care a înlocuit prima Directivă NIS, adoptată în anul 2016. Spre deosebire de Republica Moldova, statele membre ale UE, la momentul adoptării Directivei NIS2, atinseseră un nivel destul de ridicat al securității infrastructurii informaționale critice prin punerea în aplicare a Directivei NIS1. Cu alte cuvinte, Directiva NIS2 a constituit pentru ele o nouă treaptă în procesul de asigurare a securității rețelelor și sistemelor informatice. Din această perspectivă, armonizarea legislației naționale la prevederile Directivei NIS2 a fost una parțială nu doar din pricina faptului că Republica Moldova nu este un stat membru al UE, ci și din punctul de vedere a necesității

de a asigura implementarea treptată a unor măsuri care, pe de o parte, să garanteze o creștere a nivelului de reziliență cibernetică a serviciilor esențiale, iar pe de altă parte să nu constituie o povară insurmontabilă pentru subiecții legii.

De asemenea, contextul în care a fost adoptată Legea nr. 48/2023 a fost influențat și de adoptarea concomitent cu Directiva NIS2, a alte două acte normative ale UE cu incidență domeniului reglementat de directiva respectivă și anume:

- Directiva (UE) 2022/2557⁷ a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (Directiva CER);

- Regulamentul (UE) 2022/2554⁸ al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (Regulamentul DORA).

Atât la etapa adoptării Legii nr. 48/2023 privind securitate cibernetică, cât și în prezent armonizarea legislației naționale trebuie concepută din perspectiva interconexiunilor dintre cele trei documente. Regulamentul DORA are un caracter de *lex specialis* față de prevederile conținute în Directiva NIS2⁹, iar interconexiunile¹⁰ *dintre Directiva CER și Directiva NIS2 urmează a fi abordate din perspectiva unor cadre de politici coerente pentru o coordonare consolidată și cooperare eficientă dintre autoritățile competente conform ambelor directive, inclusiv din punctul de vedere al raționalizării activităților de supraveghere și reducerii la minimum a sarcinii administrative.*¹¹ Desincronizarea acestor procese la nivel național, de transpunere a celor trei acte europene, a constituit și constituie în continuare un risc serios de implementare a prevederilor proiectului de lege. *Având în vedere importanța securității cibernetice pentru reziliența entităților critice și din motive de consecvență, ar trebui să se asigure o abordare coerentă, ori de câte ori este posibil, între Directiva CER și Directiva NIS2*¹². *După cum se subliniază în propunerea privind o abordare coordonată de către Uniune pentru consolidarea rezilienței infrastructurilor critice, având în vedere interconexiunile dintre securitatea cibernetică și securitatea fizică a operatorilor, este important ca lucrările de pregătire pentru transpunerea și aplicarea noii directive NIS2 să înceapă cât mai curând posibil și ca aceste lucrări în cadrul noii directive CER să progreseze, de asemenea, în paralel*¹³.

⁷ Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (Text cu relevanță pentru SEE) <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557>

⁸ Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (Text cu relevanță pentru SEE): <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022R2554>

⁹ Considerentul (28) din Directiva NIS2: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555>

¹⁰ Considerentul (30) din Directiva NIS2: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555>

¹¹ Considerentul 24 din Directiva CER evidențiază că este important ca statele membre să se asigure că cerințele prevăzute în prezenta directivă și în Directiva (UE) 2022/2555 sunt puse în aplicare în mod complementar și că entitățile critice nu sunt supuse unei sarcini administrative mai mari decât cea necesară pentru a atinge obiectivele prezentei directive și pe cele ale directivei menționate.

¹² Recitalul (9) al Directivei CER: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557>

¹³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0551&qid=1666351317270>

Astfel, Legea nr. 48/2023 a constituit o primă „iterație” în crearea unui model de guvernanta în domeniul securității cibernetice care să fie conform atât cerințelor stabilite de Directiva NIS2, cât și cerințelor stabilite de cadrul normativ național care reglementează modul de organizare și funcționare a administrației publice centrale de specialitate. Legea a asigurat o armonizare parțială, la nivelul normelor primare, a legislației naționale la Directiva NIS2. Pe de o parte armonizarea parțială a fost determinată de lipsa calității de stat membru al UE al Republicii Moldova, pe de altă parte această parțialitate în armonizare a rezultat din necesitatea unei abordări prudente în ce privește domeniul de aplicare al Legii (sectoare subsectoare critice și tipuri de organizații care ar urma să intre în acest domeniu) atât din cauza lipsei unor analize a riscurilor și determinării și evaluării interdependențelor de infrastructuri critice la nivel național care să reflecte o stare reală a lucrurilor și nu una formală, cât și din cauza desincronizării în promovarea inițiativelor de armonizare a legislației naționale la celelalte două acte UE: Directiva privind reziliența entităților critice și Regulamentul privind reziliența operațională digitală a sectorului financiar.

Deși la data de 22 august 2025 a fost publicată Legea nr. 223/2025 privind identificarea desemnarea și protecția infrastructurii critice naționale, act care parțial asigură armonizarea legislației naționale la Directiva CER, aceasta nu a soluționat problematica expusă. De asemenea, în lipsa unei legi prin care să se asigure aducerea în concordanță a cadrului normativ la această lege, în prezent la nivel național, cel puțin formal, există două mecanisme de identificare și protecție a infrastructurii critice: unul nou instituit prin legea în cauză și al doilea cel instituit prin Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului. Invocarea în acest caz a art. 7 alin. (3) din Legea nr. 100/2017 cu privire la actele normative nu rezolvă problematica conflictului dintre normele acestor legi, având în vedere caracterul special al normelor de protecție a infrastructurii critice în contextul prevenirii și combaterii terorismului.

De asemenea, după cum s-a menționat mai sus Legea nr. 48/2023 privind securitatea cibernetică a determinat în mod generic domeniul de aplicare al legii, lăsând la discreția Guvernului aprobarea mecanismelor necesare pentru realizarea identificării persoanelor care vor intra în acest domeniu de aplicare. Guvernul a soluționat această problematică prin adoptarea Hotărârii nr. 860/2024 cu privire la identificarea furnizorilor de servicii. Cu toate acestea pentru a asigura corespunderea reglementărilor în materie de elaborarea și promovare a actelor normative, în mod specific a principiilor legiferării domeniul de aplicare a Legii nr. 48/2023 necesită o clarificare la nivel primar cel puțin din perspectiva determinării sectoarelor și subsectoarelor critice, precum și a normelor juridice primare de separare în două categorii distincte a furnizorilor de servicii, și anume: esențiali și importanți.

Totodată, în procesul elaborării și promovării cadrului normativ guvernamental orientat spre punerea în aplicare a Legii nr. 48/2023 s-a constatat necesitatea completării legii cu norme juridice de natură primară în ce privește:

- procesul de identificare: mențiunea expresă în textul legii a sectoarelor și subsectoarelor critice; determinarea condițiilor de atribuire a furnizorilor de servicii la categoria de esențial sau important, precum și modul de întocmire a listei furnizorilor de servicii;
- modul de realizare de către furnizorii de servicii a obligațiilor de asigurare a securității cibernetice: guvernanta în implementarea cerințelor de gestionare a riscurilor; modul de raportare a incidentelor cibernetice semnificative și conținutul rapoartelor respective.

Un alt aspect important, constatat în procesul de identificare a furnizorilor de servicii, este faptul că în domeniul de aplicare a Legii nr. 48/2023 nu include și persoanele fizice care desfășoară activitatea de întreprinzător, adică întreprinderile individuale. Aceste întreprinderi, chiar dacă au o formă specifică de desfășurare a activității, care nu implică constituirea în una din formele de organizare prevăzute pentru persoanele juridice de drept privat, totuși ar putea desfășura activități, a căror

perturbare ar putea avea un impact semnificativ asupra continuității serviciilor esențiale sau asupra activităților societale sau economice critice, precum și asupra siguranței publice, a securității publice sau a sănătății publice.

O problemă pentru integritatea cadrului normativ în domeniul securității cibernetice o constituie lipsa mecanismelor de sancționare pentru nerespectarea prevederilor legii. În procesul promovării proiectului de lege pentru modificarea unor acte normative (aducerea în concordanță a cadrului normativ la prevederile Legii nr. 48/2023 privind securitatea cibernetică – Legea nr. 58/2024) au fost înaintate propuneri de completare a Codului Contravențional cu componente noi de contravenții. Însă în procesul avizării Ministerul Justiției a obiectat cu excluderea acestor propuneri din proiectul respectiv de lege și includerea lor într-un proiect de lege consolidat pentru modificarea Codului Contravențional care la acel moment se afla în proces de elaborare în cadrul Ministerului Justiției. Până în prezent modificările propuse la Codul Contravențional în ce privește instituirea răspunderii contravenționale pentru nerespectarea legislației în domeniul securității cibernetice nu au fost adoptate.

Cercul de subiecți interesați în intervenția propusă rămâne același determina prin analiza de impact la proiectul de lege privind securitatea cibernetică, și 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 finalizării procesului de armonizare a legislației naționale la Directiva NIS2, inclusiv clarificarea mecanismelor de cooperare și schimb de informații la nivel național și internațional, în particular la nivelul UE, precum și de coordonarea la nivel național a procesului de asigurare a securității cibernetice;

2. Persoanele juridice de drept public, inclusiv autoritățile administrației publice locale – categorie care prin efectul legii sunt identificate ca furnizori de servicii;

3. Întreprinderile (persoanele fizice și juridice de drept privat), inclusiv întreprinderile de stat, care cad sub incidența prevederilor proiectului de act normativ, adică care urmează, în baza mecanismului propus în proiectul de act normativ și dezvoltat în actele normative de punere în aplicare al acestuia, să fie identificate de autoritatea competentă ca furnizori de servicii, în funcție de sectoarele/subsectoarele în care aceștia prestează serviciile respective – din perspectiva clarificării aspectelor legate de procesul de identificare și a aspectelor privind obligațiile ce le revin în cadrul asigurării securității cibernetice;

4. Persoanele juridice de drept privat, altele decât cele menționate la pct. 3, care deținând rețele și sisteme informatice ce sunt utilizate în procesul de prestare a serviciilor, deși nu vor cădea sub incidența obligațiilor stabilite de actul normativ, totuși vor dispune de dreptul de notificare voluntară și participare la platforme și comunități privind schimbul de informații în materie de securitate cibernetică.

5. Utilizatorii finali ai serviciilor prestate de furnizorii de servicii 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.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Obiectivul general urmărit prin elaborarea și promovarea proiectului de lege propus spre examinare rămâne în principiu obiectivul general stabilit în analiza de impact la proiectul de lege privind securitatea cibernetică și anume:

1) Creșterea și menținerea unui nivel minim uniform de securitate a rețelelor și sistemelor informatice utilizate în prestarea serviciilor esențiale prin instituirea unor reglementări care să asigure că atât organizațiile din sectorul public, cât și cele din sectorul privat, care prestează astfel de servicii sau desfășoară activități importante pentru economie și societate în ansamblu sunt obligate să ia măsurile corespunzătoare pentru asigurarea securității cibernetice, inclusiv măsuri de gestionare a riscurilor și răspuns la incidentele cibernetice.

2) Îmbunătățirea climatului de cooperare la nivel național în domeniul asigurării securității rețelelor și sistemelor informatice dintre entitățile care prestează servicii esențiale atât din sectorul public, cât și din cel privat, precum și dintre aceste entități și autoritățile responsabile de asigurarea securității cibernetice la nivel național.

3) Crearea unor practici uniforme de gestionare a riscurilor și vulnerabilităților atât în sectorul public cât și în cel privat, astfel încât să se asigure o interoperabilitate corespunzătoare, în mod special în procesul de gestionare a crizelor.

În același context este necesar de evidențiat că un obiectiv convergent al contextului expus îl constituie necesitatea finalizării armonizării legislației naționale la legislația Uniunii Europene, în particular la Directiva NIS2.

Conținutul de bază al proiectului de lege vizează modificările la Legea nr. 48/2023 privind securitatea cibernetică. Modificările propuse la Codul Contravențional nr. 218/2008 și Legea nr. 72/2025 comunicațiilor electronice sunt modificări necesare pentru punerea în aplicare a viitoarelor prevederi ale Legii nr. 48/2023.

Astfel, **art. II** din proiectul de lege cuprinde modificările propuse la **Legea nr. 48/2023 privind securitatea cibernetică**:

La **punctul 1** se propune o redacție nouă a clauzei de armonizare. Potrivit Regulamentului privind armonizarea legislației Republicii Moldova cu legislația UE, aprobat prin Hotărârea Guvernului nr. 1171/2018, una din cerințele obligatorii pentru proiectul de act normativ care are ca scop transpunerea actelor juridice europene este ca acesta să conțină în mod obligatoriu clauza de armonizare, care indică gradul de transpunere a actului juridic european. Diferența dintre noua redacție și actuala constă în faptul că prin proiectul de lege practic se asigură, la nivelul cadrului normativ, *transpunerea integrală* a Directivei NIS2, cu următoarele excepții, determinate de necesitatea transpunerii altor acte ale UE în legislația națională:

a) Transpunere parțială: noțiunile de *serviciu de încredere*, *prestator de servicii de încredere*, *serviciu de încredere calificat* și *prestator de servicii de încredere calificat*, prevăzute la art. 6 punctele 24 – 27 din Directiva NIS2, sunt utilizate atât în Legea nr. 48/2023, dar și în proiectul de lege de față, în înțelesul original conferit acestora de Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere. Aceste noțiuni și definițiile lor au fost preluate, în procesul armonizării, din Regulamentul eIDAS¹⁴. Acesta din urmă însă prin Regulamentul (UE) 2024/1183¹⁵ (Regulamentul eIDAS 2.0) a fost modificat, noțiunile menționate mai sus suferind de asemenea modificări substanțiale. În prezent, MDDE, în comun cu Serviciul de Informații și Securitate, a elaborat și inițiat deja procesul de consultare publică și avizare a proiectului de lege privind identificarea electronică și

¹⁴ Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910>

¹⁵ Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R1183>

serviciile de încredere (proiectul cu nr. unic 395/MDED/SIS/2026) care are ca obiectiv transpunerea regulamentului menționat.

b) Norme UE netranspuse și opționale: Alineatul (10) din Directiva NIS2 exclude din domeniul de aplicare al acestei directive entitățile pe care statele membre le-au exclus din domeniul de aplicare al Regulamentului (UE) 2022/2554 în conformitate cu articolul 2 alineatul (4) din regulamentul respectiv. Articolul 2 alineatul (4) din Regulamentul (UE) 2022/2554 acordă statelor membre dreptul de a „*exclude din domeniul de aplicare al acestui regulament entitățile menționate la articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE¹⁶ care sunt situate pe teritoriile lor.*”. Articolul 2 alineatul (5) punctele 4-23 din Directiva 2013/36/UE exclude din domeniul de aplicare al acestei directive instituțiile de credit expres listate în conținutul alineatului respectiv. Prin urmare, transpunerea integrală a prevederilor alin. (10) din art. 2 al Directivei NIS2 va fi posibilă atunci când Republica Moldova va asigura transpunerea Regulamentului (UE) 2022/2554 și armonizarea legislației naționale la Directiva 2013/36/UE și dacă în conformitate cu Articolul 2 alineatul (4) din Regulamentul (UE) 2022/2554 va exclude din domeniul de aplicare al acestuia anumite entități financiare.

Cu referire la **punctul 2** prin care se propune o nouă redacție a art. 1 din Legea nr. 48/2023, această modificare este determinată de necesitatea clarificării obiectului de reglementare al legii. Aspectul fundamental în acest sens constă în faptul că Directiva NIS2 nu se axează doar pe protecția rețelelor și sistemelor informatice pe care se bazează furnizarea serviciilor esențiale, ci pe protecția organizațiilor, în întregul lor, de tipurile stabilite de anexele la Directiva respectivă. În mod elocvent acest aspect este dezvoltat și explicat în Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555 (Directiva NIS 2) 2023/C 328/02 (*n.n. – aplicarea legii sectoriale atunci când aceasta este echivalentă în efecte cu legea securității cibernetice*): „*Obligația prevăzută la articolul 21 alineatul (1) din Directiva (UE) 2022/2555 care impune entităților esențiale și importante să ia măsuri adecvate și proporționale de gestionare a riscurilor în materie de securitate cibernetică se referă la toate operațiunile și serviciile entității în cauză, nu numai la anumite active sau servicii informatice („IT”) critice pe care entitatea le furnizează...*”. Din perspectiva celor menționate, actuala redacție a art. 1 din Legea nr. 48/2023 restrânge sfera de aplicare a legii la obligații pentru furnizorii de servicii doar în ce privește implementarea cerințelor privind măsurile de gestionare a riscurilor la adresa securității rețelelor și sistemelor informatice care sunt critice sau esențiale pentru funcționarea societății, ceea ce nu corespunde conceptului noii directive de a avea o abordare multirisică și una care să cuprindă întreaga organizație.

Punctul 3 din art. II al proiectului de lege cuprinde modificări la art. 2 din Legea securității cibernetice, care definește noțiunile utilizate în textul legii.

Modificările propuse la noțiunile de *amenințare cibernetică semnificativă* și cea de *furnizor de servicii* sunt determinate de necesitatea includerii în domeniul de aplicare al legii și a persoanelor fizice care practică activitate de întreprinzător sau întreprinzătorilor individuali. Aceste modificări sunt în principiu conexe modificărilor de bază care sunt propuse a fi operate la art. 3 din legea nr. 48/2023. Prin urmare, argumentarea mai detaliată a extinderii domeniului de aplicare al legii este expusă în prezenta notă în continuare cu referire la punctul 4 din art. II al proiectului de lege. Totodată, din noțiunea de furnizor de servicii este exclusă referirea la faptul stabilirii de către Guvern a sectoarelor și subsectoarelor critice, având în vedere că în conformitate cu noul concept propus al domeniului de aplicare sectoarele și subsectoarele critice vor fi stabilite în lege.

¹⁶ Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02013L0036-20260111>.

În **subpunctele 3), 6), 9) și 12)**, se propune introducerea în textul legii a noțiunilor de „furnizor de servicii DNS”, „furnizor de servicii gestionate”, „furnizor de servicii de securitate gestionate”, „motor de căutare online”, „piață online” și „platformă de servicii de socializare în rețea”, „punct de schimb de internet (internet exchange point sau IXP)”, „registru de nume de domenii de prim nivel sau „registru de nume TLD” (top-level domain – TLD)”, „reprezentant”, „rețea de furnizare de conținut”, „serviciu de centre de date”, „serviciu de cloud computing”, „serviciu de securitate gestionat”, „serviciu digital”, „sistem de nume de domenii sau DNS”. Cu toate că aceste noțiuni derivă din prevederile Directivei NIS2 (art. 6), includerea acestora în Legea nr. 48/2023 nu este determinată de necesitatea transpunerii acestora în legislația națională. Noțiunile respective au fost deja definite în Regulamentul privind identificarea furnizorilor de servicii, aprobat prin Hotărârea Guvernului nr. 860/2023, care în principiu a asigurat transpunerea acestora în legislația națională. Cu toate acestea, completarea Legii nr 48/2023 este determinată de necesități practice de legiferare care derivă din utilizarea în textul legii a acestor noțiuni. Astfel la pct. 5 art. II din proiectul de lege în partea completării Legii nr. 48/2023 cu art. 4³ noțiunile date sunt utilizate în contextul stabilirii unor cerințe specifice față de aceste tipuri de entități, precum și aspecte legate de cazurile în care acestea intră în jurisdicția Republicii Moldova, atunci când aceasta va avea calitatea de stat membru al UE.

Definirea **noțiunii de „reprezentant”** este preluată din pct. 34 al art. 6 din Directiva NIS2. Conform explicațiilor dare de recitalul 116 al Directivei NIS2 în cazul în care entitățile de aceste tipuri nu sunt stabilite în UE, dar oferă servicii pe teritoriul acesteia, aceste entități trebuie să desemneze un reprezentant în Uniune, adică o persoană fizică sau juridică căreia autoritatea competentă i se poate adresa în locul furnizorului de servicii în cauză în ceea ce privește obligațiile ce îi revin acestuia conform legii.

La **subpunctul 4)** se propune introducerea în textul legii a noțiunii și definiției acesteia de *incident cibernetic de mare amploare*. Această propunere transpune prin preluare textuală art. 6 pct. 7 din Directiva NIS2. Sub aspect practic necesitatea definirii acestei noțiuni este determinată de faptul că ea este utilizată în textul proiectului de lege atât în contextul cadrului național de gestionare a crizelor cibernetice (articolul 9 din Legea nr. 48/2023) cât și în contextul relaționării în domeniul schimbului de informații și cooperării cu alte state membre în relații bilaterale, cât și în cadrul organizațiilor constituite prin Directiva NIS2 (Grupul de cooperare , Rețeaua CSIRT și Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice - EU-CyCLONe). În acest context unitate terminologică este importantă în mod special din perspectiva naturii transfrontaliere a astfel de incidente și a nivelului de impact pe care îl au. În acest sens, recitalul 69 din Directiva NIS2 stabilește că „în conformitate cu anexa la Recomandarea (UE) 2017/1584¹⁷, un incident de securitate cibernetică de mare amploare ar trebui să însemne un incident care provoacă un nivel de perturbare care depășește capacitatea unui stat membru de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două state membre. În funcție de cauza și de impactul lor, incidentele de securitate cibernetică de mare amploare pot escalada și se pot transforma în crize de sine stătătoare, care să împiedice buna funcționare a pieței interne sau să prezinte riscuri grave pentru securitatea și siguranța publică, pentru entități sau cetățeni, în mai multe state membre sau în Uniune în ansamblul său. **Având în vedere domeniul larg de aplicare și, în cele mai multe cazuri, natura transfrontalieră a unor astfel de incidente, statele membre și instituțiile, organele, oficiile și agențiile relevante ale Uniunii ar**

¹⁷ Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare: <https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX:32017H1584>

trebui să coopereze la nivel tehnic, operațional și politic pentru a coordona în mod corespunzător răspunsul în întreaga Uniune”.

Modificarea propusă la **punctul 5)** constă în completarea noțiunii de *incident cibernetic evitat la limită*. Această completare presupune în principiu ajustarea textuală a definiției acestei noțiuni, date de Legea nr. 48/2023, la definiția dată în art. 6 punctul 5. Din Directiva NIS2.

Același obiectiv de aliniere textuală în vederea evitării potențialelor disfuncționalități de interpretare practică îl au și modificările propuse la **punctele 7), 8) și 11)**. Punctele respective vizează modificări la noțiunile de „proces al tehnologiei informației și comunicațiilor (proces TIC)”, „produs al tehnologiei informației și comunicațiilor (produs TIC)”, „securitatea rețelelor și sistemelor informatice”.

La **punctul 10)** în definiția noțiunii de *rețea și sistem informatic* se propune expunerea normei de trimitere într-o formulă care să evite în viitor necesitatea modificării în caz de revizuire a legislației respective, cum a fost cazul abrogării Legii nr. 241/2007 prin Legea nr. 72/2025.

Punctul 4 al art. II din proiectul de lege propune expunerea într-o redacție nouă a articolelor 3 și 4 din Legea nr. 48/2023.

În ce privește noua redacție a art.3 aceasta vine cu un set de clarificări al domeniului de aplicare al legii și anume:

1. Alin. (1) al noii redacții propuse a art. 3 stabilește criteriile generale conform cărora urmează a fi definitivat domeniul de aplicare a legii prin realizarea procesului de identificare de către ASC. Punctul 1) din acest alineat reflectă regula dimensiunii, punctul 2) determină sectoarele, iar punctul 3) stabilește criteriul tipului concret de organizație care urmează să intre în sfera de aplicare a legii. Aceste criterii urmează a fi aplicate cumulativ în conformitate cu procedurile stabilite de Guvern prin Hotărârea Guvernului nr. 860/2024.

După cum s-a menționat în prezenta notă la explicațiile date noii redacții a noțiunii de *furnizor de servicii* în domeniul de aplicare al legii sunt incluse și persoanele fizice care practică activitate de întreprinzător sub formă de întreprindere/ întreprinzător individual. Deși aceste persoane ar putea fi de dimensiuni mai mici, totuși există riscul ca anumiți întreprinzători individuali care desfășoară activități și prestează servicii esențiale pentru funcționarea societății și economiei, adică corespund criteriilor legale pentru a fi identificați ca furnizori de servicii, să rămână în afara ariei de aplicare a legii, ceea ce ar putea prejudicia interesele persoanelor, a societății în general și a statului. Formularea actuală „persoane juridice” din textul legii exclude nejustificat această categorie de organizații.

2. Un alt element definitoriu al noii redacții propuse este clarificarea din perspectiva identificării, a distincției dintre furnizorii de servicii din sectorul public și a celor din sectorul privat, adică persoane juridice de drept public și întreprinderi. Conform **alineatului (1) din redacția propusă** a acestui articol în coroborare cu **alin. (7)** toate persoanele juridice de drept public urmează a fi identificate ca furnizori de servicii prin efectul legii și incluși în Lista furnizorilor de servicii din oficiu de către ASC.

Clarificarea aspectelor respective este necesară din raționamente de economie de resurse în exercitarea de către ASC a procesului de identificare a furnizorilor de servicii. În cazul persoanelor juridice de drept public acest proces ar trebui realizat prin efectul legii, fără emiterea unor acte administrative și, implicit, desfășurarea unor proceduri de identificare. În ce privește sectorul privat, procedura de identificare ar trebui să rămână în continuare una riguroasă, astfel încât, pe de o parte, să nu fie afectate drepturile și interese legitime ale întreprinderilor prin identificarea și supunerea acestora realizării unor obligații în mod nejustificat, iar pe de altă parte, să se asigure protecția adecvată a intereselor generale ale societății și a securității statului prin evitarea rămânerii în afara obligațiilor stabilite de lege a unor entități care într-adevăr sunt de natură critică pentru societate și economie, iar

perturbarea activității sau serviciilor esențiale prestate de acestea ar putea avea un impact semnificativ asupra acestor valori social-economice.

Un aspect nu mai puțin important în motivarea acestor clarificări în domeniul de aplicare al legii îl constituie și necesitatea de a distinge nu doar la nivel formal-juridic, ci și sub aspect practic tratamentul separat care urmează a fi aplicat autorităților și instituțiilor publice și întreprinderilor în cadrul desfășurării procesului de identificare. Omiterea unor proceduri în cazul persoanelor juridice de drept public este justificat și din punctul de vedere al faptului că acestea sunt parte al aceluiași sector public ca și autoritatea publică responsabilă de procesul de identificare, iar datele necesare sunt deja disponibile în resursele informaționale de stat și nu necesită a fi verificate factologic. În cazul întreprinderilor procesul de identificare trebuie realizat conform unor proceduri care să le ofere anumite garanții, inclusiv în ce privește dreptul acestora de a contesta activitatea administrativă respectivă. Această disjungere în procesul de identificare între public - privat este dictată și de faptul că regula dimensiunii (identificarea utilizând criteriile de clasificare a întreprinderilor ici și mijlocii) nu poate și nici nu trebuie aplicată persoanelor juridice de drept public. De asemenea pentru persoanele juridice de drept public nu sunt relevante nici sectoarele și subsectoarele critice ca unul din criteriile de eligibilitate.

Alegerea termenului de întreprindere este justificată de faptul că acesta cuprinde atât organizațiile private cu personalitate juridică, cât și persoanele fizice care practică activitate de întreprinzător. Potrivit articolul 34 alin. (1) și alin. (4) din Codul civil *persoana fizică are dreptul să practice activitate de întreprinzător din nume și pe cont propriu din momentul înregistrării de stat în calitate de întreprinzător individual sau în alt mod prevăzut de lege. Asupra activității de întreprinzător desfășurate fără constituirea de persoană juridică se aplică regulile care reglementează activitatea persoanelor juridice cu scop lucrativ dacă din lege sau din esența raporturilor juridice nu rezultă altfel*. Potrivit articolului 3 pct. 1 din Legea nr. 845/1992 cu privire la antreprenoriat și întreprinderi, *forma organizatorico-juridică a activității de antreprenoriat este întreprinderea*. Pct. 3. din același articol stabilește că *întreprinderea are dreptul de persoană juridică sau de persoană fizică, Întreprinderea-persoană juridică și întreprinderea-persoană fizică au aceleași drepturi și obligații, cu excepția răspunderii patrimoniale pentru obligațiile lor*.

3. Un alt element distinct în raport cu prevederile actuale ale legii îl constituie propunerea de **determinare în textul legii a sectoarelor și subsectoarelor critice (alin. 1)**. Sectoarele și subsectoarele critice enumerate la art. 3 alin. (1) pct. 2 din textul propunerii, sunt preluate din anexa nr. 2 la Hotărârea Guvernului nr. 860/2024 care, la rândul lor, se bazează pe anexele I și II ale Directivei NIS2, adaptate terminologiei legale a Republicii Moldova. Necesitatea de a reglementa la nivelul cadrului primar a sectoarelor și subsectoarelor critice este justificată de rațiuni de garantare a unei predictibilități mai ridicate a legislației, în raport spre exemplu cu tipurile de întreprinderi. Tipologia întreprinderilor este una mai dinamică și în cazul acesteia ar putea fi admisă o flexibilitate normativă mai mare. Adică, atunci când spre exemplu în baza unor analize a riscurilor, inclusiv în domeniul securității cibernetice, sau a unor modificări ale legislației sectoriale la nivel național sau european, va fi stringentă revizuirea acestei tipologii, la nivelul cadrului normativ guvernamental aceasta va putea fi asigurat mult mai rapid. În ce privește sectoarele și subsectoarele critice listarea lor în textul legii constituie un compromis dintre predictibilitatea legii, inclusiv determinarea la nivel primar a ariilor de activitatea pe care le acoperă, și principiul minimei armonizări stabilit în art. 5 din Directiva NIS2, care presupune nu doar limita minimă de reglementare, ci și uniformitatea acesteia la nivelul statelor membre în vederea asigurării unei competitivități echitabile pe piața internă.

4. Alin. (2) din noua redacție propusă a art. 3 transpune prevederile art. 2 alin. (1) din Directiva NIS2, care face o excepție de la aplicabilitatea Recomandării 2003/361/CE¹⁸. Această recomandare este instrumentul de bază în aplicarea regulii dimensiunii în procesul de determinare a domeniului de aplicare a Directivei NIS2. În legislația națională actul normativ care actualmente transpune parțial prevederile acestei Recomandări este Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii. Legea respectivă nu conține prevederi care să transpună norme juridică în speță din Directiva NIS2. Reglementarea în Legea nr. 48/2023 a aspectelor netranspuse în legislația națională din Recomandarea respectivă este nerațională și nejustificată din punct de vedere juridic, în special prin prisma principiilor de legiferare. Aceasta ar depăși obiectul de reglementare al Legii nr. 48/2023 și ar crea ulterior, după transpunerea integrală a Recomandării, a dublărilor de norme juridice sau necesitatea modificării Legii nr. 48/2023. În contextul respectiv, ținem să relevăm faptul că MDDE a elaborat și remis deja în consultări publice și avizare oficială proiectul de lege pentru modificarea Legii nr. 179/2016¹⁹ (proiect cu număr unic: 398/MDDE/2026), unul din obiectivele căreia este să transpună integral Recomandarea menționată mai sus.

Sub aspectul reglementărilor materiale ale acestei propuneri relevăm că prevederea la care ne referim din Directiva NIS2 stabilește că „*articolul 3 alineatul (4) din anexa la recomandarea respectivă nu se aplică în sensul prezentei directive.*” Art. 3 din anexa la recomandarea respectivă stabilește tipurile de întreprinderi luate în considerare la calcularea efectivelor de personal și a sumelor financiare, definind întreprinderea autonomă, întreprinderile partenere și întreprinderile legate și criteriile de determinare a acestora. Art. 3 alin. (4) din anexa la recomandarea respectivă prevede „*Cu excepția cazurilor prevăzute la alineatul (2) al doilea paragraf, o întreprindere nu poate fi considerată IMM dacă 25 % sau mai mult din capitalul social sau din drepturile de vot sunt controlate, direct sau indirect, în comun sau individual, de unul sau mai multe organisme publice.*”. Prin urmare aceste întreprinderi vor fi considerate în sensul Directivei NIS2 IMM-uri, cu excepția cazului specificat la art. 3 alin. (2) subparagraful al doilea din anexa la recomandare. Acesta din urmă stabilește „*...o întreprindere poate fi considerată autonomă și, prin urmare, fără întreprinderi partenere, chiar dacă acest prag de 25 % este atins sau depășit de către următorii investitori, cu condiția ca acești investitori să nu fie legați, în sensul alineatului (3), nici individual, nici în comun, de întreprinderea în cauză:*

(a) *societăți publice de investiții, societăți de capital de risc, persoane fizice sau grupuri de persoane fizice care desfășoară o activitate regulată de investiții de capital de risc și care investesc capital propriu în întreprinderi necotate la bursă („investitori providențiali”), cu condiția ca investiția totală a acestor investitori providențiali în aceeași întreprindere să fie mai mică de 1 250 000 EUR;*

(b) *universități sau centre de cercetare fără scop lucrativ;*

(c) *investitori instituționali, inclusiv fonduri de dezvoltare regională;*

(d) *autorități locale autonome cu un buget anual mai mic de 10 milioane EUR și cu un număr de locuitori mai mic de 5 000.*”.

Aceste prevederi sunt transpuse integral prin proiectul de lege pentru modificarea Legii nr. 179/2016 menționat mai sus. Prin urmare în alin. (2) al noii redacții propuse în proiectul de lege a art. 3 din Legea privind securitatea cibernetică, se face trimitere la elementul structural care actualmente propune transpunerea prevederilor art. 2 alin. (1) a doua propoziție din proiectul de lege pentru modificarea Legii nr. 179/2016 – art. 5² alin. (4). În procesul promovării ambelor proiecte se va asigura sincronizarea dintre prevederile acestora.

¹⁸ Recomandarea Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii: <https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=celex:32003H0361>

¹⁹ <https://particip.gov.md/ro/document/stages/anunt-de-initiere-a-elaborarii-proiectului-de-lege-de-modificare-a-legii-nr-1792016-cu-privire-la/15778>

5. Conceptual redacția nouă a **alin. (3) al art. 3** păstrează esența redacției actuale a alin. (2) art. 3 din Legea nr. 48/2023 și anume excepțiile de la regula dimensiunii a unor tipuri de întreprinderi în cazul literelor a)-e) și j) și cumularea excepției de la regula dimensiunii cu criterii specifice în cazul literelor f) – i).

Elementele noi în raport cu redacția actuală a acestui alineat constau în următoarele:

a) Includerea în lista excepțiilor de la regula dimensiunii a furnizorilor de servicii DNS (**lit. d)**). Actualmente aceștia intră în domeniul de aplicare al legii dacă se califică cel puțin ca întreprinderi mijlocii. Conform propunerii de modificare aceștia vor intra în domeniul de aplicare al legii indiferent de dimensiune să presteze servicii de servicii de rezoluție a numelor de domenii recursive accesibile publicului pentru utilizatorii finali de internet sau servicii de rezoluție a numelor de domenii cu autoritate pentru utilizarea de către terți, cu excepția serverelor pentru nume primare. Această modificare transpune prevederile art. 2 alin. (2) lit. (a) punctul (iii) din Directiva NIS2. Este important de relevat faptul că potrivit propunerii de modificare a Directivei NIS2, la care se face referire în punctul 5.1 al prezentei note de fundamentare, acest tip de furnizori va fi exclus din lista excepțiilor de la regula dimensiunii.

b) Lit. f) din redacția actuală a Legii nr. 48/2023 a fost separată în două criterii distincte, reflectate în proiect la **literele g) și h)**. Această separare este necesară pentru a asigura corespunderea tehnică prevederilor art. 2 alin. (2) Directivei NIS2 literele c) și d), din rațiuni de raportare conform prevederilor art. 3 alin. (5) din Directiva respectivă, transpuse prin prevederile art. art. 7¹ alin. (1) lit. b), propuse în proiectul de lege.

c) **Lit. j) din alin. (3) al art. 3 din proiect** propune în esență o redacție nouă a lit. h) alin. (2) art. 3 din Legea nr. 48/2023, revizuită în conformitate cu terminologia Legii nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurii critice. Este important de relevat faptul că în redacția propusă în proiect a acestei prevederi este păstrat și termenul de operator al obiectivului de infrastructură critică, specific Legii nr. 120/2017 cu privire la prevenirea și combaterea terorismului. Utilizarea acestor două noțiuni este determinată de faptul că în prezent sunt în vigoare două mecanisme de protecție a infrastructurii critice: unul stabilit prin Legea 223/2025 și al doilea cel stabilit de Legea nr. 120/2017. Legea nr. 223/2025 în dispozițiile sale tranzitorii nu stabilește în sarcina Guvernului înaintarea propunerilor de aducere a legilor în concordanță cu legea respectivă. Prin urmare intenția legiuitorului a fost ca aceste două mecanisme să rămână în vigoare. Din această perspectivă prevederile Legii nr. 120/2017, în conformitate cu art. 5 din Legea nr. 100/2017 au caracter special, în raport cu cele ale Legii nr. 223/2025 sub aspectul protecției infrastructurii critice exclusiv din punctul de vedere al prevenirii și combaterii terorismului, care intră în competența Serviciului de Informații și Securitate.

6. **Alin. (4) și (5) ale art. 3** în redacția propusă în proiectul de lege este un element nou pentru Legea nr. 48/2023 prin faptul că introduce categoriile de furnizori de servicii: esențiali și importanți, transpunând prevederile art. 3 alin. (1) și (2) din Directiva NIS2. Această categorizare actualmente este prevăzută în anexa nr. 2 la Hotărârea Guvernului nr. 860/2024. Reglementarea acestui aspect la nivel de norme legale este necesară pentru a asigura respectarea principiilor stabilității și predictibilității normelor juridice și respectării ierarhiei normelor juridice. Actualmente în Legea nr. 48/2023 o astfel de separare a furnizorilor de servicii nu a fost realizată din lipsa utilității juridice și necesității practice. Or, diferențierea în categorii făcută de Directiva NIS2 este determinată în mod special de regimul de supraveghere diferit aplicat în cazul entităților esențiale (regim de supraveghere ex ante și ex-post) și a celor importante (regim de supraveghere ex-post). În prezent Legea nr. 48/2023 nu stabilește o astfel de diferențiere de regimuri în exercitarea supravegherii și controlului, aplicând regimul ex-post pentru toți furnizorii de servicii. Însă, reieșind din faptul că proiectul preconizează transpunerea integrală a Directivei NIS2, este necesară și revizuirea reglementării juridice a supravegherii și controlului de stat

din Legea nr. 48/2023 (pct. 8 din art. II l proiectului – noua redacție a art. 19). Aceasta determină necesitatea separării furnizorii de servicii în aceste două categorii distincte. Factorii care determină atribuirea unei întreprinderi la categoria furnizorilor de servicii esențiali sau importanți sunt gradul de importanță critică și dimensiunea acestora. Recitalul 15 din preambulul la Directiva NIS2 explică acest aspect mai detaliat: „(15) *Entitățile care intră în domeniul de aplicare al prezentei directive în scopul respectării măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare ar trebui clasificate în două categorii, entități esențiale și entități importante, reflectând măsura în care acestea sunt critice în ceea ce privește sectorul lor sau tipul de serviciu pe care îl prestează, precum și dimensiunea lor. În acest sens, ar trebui să se țină seama în mod corespunzător de orice evaluări ale riscurilor sau de orice orientări specifice unui sector relevante emise de către autoritățile competente, după caz. Regimurile de supraveghere și de asigurare a respectării legii corespunzătoare acestor două categorii de entități ar trebui să fie diferențiate pentru a asigura un echilibru corect între cerințele și obligațiile bazate pe riscuri, pe de o parte, și sarcina administrativă care decurge din supravegherea conformității, pe de altă parte.*”.

7. Alin. (6) literele a) și b) în principiu sunt corespundentele art. 3 alin. (3) din Legea nr. 48/2023, și vizează transpunerea prevederilor alineatelor (6), (7) și (8) din art. 2 al Directivei NIS2. **Literele c) și d)** decurg din ultimele două propoziții ale recitalului (8) din preambulul Directivei NIS2. Conform acestuia: *Entitățile administrației publice care sunt înființate în comun cu o țară terță în conformitate cu un acord internațional sunt excluse din domeniul de aplicare al prezentei directive. Prezenta directivă nu se aplică misiunilor diplomatice și consulare ale statelor membre în țări terțe sau rețelelor și sistemelor informatice ale acestora, în măsura în care aceste sisteme se află la sediul misiunii sau sunt utilizate pentru utilizatori dintr-o țară terță.* Această excludere se bazează pe criteriul utilizării acestor rețele și sisteme informatice în raport cu și de către țările terțe partenere, cărora nu le pot fi impuse unilateral anumite cerințe de securitate, obligatorii pe piața internă a UE.

8. Alin. (7) păstrează redacția actuală a alin. (4) al art. 3 din Legea nr. 48/2023.

9. Alineatele (8) – (11) transpun prevederile alineatelor (1) și (2) ale art. 4 din Directiva NIS2. Aceste prevederi stabilesc principiile de aplicabilitate a actelor juridice sectoriale ale Uniunii Europene în raport cu prevederile Directivei NIS2. În acest caz principiul *lex specialis derogat lex generalis* are o limitare și anume echivalența în efecte a legii speciale în raport cu cea generală. Cu alte cuvinte dacă o lege sectorială prevede anumite cerințe de securitate sau obligații de notificare similare legii generale (privind securitatea cibernetică), legea sectorială nu va fi aplicabilă dacă efectele pe care le produc normele sale nu sunt cel puțin la fel ca și cele stabilite de legea generală. Condiția echivalenței în efecte presupune că legea sectorială trebuie să stabilească cerințe la fel de stricte sau mai stricte decât legea securității cibernetică. Explicarea detaliată a chestiunii legii aplicabile și a modului în care urmează a fi tratată și interpretată condiția echivalenței în efecte este dată de Orientările Comisiei²⁰ privind modul de aplicare a art. 4 alin. (1) și (2) din Directiva NIS2. Prevederi relevante din punct de vedere normativ ale acestei orientări a Comisiei sunt reflectate în capitolul III din Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetică de către furnizorii de servicii în sectoarele critice, aprobat prin Hotărârea Guvernului nr. 562/2025.

10. Alin. (12) transpun prevederile art. 26 alin. (1) lit. a) din Directiva NIS2. Aceasta este o excepție de la regula generală conform căreia sub jurisdicția Republicii Moldova intră întreprinderile înregistrate în Republica Moldova (conform definiției de furnizor de servicii dat în art. 2 al Legii nr. 48/2023). Derogarea respectivă este explicată în recitalurile corespunzătoare ale acestei Directive. Potrivit recitalului (113) „(113) *Entitățile care intră în domeniul de aplicare al prezentei directive ar*

²⁰ Comunicare a Comisiei Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555 (Directiva NIS 2)
[https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918\(01\)](https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918(01))

trebui considerate ca fiind sub jurisdicția statului membru în care sunt stabilite. Totuși, ar trebui să se considere că furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului intră sub jurisdicția statului membru în care își prestează serviciile.... În cazul în care entitatea furnizează servicii sau își are sediul în mai multe state membre, aceasta ar trebui să intre sub jurisdicția separată și concurentă a fiecăruia dintre respectivele state membre. Autoritățile competente din respectivele state membre ar trebui să coopereze, să își ofere asistență reciprocă și, după caz, să întreprindă acțiuni comune de supraveghere. În cazul în care statele membre își exercită jurisdicția, acestea nu ar trebui să aplice măsuri de asigurare a respectării legii sau sancțiuni de mai multe ori pentru același comportament, în conformitate cu principiul ne bis in idem.” . Conform art. IV din proiectul de lege această prevedere urmează să intre în vigoare la data intrării în vigoare a tratatului de aderare a Republicii Moldova la Uniunea Europeană.

Redacția nouă a **art. 4 propusă în art. II pct. 4 și completarea legii cu articolele 4¹ și 4², propusă în punctul 5 art. II din proiectul de lege** vine cu clarificările necesare la nivelul normelor legale primare a procesului de identificare a furnizorilor de servicii. Prevederile respective se regăsesc actualmente în Regulamentul cu privire la identificarea furnizorilor de servicii, aprobat prin Hotărârea Guvernului nr. 860/2024. O detaliere la nivelul normelor primare a principalelor elemente ale procesului de identificare va oferi un plus de valoare previzibilității și stabilității normelor juridice precum și clarității și coerenței corpului de norme juridice incluse în Legea securității cibernetice și va evita riscuri de depășire a competenței Guvernului de organizare a executării legii statuat în art. 102 din Constituție. De asemenea, aceste modificări vor oferi garanții entităților din sectorul privat în ce privește securitatea raporturilor juridice.

Cu referire la propunerea de completare a legii cu art. 4³, propusă în pct. 5 al art. II din proiectul de lege, menționăm că alineatele (1)-(3) transpun prevederile art. 27 alin. (2) din Directiva NIS2, iar alineatele (4)-(8) - ale art. 26 alin. (1) lit. b) și alin. (2) – alin. (4) din aceeași directivă. În primul caz, instituirea cerințelor respective este determinată de necesitatea instituirii și menținerii de către ENISA a unui registru a furnizorilor de tipurile menționate în prevederea respectivă. Conform art. 26 alin. (1) din Directiva NIS2, ENISA creează și păstrează un registru al acestor entități pe baza informațiilor primite de la punctele unice de contact ale statelor membre ale UE. Prin urmare introducerea acestor obligații în textul legii este determinată de necesitatea garantării că autoritatea competentă va dispune de pârghii legale pentru obținerea acestor informații și în consecință își va putea realiza obligațiile de informare în raport cu ENISA. În al doilea caz, dispozițiile propuse în redacția proiectului derivă din necesitatea stabilirii regulilor de determinare a cazurilor când aceste tipuri de furnizori intră în jurisdicția autorităților competente ale Republicii Moldova, din perspectiva calității sale viitoare de stat membru al Uniunii Europene. Regula generală este că în jurisdicția Republicii Moldova intră întreprinderile care sunt înregistrate în Registrul de stat al unităților de drept în conformitate cu Legea nr. 220/2007 privind înregistrarea de stat a persoanelor juridice și a întreprinzătorilor individuali. În cazul entităților de tipul celor menționate la art.26 alin. (1) lit. b) din Directiva NIS2 și corespunzător art. 4³ alin. (1) din proiectul de lege, regula generală nu este aplicabilă, acestea fiind o excepție urmează a fi considerate că se află în jurisdicția statului membru în care își au sediul principal în Uniune. Spre deosebire de furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului, în privința cărora jurisdicția este atribuită mai multor state membre²¹, în cazul tipurilor de entități menționate la art.26 alin. (1) lit. b) din Directiva NIS2 doar un stat membru ar trebui să aibă jurisdicție asupra entităților respective. Recitalul

²¹ Recitalul 113 din preambulul la Directiva NIS2: „... În cazul în care entitatea furnizează servicii sau își are sediul în mai multe state membre, aceasta ar trebui să intre sub jurisdicția separată și concurentă a fiecăruia dintre respectivele state membre. Autoritățile competente din respectivele state membre ar trebui să coopereze, să își ofere asistență reciprocă și, după caz, să întreprindă acțiuni comune de supraveghere.”

(114) și (115) vine cu clarificări mai detaliate ale dispozițiilor normative în discuție, în ce privește motivarea determinării jurisdicției după sediul principal al acestor entități în UE și regulile de determinare a sediului principal. Alineatele (7) și (8) din art. 4³ reglementează cazurile când aceste entități sunt obligate să desemneze un reprezentant în UE.

Punctul 6 al art. II din proiectul de lege propune ajustări terminologice derivate din recenta modificare a Legii nr. 98/2012 privind administrația publică centrală de specialitate efectuată prin Legea nr. 140/2025.

Punctul 7 al art. II din proiectul de lege cuprinde **modificări ale art. 7** din Legea nr. 48/2023.

1. Modificările propuse în **titlul art. 7, la alin. (2), alin. (3) lit. a), alin. (4)** rezidă în ajustări textuale pentru clarificarea respectivelor norme juridice, astfel încât acestea să corespundă principiilor clarității și coerenței legii.

2. Propunerea de completare a **art. 7 alin. (3) cu literele c¹) și c²)** și a **alin. (4) cu punctul 7²)** derivă din necesitatea alinierii conținutului funcțional al competenței ASC la obligațiile de cooperare și schimb de informații ale Republicii Moldova ce decurg din prevederile Directivei NIS2. În speță propunerile respective stabilesc în sarcina ASC reprezentarea Republicii Moldova în cadrul Grupului de cooperare în materie de rețele și sisteme informatice și în cadrul Rețelei echipelor de răspuns la incidente de securitate informatică (Rețeaua CSIRT), precum și participarea la evaluările inter pares în condițiile legislației relevante a Uniunii Europene și în conformitate cu metodologia stabilită de Grupul de cooperare. Astfel, conform art. 10 (6) din Directiva NIS2 statele membre trebuie să asigure cooperarea efectivă, eficientă și sigură a propriilor CSIRT naționale în cadrul rețelei CSIRT, iar potrivit art. 14 alin. (5) din aceeași directivă - cooperarea eficientă și sigură a reprezentanților lor în Grupul de cooperare. Atribuția de participare la evaluările inter pares derivă din prevederile art. 10 alineatul (5) din Directiva NIS2.

3. Completarea propusă la **alineatul (4) punctul 2)** constituie o **ajustare a textului actual la prevederile art. 11 (3)** din Directiva NIS2 conform căruia una din sarcinile care revine CSIRT-urilor naționale este acordarea, la cerere, de asistență entităților esențiale și entităților importante implicate cu privire la monitorizarea **în timp real sau în timp aproape real** a rețelei lor și a sistemelor lor informatice. Această atribuție trebuie privită în strânsă legătură cu competența ASC de monitorizare și analiză a amenințărilor cibernetice, vulnerabilităților și incidentelor cibernetice la nivel național. Recitalul (44) din preambulul la Directiva NIS2 clarifică acest aspect: *„CSIRT ar trebui să aibă capacitatea, la cererea unei entități esențiale sau importante, de a monitoriza resursele entității conectate la internet, atât în incinta sediului, cât și în afara acestuia, pentru a identifica, înțelege și gestiona riscurile organizaționale generale ale entității în ceea ce privește compromiterile recent identificate ale lanțului de aprovizionare sau vulnerabilitățile critice. Entitatea ar trebui încurajată să comunice echipei CSIRT dacă utilizează o interfață de administrare cu drepturi privilegiate, întrucât acest lucru ar putea afecta rapiditatea cu care se întreprind acțiunile de atenuare.”*.

4. Redacția nouă propusă a punctului 3) din alineatul 4 este o ajustare textuală la prevederile art. 11 alin. (3) lit.(b) din Directiva NIS2, care în raport cu prevederea actuală introduce prioritatea informării furnizorilor de servicii și atunci când este posibil informarea acestora în timp aproape real.

5. Completarea cu pct. 3¹) propusă la alin. (4) transpune prevederile paragrafului al doilea din art. 11 alin. (3) din Directiva NIS2, conform căruia *„echipele CSIRT pot efectua scanări proactive și neintruzive ale rețelelor și sistemelor informatice accesibile publicului ale entităților esențiale și ale entităților importante. Asemenea scanări se efectuează pentru a detecta rețelele și sistemele informatice vulnerabile sau configurate în mod nesigur și pentru a informa entitățile în cauză. Asemenea scanări nu au niciun impact negativ asupra funcționării serviciilor entităților.”*.

Această atribuție a CSIRT național este diferită de cea deja prevăzută la art. 7 alin. (4) pct. 8) din Legea nr. 48/2023, corespondent art. 11 alin. (3) lit. e) din Directiva NIS2, conform căruia CSIRT poate furniza scanări proactive a rețelelor și a sistemelor informatice ale entității esențiale sau importante pentru a detecta vulnerabilitățile cu un impact potențial semnificativ doar la cererea acestor entități. Diferențele constau în principal în factorul declanșator cererea entității vs inițiativa CSIRT, obiectul supus scanării: perimetrul interior (intrusiv) vs perimetru exterior și interior (neintrusiv) și consimțământ: obligatoriu vs discreția CSIRT. În principiu atribuția propusă la pct 3¹) are o natură de supraveghere preventivă neintrusivă cu caracter sistemic menit să monitorizeze igiena spațiului cibernetic național.

6. Punctul nou 7¹, cu care se propune completarea alineatului (4) din art. 7 al Legii nr. 48/2023, stabilește o sarcină a CSIRT care derivă din dispoziția alineatului (4) al art. 11 din Directiva NIS2. Dispoziția respectivă din Directiva NIS2 prevede că CSIRT-urile naționale trebuie să stabilească *relații de cooperare cu părțile interesate relevante din sectorul privat, în vederea îndeplinirii obiectivelor prezentei directive*.

7. Excluderea textului din pct. (8) alin. (4) al art. 7 este determinată de faptul că condițiile de efectuare a scanărilor proactive la cererea furnizorilor de servicii urmează a fi decise la nivel bilateral de către autoritatea competentă și furnizorul de servicii vizat, conform metodologiilor și bunelor practici în realizarea unor astfel de scanări.

8. Propunerea de completare cu pct. 9¹ transpune prevederile art. 11 alin. (5) din Directiva NIS2, coroborate cu cele de la alin. (4) al aceluiași articol. Scopul acestei propuneri este să ofere competența necesară ASC în stabilirea unei abordări unificate în ce privește chestiunile operaționale în ce privește prevenirea, detectarea și răspunsul la incidentele cibernetice.

9. Completarea punctului 10) din alin. (4) al art. 7 este determinată de necesitatea clarificării competenței ASC din punctul de vedere a realizării atribuției sale de cooperare la nivel internațional, în mod special la nivelul Uniunii Europene, în contextul realizării funcției de coordonator al procesului de divulgare coordonată a vulnerabilităților la nivel național. Prevederea asigură armonizarea legislației naționale la prevederile ultimul paragraf art. 12 alin. (1) din Directiva NIS2, conform căruia *în cazul în care o vulnerabilitate raportată ar putea avea un impact semnificativ asupra entităților în mai multe state membre, echipa CSIRT desemnată drept coordonator din fiecare stat membru în cauză cooperează, dacă este cazul, cu alte echipe CSIRT desemnate drept coordonatori în cadrul rețelei CSIRT*.

10. Propunerea de completare a art. 7 cu alin. (4)¹ are ca obiectiv determinarea unui nivel minim de condiții cărora trebuie să corespundă CSIRT-ul național, constituit în cadrul ASC. Acestei condiții sunt corespondente condițiilor care sunt stabilite la art. 11 alin. (1) din Directiva NIS2. Responsabilitatea primară pentru respectarea acestor condiții cade în sarcina conducerii ASC, iar norma respectivă îi oferă temeiul juridic necesar pentru a înainta demersurile necesare pentru asigurarea CSIRT cu resurse necesare și capacități operaționale suficiente. Deși transpunerea acestei norme nu necesită o reproducere textuală în legislația națională, totuși ea oferă pe plan intern garanții că gradul de operaționalizare a CSIRT național va fi menținut la un nivel adecvat.

În punctul 8 al art. II din proiectul de lege se propune completarea Legii nr. 48/2023 cu articolele 7¹, 7² și 7³.

1. Art. 7¹ reglementează chestiuni esențiale de cooperare și schimb de informații cu autoritățile și instituțiile Uniunii Europene. Obligațiile ASC, specificate la alin. (1), de a informa instituțiile UE cu competențe în domeniul securității cibernetice asigură transpunerea unui set de prevederi ale Directivei NIS2 și anume: art. 3 alin. (5) – literele a) și b); art. 3 alin. (6) – lit. c); art. 7 alin. (3) – lit. d); art. 8

alin. (6), art. 9 alin. (5) prima propoziție, art. 10 alin. (9) – lit. e); art. 9 alin. (5) a doua propoziție – lit. f); art. 23 alin. (9) – lit. g).

Alineatele (2) – (4) reglementează cadrul general privind limitările schimbul de informații atunci când obiectul acestui schimb îl constituie informații ce vizează securitatea națională, ordinea publică sau apărarea națională. Limitările stabilite la alin. (2) vizează protecția nu doar a intereselor Republicii Moldova, ci și a altor State Membre. Această limitare este necesară din perspectiva faptului că în cadrul cooperării în aceste domenii a autorităților publice naționale cu cele ale statelor membre, informațiile sensibile furnizare autorităților naționale ar trebui să se bucure de aceeași protecție. Potrivit alin. (3) informațiile confidențiale pot constitui obiect al schimbului de informații doar dacă acest lucru este necesar pentru aplicarea legislației UE sau naționale în domeniul securității cibernetice, dacă corespunde scopului urmărit și este strict proporțională acestuia. Aceste condiții trebuie aplicate cumulativ. Alin. (4) oferă o protecție din perspectiva intereselor organizațiilor care cad sub incidența obligațiilor stabilite de lege. Furnizorii de servicii de asemenea trebuie să beneficieze de garanțiile necesare că informații care constituie secret comercial spre exemplu nu vor fi divulgate nejustificat și disproporționat de către deținătorii statali ai astfel de informații.

2. Art. 7² transpune prevederile art. 19 din Directiva NIS2. Evaluările inter-pares sunt un mecanism prin care statele membre se supun, în mod voluntar, unei evaluări reciproce bazate pe expertiza externă independentă, în vederea verificării implementării cadrului stabilit de Directiva NIS2 și actele de punere în aplicare a acesteia și a consolidării capacităților naționale și cooperării la nivel european în domeniul securității cibernetice. Metodologia²² de evaluare este aprobată de Grupul de cooperare. Obiectivele acestui instrument sunt expuse în art. 19 alin. (1) din Directiva NIS2 și rezidă în a învăța din experiențele comune, a consolida încrederea reciprocă, a atinge un nivel comun ridicat de securitate cibernetică, precum și a consolida capacitățile și politicile de securitate cibernetică. Având în vedere că participarea la un astfel de instrument este unul voluntar, în proiect se propune atribuirea dreptului discreționar de participa la aceste evaluări ASC, precum și stabilirea competențelor acesteia în exercitarea acestui drept discreționar.

3. În art. 7³ se propune reglementarea unor aspecte specifice de cooperare a ASC cu autoritățile și instituțiile publice la nivel național. Un aspect important în această cooperare decurge din caracterul de completare reciprocă pe care îl au legislațiile în domeniul protecției fizice a infrastructurii critice și protecției cibernetice a acesteia. Acest caracter de complementaritate derivă din actele legislative ale UE, extrapolat la nivelul legislației naționale. Conform recitalului (24) din Directiva CER²³: *Autoritățile competente în temeiul prezentei directive și autoritățile competente în temeiul Directivei (UE) 2022/2555 ar trebui să coopereze și să facă schimb de informații în ceea ce privește riscurile de securitate cibernetică, amenințările cibernetice și incidentele cibernetice și riscurile, amenințările și incidentele non-cibernetice care afectează entitățile critice, precum și în ceea ce privește măsurile relevante luate de autoritățile competente în temeiul prezentei directive și de autoritățile competente în temeiul Directivei (UE) 2022/2555. Este important ca statele membre să se asigure că cerințele prevăzute în prezenta directivă și în Directiva (UE) 2022/2555 sunt puse în aplicare în mod complementar și că entitățile critice nu sunt supuse unei sarcini administrative mai mari decât cea necesară pentru a atinge obiectivele prezentei directive și pe cele ale directivei menționate.*

²² <https://digital-strategy.ec.europa.eu/ro/policies/nis-cooperation-group>

²³ Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557>

Alin. (2) specifică o obligație de asigurare a unei cooperări periodice dintre ASC și autoritățile competente în domeniile sensibile și de o înaltă importanță critică cu sunt cele ale identificării electronice și serviciilor de încredere, comunicațiilor electronice și al bancar și al pieței financiare.

Sub aspect practic, având în vedere conținutul destul de tehnic, sensibilitatea informațiilor ce ar putea constitui obiectul cooperării și schimbului, precum și nivelul ridicat de detaliere al acestor informații, în **alin. (3)** se propune acordarea dreptului discreționar autorităților publice în speță să reglementeze la nivelul unor acte comune, procedurile operaționale de schimb de informații și cooperare în legătură cu obiectivele pe care le urmăresc și în funcție de domeniile în care își exercită competența.

Punctul 9 al art. II din proiectul de lege conține propuneri de modificare și completare a art. 9 din Legea nr. 48/2023, care reglementează chestiunile privind cadrul de coordonare și răspuns la crizele cibernetice. Propunerile respective vizează ajustări terminologice și textuale. Astfel, excluderea textului „în domeniul securității” va oferi concizie termenului de „criză cibernetică” și corelarea acestuia cu prevederile art. 9 din Directiva NIS2. Redacția propusă a **alin. (1)** vine cu unele clarificări și ajustări textuale și terminologice are ca scop reflectarea în textul legii a cerinței stabilite la art. 9 alin. (1) din Directiva NIS2, conform căruia *„fiecare stat membru desemnează sau instituie una sau mai multe autorități competente responsabile cu gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor (denumite în continuare „autorități de gestionare a crizelor cibernetice”).* Astfel, conform acestui alineat ASC este desemnată ca autoritate de gestionare a crizelor cibernetice și va exercita rol de coordonare în acest proces. Norma juridică de desemnare expresă a acestei autorități este prevăzută la pct. 1 din Hotărârea Guvernului nr. 1028/2023 *„Cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică”*. La **alin. (2)** se propune excluderea textului „în acest scop” de la începutul, pentru a conferi claritate și a exclude eventuale deficiențe de interpretare precum și pentru a asigura coerență și concordanță între dispozițiile alineatului (1) și alineatului (2). Or, alineatul (1) definește competența autorității competente în domeniul securității cibernetice din perspectiva gestionării crizelor cibernetice. Păstrarea acestei sintagme ar putea duce la interpretări inconsistente conform căror autoritatea competentă își poate exercita mandatul de gestionare a crizei cibernetice exclusiv în limitele planului menționat la alin. (2). Deși acesta constituie un instrument operațional fundamental de pregătire și răspuns la crize cibernetice, totuși spectrul de activități la nivel operațional al ASC ar putea depăși situațiile descrise în plan. Modificarea propusă la **alineatul (3)** este determinată de necesitatea unei clarificări²⁴ în legătură cu noțiunile utilizate în lege, textul „de mare amploare” urmând a fi atribuit termenului de *incident cibernetic* și nu celui de *criză cibernetică*. La alin. (4) se propune excluderea cuvântului *metodologic*, pentru a face mai coerent textul acestei dispoziții legale în contextul în care este utilizat deja cuvântul normativ, utilizarea ambelor termen ar putea crea confuzie. Sub aspectul fondului acestei ajustări menționăm că Guvernul ar trebui să organizeze punerea în aplicare a prevederilor alineatului (3) în mod special, iar abordările standardizate bazate pe metodologii și bune practici să rămână la discreția autorității competente.

Punctul 10 al art. II din proiectul de lege propune modificări și completări la art. 11 din Legea nr. 48/2023. Modificările și completările propuse la alineatul (2) pct. 2 au ca scop ajustarea

²⁴ Spre exemplu versiunea română a Recomandării (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și **crizele de securitate cibernetică de mare amploare**, utilizează sintagma *de mare amploare* în raport cu cuvântul *criză*.

terminologică și textuală cu prevederile alineatelor (1) și (2) ale art. 21 din Directiva NIS2. Excluderea normei de trimitere de la alin. (4) lit. a) vizează aspectul formal: aducerea în concordanță cu realitățile normative create prin Hotărârea Guvernului nr. 562/2025, și aspectul de fond: excluderea obligativității de utilizare a standardelor, furnizorii de servicii fiind obligați să asigure conformitatea cu cadrul normativ relevant, iar standardele urmând a le utiliza în mod voluntar pentru orientare în procesul de implementare a măsurilor de securitate. În acest context dispoziția de la alin. (4) al acestui articol rămâne a fi util din punctul de vedere al accesibilității la standarde naționale care corespund bunelor practici internaționale și sunt corespunzător actualizate. Completarea propusă decurge din alin. (2) al art. 21 din Directiva NIS2. Introducerea abordării multirisc în textul legii derivă din necesitatea clarificării obligațiilor legale pentru furnizorii de servicii. Dată fiind natura diferită a amenințărilor și diversitatea consecințelor pe care, odată materializate, acestea ar putea să le producă, precum și interdependențele tot mai consistente dintre diferite sectoare și subsectoare critice, este necesară implementarea unei abordări care să implice evaluarea riscurilor nu doar din perspectivă cibernetică, ci să ia în considerare cel puțin și mediul fizic al infrastructurii informaționale critice ce trebuie protejată.

Redacția **alineatului (2¹)** transpune prevederile art. 20 din Directiva NIS2. Articolul 20 din directiva respectivă reglementează chestiuni de guvernanță în ce privește gestionarea riscurilor în materie de securitate cibernetică la nivelul entităților care cad sub incidența obligațiilor stabilite de directivă. Conținutul acestor obligații este determinat de necesitatea asumării plenare de către conducerea furnizorului de servicii a responsabilității pentru asigurarea securității cibernetice în cadrul furnizorului de servicii. Conform recitalul (137) din preambulul la Directiva NIS2, directiva și, implicit, legislația națională ”...ar trebui să vizeze asigurarea unui nivel ridicat de responsabilitate pentru măsurile de gestionare a riscurilor în materie de securitate cibernetică și pentru obligațiile de raportare la nivelul entităților esențiale și al entităților importante. Din aceste motive, organele de conducere ale entităților esențiale și ale entităților importante ar trebui să aprobe măsurile privind riscurile în materie de securitate cibernetică și să supravegheze punerea lor în aplicare.”.

Alineatul (2²) stabilește reglementări de ordin primar privind determinarea proporționalității măsurilor de securitate aplicate cu riscurile evaluate, transpunând prevederile propoziției a doua din subparagraful doi al alin. (1) din art. 21 al Directivei NIS2. Aceasta proporționalitate are două dimensiuni: una la nivelul furnizorului de servicii în procesul de implementare a măsurilor de securitate, și a doua la nivelul autorității competente în procesul de evaluare a conformității măsurilor de securitate implementate cu riscurile la adresa rețelelor și sistemelor informatice ale furnizorului de servicii.

Alineatul (2³) asigură transpunerea la nivel de norme primare a prevederilor alin. (3) din art. 21 al Directivei NIS2 și este adresat obligațiilor furnizorilor de servicii în implementarea măsurilor de securitate privind asigurarea securității lanțului de aprovizionare, inclusiv aspectele, legate de securitate, referitoare la relațiile furnizorului de servicii cu prestatorii sau cu furnizorii direcți de servicii ai acestuia. La determinarea proporționalității și corespondenței măsurilor de securitate riscurilor identificate de furnizorului de servicii, acesta trebuie să țină seama de vulnerabilitățile prestatorilor săi de servicii și de evaluările riscurilor privind lanțul de aprovizionare, efectuate de autoritățile competente ale Uniunii Europene, în mod specific de Grupul de cooperare.

Propunerea de modificare de la **alineatul (4) lit. b)** este determinată de necesitatea reconsiderării redacției acestui alineat prin prisma faptului că pentru implementarea prevederilor legii sunt necesare (și au fost deja stabilite) cerințe privind măsurile de securitate cu caracter orizontal valabile pentru toți furnizorii de servicii în toate sectoarele și subsectoarele critice. Adoptarea unor cerințe specifice este o prerogativă care vizează competența autorităților publice sectoriale, complementată de competența

orizontală a MDED în domeniul securității cibernetice. Determinarea necesității unor cerințe specifice anumitor sectoare critice intră în sfera de acțiune a atribuțiilor de elaborare, promovare și implementare a politicii de stat în sectorul sau subsectorul critic respectiv.

Punctul 11 al art. II cuprinde modificări la art. 12 din Legea nr. 48/2023 care au ca obiectiv transpunerea prevederilor art. 23 din Directiva NIS2. Propunerile vizează precizarea unor aspecte esențiale în procesul de raportare a incidentelor cibernetice semnificative de către furnizorii de servicii către ASC. Aceste aspecte se referă la consecutivitatea acțiunilor de raportare și conținutul informațiilor ce urmează a fi prezentate autorității competente în acest scop. Astfel în lege se propune introducerea termenilor de avertizare timpurie, notificare, raport intermediar și raport de progres. **Avertizarea timpurie**, prevăzută actualmente la alin. (1), nu este menționată expres și nu îi este definit conținutul. Conform propunerii aceasta urmează să conțină informațiile care sunt disponibile la furnizorul de servicii la momentul remiterii acesteia ASC. **Notificarea** este, de asemenea, prevăzută în redacția actuală a legii la alin. (3) din art. 12. Totuși din rațiuni de asigurare a conformității, inclusiv terminologice cu legislația UE, este necesară formalizarea denumirii acesteia pentru a o distinge de celelalte componente ale obligațiilor de raportare a incidentelor cibernetice semnificative. **Raportul intermediar** se introduce în textul legii prin completarea cu alin. (7¹). Regimul juridic al acestei obligații de raportare însă este diferit. Factorul declanșator în cazul raportului respectiv este solicitarea expresă venită din partea autorității competente. În ce privește **raportul final** acesta este reglementat actualmente de alin. (8) din art. 12. Totuși pentru a asigura conformitatea cu cerințele de conținut stabilite de art. 23 alin. (4) lit. d) din Directiva NIS2 în proiect se propune o nouă redacție a acestui alineat. De asemenea alineatul respectiv se completează în final cu o prevedere care are scopul soluționării situațiilor când la scadența termenului de prezentare a raportului final, incidentul cibernetic este încă în desfășurare. În aceste situații furnizorul de servicii urmează să remită ASC un **raport de progres**, iar raportul final într-un termen de o lună de la soluționarea incidentului cibernetic. Recitalurile 101 și 102 din preambulul la Directiva NIS2 vin cu o explicare detaliată a rațiunilor care stau la baza mecanismul de raportare prevăzut de Directiva respectivă.

Propunerea de completare a articolului cu **alin. (3¹)** este o normă juridică specială în raport cu norma generală prevăzută la alin. (3) pentru prestatorii de servicii de încredere. În cazul acestora obligația de notificare este una mai severă, dat fiind gradul ridicat de importanță critică a activelor (date, informații, sisteme) care ar putea fi afectate și impactul pe care ar putea să-l aibă un incident cibernetic asupra serviciilor de încredere, precum și prejudiciile care ar putea să le producă. Alineatul respectiv asigură transpunerea paragrafului al doilea din alin. (3) al art. 23 din Directiva NIS2.

Redacția **alineatului (6¹)**, propusă în proiect transpune prevederile alin. (7) din art. 23 al Directivei NIS2. Această prevedere oferă dreptul discreționar limitat de consultarea furnizorului de servicii vizat, să informeze publicul în situații de excepție. Scopul unei astfel de informări asigurarea nu doar a interesului public, dar și protecția drepturilor individuale ale utilizatorilor serviciilor esențiale. Furnizarea informațiilor respective trebuie să aibă ca efect oferirea oportunității utilizatorilor de a lua măsuri adecvate pentru a se proteja.

Alineatul (8¹) transpune prevederile propoziției a patra din primul paragraf și al ultimului paragraf din alin. (1) al art. 23 din Directiva NIS2. Acest alineat instituie obligația expresă pentru furnizorii de servicii să notifice autoritatea competentă cu privire la informațiile care permit calificarea incidentului ca fiind cu impact transfrontalier. Această obligație este strâns conectată cu obligațiile autorității competente și ale Republicii Moldova în general de cooperare la nivelul Uniunii Europene atât cu statele membre ale acesteia, cât și cu instituțiile UE și cu obligațiile care decurg din directiva NIS2 în ce privește schimbul de informații în materie de securitate cibernetică. În acest sens, **alineatul**

(8²) care transpune prevederile alin. (6) al art. 23 din Directiva NIS2, stabilește expres obligații de raportare pentru autoritatea competentă a incidentelor cibernetice cu impact semnificativ, care afectează două sau mai multe state membre, către statele membre și ENISA. Această obligație însă este limitată de prevederile alineatului (8³) la necesitatea de a proteja interesele furnizorului de servicii. Autoritatea competentă în realizarea acestei obligații trebuie să asigure respectarea principiului proporționalității cu scopurile urmărite. Prevederea propusă la alin. (8¹) trebuie aplicată în coroborare cu prevederile propuse în alin. (2)-(4) din articolul 7¹ propus în proiect. Alineatul (8³) stabilește obligații pentru autoritatea competentă în ce privește protecția intereselor de securitate și comerciale ale furnizorului de servicii. Această obligație se extinde asupra întregului spectru de activități ale autorității competente în gestionarea informației care îi devine cunoscută în procesul gestionării incidentelor cibernetice semnificative. Alineatul respectiv reflectă și prevederile alin. (4) al art. 15 din redacția actuală a Legii nr. 48/2023.

Abrogarea alin. (10) din art. 12 este determinată de transferul acesteia în art. 13, dat fiind natura voluntară a acestei obligații de raportare, și absorbirea acestei norme de alin. (1) al art. 13.

Alineatul (11) deși este expus într-o redacție nouă, totuși păstrează esența actualei redacții din Legea nr. 48/2023. În noua redacție se vine cu unele îmbunătăți determinate de necesitatea clarificării modului de realizare a obligațiilor de notificare stabilite de art. 12, de către furnizorii de servicii din sectorul public. Având în vedere că una din caracteristicile modelului de guvernare în domeniul securității cibernetice în Republica Moldova este separarea rolului de CERT-Gov de autoritatea competentă, în cadrul unui model de guvernare mai degrabă centralizat, este necesară elucidarea aspectului privind îndeplinirea obligațiilor de notificare a incidentelor cibernetice cu impact semnificativ de către furnizorii de servicii din sectorul public. Astfel pentru aceștia obligația va fi realizată din momentul notificării conform prevederilor alineatelor anterioare ale art. 12 a STISC. La rândul STISC este responsabil de notificarea CSIRT național cu privire la incidentele cibernetice cu impact semnificativ produse în sectorul public. De notat că persoanele juridice de drept public nu sunt obligate în temeiul legii să notifice celelalte incidente cibernetice (care nu au impact semnificativ) către STISC. Această obligație decurge din actele normative ale Guvernului și actele operaționale semnate de către aceștia cu STISC. Totodată, trebuie de remarcat că prevederile Legii nr. 48/2023 stabilesc un set de cerințe minime ce trebuie îndeplinite pentru a asigura conformitatea cu aceasta. Din această perspectivă furnizorii de servicii din sectorul public sunt în drept să notifice CSIRT național direct despre incidentele cu impact semnificativ.

Alineatul (11¹) transpune alin. (10) al art. 23 din Directiva NIS2 și se înscrie în contextul mai larg de necesitate de asigurare a unei cooperări strânse dintre autoritățile competente în domeniul protecției fizice a infrastructurii critice cu autoritate competentă de protecția cibernetică a acestei infrastructuri.

Punctul 12 al art. II cuprinde propuneri de modificare a **art. 13** din Legea nr. 48/2023. Noua redacție a alin. (1) din acest articol este determinată de necesitatea asigurării conformității de conținut cu prevederile art. 30 din Directiva NIS2 și conferirii textului mai multă coerență și precizie. De asemenea, redacția respectivă a absorbit prevederea de la alin. (10) art. 12 în redacția legii în vigoare. Modificările propuse la alineatele (2) și (3) sunt în principiu conexe noii redacții a alineatului (1).

Punctul 13 al art. II propune abrogarea **art. 14, art. 15 și art. 16** din Legea nr. 48/2023.

Art. 14 reglementează aspecte generale privind măsurile de securitate privind rețelele și sistemele informatice ale persoanelor juridice de drept public. În contextul actual, când Guvernul, pentru organizarea executării prevederilor art. 11 și art. 12 din Legea nr. 48/2023, a adoptat Hotărârea

sa nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii, abrogând și Hotărârea Guvernului nr. 201/2017 cu privire la cerințele minime obligatorii de securitate cibernetică în sectoarele critice, prevederile art. 14 au devenit desuete.

Abrogarea art. 15 este determinată de faptul că prevederile acestuia fie au fost transferate în cuprinsul altor articole, fie sunt cuprinse de alte propuneri de modificare din proiectul de lege. În primul caz este vorba de alin (1) care a fost transferat la alin. (4) din art. 7 (pct. 7 art. II din proiectul de lege), alin. (2) și alin. (3), care au fost transferate la alin. (8) din art. 19 (pct. 16 art. II din proiectul de lege) și alin (4) care a fost înglobat de redacția alineatului (8³) a art. 12 (punctul 11 art. II din proiectul de lege.). În al doilea caz, alin. (5) se regăsește în alin. (1) art. 7³ (pct. 8 din art. II al proiectului de lege).

Abrogarea art. 16 este determinată de necesitatea transferării conținutului acestuia la noul articol 7³ care absoarbe obiectul de reglementare al art. 16.

Punctul 14 al art. II conține propunerea de modificare a alineatelor (2) și (3) din art. 17 al Legii nr. 48/2023. Acest articol reglementează aspecte ce țin de schimbul voluntar de informații și asigură transpunerea prevederilor art. 29 din Directiva NIS2. Modificările în principiu asigură o transpunere textuală a prevederilor din actul juridic al UE din rațiuni de asigurare a conformității cu efectele pe care aceste prevederi le vor produce. Trebuie de remarcat faptul că în sensul conceptului propus în proiect, care derivă din cel reglementat la nivelul UE, termenul *acord* trebuie înțeles ca mecanisme sau aranjamente/înțelegeri și nu în sensul unor acte juridice formale semnate de părțile participante. Aceste mecanisme de schimb voluntar de informații în materie de securitate cibernetică vizează nu doar semnarea unor acte juridice formale, ci stabilesc cadre structurate la nivelurile organizatoric și procedural, juridic și tehnic. Din aceste considerente prin modificările operate din textul legii exclus termenul de *semnare*, pentru a nu restrânge conținutul acestor acorduri și ai păstra sensul mai larg oferit de articolul respectiv din Directiva NIS2.

În punctul 15 al art. II din proiect se propune o nouă redacție a art. 19 care are ca obiect de reglementare aspecte privind activitatea de control de stat al respectării legislației în domeniul securității cibernetice. Conform pct. 15 din anexa la Legea nr. 131/2012, organul de control în acest domeniu este ASC. Directiva NIS2 stabilește o *diferențiere între regimul de supraveghere al entităților esențiale și cel al entităților importante, în vederea asigurării unui echilibru echitabil al obligațiilor pentru entitățile respective și pentru autoritățile competente*. Recitalul (122) explică această diferențiere: „entitățile esențiale ar trebui să fie supuse unui regim de supraveghere ex ante și ex post cuprinzător, în timp ce entitățile importante ar trebui să fie supuse unui regim de supraveghere simplificat, doar ex post. Entitățile importante nu ar trebui, așadar, să aibă obligația să documenteze în mod sistematic respectarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică, în timp ce autoritățile competente ar trebui să pună în aplicare o abordare reactivă ex post a supravegherii și, prin urmare, să nu aibă o obligație generală de a supraveghea entitățile respective. Supravegherea ex post a entităților importante poate fi declanșată de dovezi, indicii sau informații aduse la cunoștința autorităților competente, cu privire la care aceste autorități consideră că sugerează potențiale încălcări ale prezentei directive. De exemplu, astfel de dovezi, indicii sau informații ar putea fi de tipul celor furnizate autorităților competente de către alte autorități, de entități, cetățeni, mass-media sau alte surse, sau informații aflate la dispoziția publicului, sau ar putea rezulta din alte activități desfășurate de autoritățile competente în îndeplinirea sarcinilor lor.” Propunerile incluse în proiect urmează aceeași logică cu excepția faptului comasării prevederilor conținute în art. 32 și 33 din Directiva NIS2 într-un singur articol,

Conform proiectului (**alineatele (1), (2) și (3)**) normele cuprinse în noua redacție a art. 19 vor avea caracter special în raport cu normele juridice cuprinse în Legea nr. 13/2012, iar în cazul în care anumite aspecte ale desfășurării activității de control nu sunt reglementate de cea din urmă, prevederile Codului administrativ vor fi aplicate corespunzător. Prevederile noii redacții ale art. 19 asigură transpunerea integrală a prevederilor art. 31, art. 32 și art. 33 din Directiva NIS2. Preluarea normelor juridice din directivă a fost însoțită de o ajustare terminologică la sistemul legal național, în special s-a asigurat conformitate cu terminologia Legii nr. 13/2012 (Spre exemplu, termenul de *inspecții la fața locului*, utilizat în art. 32 alin. (2) lit. a) și art. 33 alin. (2) lit. a) a fost transpus prin termenul *control la fața locului*, iar termenul de supraveghere ex-situ – prin termenul *control prin solicitare directă a informației*. Termenul *audituri ad-hoc* utilizat în art. 33 alin. (2) lit. c) din Directiva NIS2 a fost transpus în lege prin termenul de *control inopinat*). **Alineatul (4)** consfințește principiul unei abordări bazate pe riscuri în planificarea și efectuarea controalelor. Principiu care este statuat de art. 31 alin. (2) din Directiva NIS2 și similar principiul stabilit la art. 3 alin. (1) lit. c) din Legea nr. 131/2012. **Alineatul (5)** enumeră împuternicirile ASC în exercitarea controlului de stat, acestea transpun prevederile art. 32 alin. (2) și art. 33 alin. (2). **Alineatul (6)** determină cerințele pentru efectuarea auditurilor de securitate specifice. Conform lit. b) de la alineatul anterior, ASC poate dispune efectuarea unor astfel de audituri de către organisme independente. Acestea sunt un instrument util atât pentru ASC cât și pentru furnizorii de servicii în evaluarea obiectivă și imparțială a conformității furnizorului de servicii cu cerințele stabilite de legislație. **Alineatul (7)** stabilește măsurile de asigurare a respectării legii, transpunând prevederile art. 32 alin. (4) și respectiv, art. 33 alin. (4) din Directiva NIS2. Astfel ca măsuri de asigurare a respectării legii sunt avertismentul, înaintarea prescripțiilor cu privire la îndeplinirea anumitor activități orientate spre remedierea deficiențelor, restricționarea utilizării ori accesului la o rețea sau un sistem informatic, desemnarea unui responsabil de monitorizarea conformării și amenda.

Măsura prevăzută la lit. c) alin. (7) al art. 19 și descrisă la **alineatul (8)** din art. 19 - restricționarea utilizării ori accesului la o rețea sau un sistem informatic - deși nu este prevăzută expres de art. 32 și 33 din Directiva NIS2, totuși se înscrie în conceptul instrumentarului de care trebuie să depună autoritățile competente în asigurarea respectării legii stabilit de Directiva NIS2. Astfel în recitalul 126 din preambulul la directivă se menționează că: „În cazuri justificate în mod corespunzător în care are cunoștință de o amenințare cibernetică semnificativă sau de un risc iminent, autoritatea competentă ar trebui să fie în măsură să ia decizii imediate de executare cu scopul de a preveni un incident sau de a răspunde la acesta.”. Această măsură ar trebui să constituie o măsură de ultim resort, atunci când alte măsuri sau dovedit a fi inutile. Principiul *ultima ratio* trebuie aplicat în coroborare cu cel al *proporționalității*, atunci când autoritate competentă va lua decizia de a aplica această măsură. Măsura restricționării utilizării ori accesului la o rețea sau un sistem informatic este în esență o măsură restrictivă în sensul art. 29¹ din Legea nr. 131/2012 și prin urmare, normele juridice relevante din această lege trebuie aplicate atunci când se va face uz de această măsură. Acest fapt asigură suficiente garanții juridice furnizorilor de servicii sau altor persoane în fața potențialelor abuzuri din partea ASC. Trebuie de remarcat că măsura dată poate fi aplicată rețelelor și sistemelor informatice ale furnizorilor de servicii și rețelelor și sistemelor informatice ale altor persoane dacă incidentul cibernetic produs în acestea compromise sau dăunează securității rețelei sau sistemului informatic al furnizorului de servicii. De asemenea, este important de relevat că atunci când aplică măsura respectivă, ASC trebuie să se asigure că toate condițiile prevăzute la literale a)-d) sunt îndeplinite cumulativ și în volum deplin. **Alineatul (9)** cuprinde măsuri de asigurare a aplicării legii care pot fi aplicate doar furnizorilor esențiali de servicii și doar în cazul în care măsurile prevăzute la 7) lit. a) și lit. b) punctele 1) – 3) și 5) s-au dovedit a fi ineficiente. La **alineatul (10)** sunt stabilite condițiile minime de individualizare a măsurilor

de asigurare a respectării legii, de care autoritatea competentă trebuie să țină cont. **Alineatul (11)** stabilește lista încălcărilor legii care urmează a fi considerate grave. La aplicarea acestui alineat, ASC trebuie să țină cont și să aplice în mod corespunzător și prevederile art. 5¹ alin. (3) lit. c) din Legea nr. 131/2012 cu privire la controlul de stat, conform căreia sunt considerate *foarte grave – încălcări ale legislației a căror înlăturare nu este posibilă în timpul controlului, însă acțiuni în acest sens necesită a fi întreprinse imediat, și care creează un pericol iminent și imediat pentru drepturile și libertățile fundamentale care fac obiectivul prezentei legi, pentru mediu ori pentru viața, sănătatea și proprietatea persoanei controlate și/sau angajații acesteia ori creează pericol iminent și imediat pentru societate. Sunt echivalente cu încălcări foarte grave încălcările grave care nu au fost înlăturate în termenul indicat în prescripție.* **Alineatul (12)** determină condițiile de aplicare a prevederilor art. 19 în privința furnizorilor importanți de servicii. După cum s-a relevat mai sus în informațiile conținute în recitalurile din preambulul la Directiva NIS2, față de această categorie de furnizori de servicii urmează a fi aplicată o procedură simplificată de supraveghere care în principal se caracterizează prin faptul că măsurile de control de stat și cele de asigurare a respectării legii pot fi aplicate doar post factum, adică doar dacă există anumite dovezi din diverse surse care ar putea oferi suficiente temeiuri de a suspecta o potențială încălcare a legii. **Alineatele (13) – (14)** cuprind norme care reglementează aspecte specifice de cooperare a autorității competente în temeiul Legii nr. 48/2023 cu autorități de supraveghere precum Banca Națională a Moldovei, Comisia Națională a Pieței Financiare, precum și au autoritățile publice cu funcții de supraveghere și control în domeniul protecției fizice a infrastructurii critice.

În punctul 16 al art. II se propune completarea Legii nr. 48/2023 cu articolele 19¹, 19² și 19³. Aceste completări vizează transpunerea prevederilor articolelor 34-37 din Directiva NIS2.

Astfel **articolul 19¹** are ca obiect de reglementare cuantumul amenzilor pentru încălcarea prevederilor legislației în domeniul securității cibernetice. Art. 19¹ și **propunerile de completare la Codul contravențional de la art. I** stabilesc regimul sancționator pentru încălcările legislației în domeniul securității cibernetice. Alegerea opțiunii reflectate în proiectul de lege este determinată de art. 10 din Codul contravențional, conform căruia în mod sintetic pasibilă de sancțiune contravențională este doar fapta prevăzută de Codul Contravențional. Aplicarea doar a regimului sancționator prevăzut de Codul contravențional nu este posibil având în vedere că regimul sancționator al Directivei NIS2 stabilește amenzi în cuantumuri care depășesc limitele admise de prevederile art. 34 din Codul contravențional.

Totuși în proiect sunt propuse completări la Codul contravențional, acestea însă au ca subiect al contravenției persoana fizică, angajat al furnizorului de servicii, care se face vinovată de comiterea contravențiilor respective.

Justificarea unei astfel de abordări este dată de recitalul (130) din preambulul la Directiva NIS2: *În cazul în care o amendă administrativă este aplicată unei entități esențiale sau unei entități importante care este o întreprindere, întreprinderea ar trebui înțeleasă ca fiind o întreprindere în conformitate cu articolele 101 și 102 din TFUE în aceste scopuri. În cazul în care o amendă administrativă se aplică unei persoane care nu este o întreprindere, autoritatea competentă ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al amenzii. Competența de a stabili dacă și în ce măsură autorităților publice ar trebui să li se poată aplica amenzi administrative ar trebui să revină statelor membre. Aplicarea unei amenzi administrative nu aduce atingere exercitării altor competențe de către autoritățile competente sau aplicarea altor sancțiuni prevăzute în normele naționale de transpunere a prezentei directive.*

Articolul 19² reglementează aspecte materiale și de procedură în cazurile când o încălcare de către furnizorul de servicii a legislației în domeniul securității cibernetice poate atrage după sine o încălcare a securității datelor cu caracter personal. Dacă în acest caz CNPDCP aplică o amendă, ASC nu va aplica amendă pentru același comportament. Prevederile **alinatului (2)** sunt în principiu o reflectare normativă a principiului ne bis in idem. Alineatul (3) reglementează situația când o încălcare a legii are caracter transfrontalier și intră în competența unei autorități de supraveghere în domeniul protecției datelor cu caracter personal dintr-un alt stat membru al UE. În acest caz autoritatea competente se adresează cu privire la potențiala încălcare autorității naționale competente în domeniul protecției datelor cu caracter personal.

Articolul 19³ are ca obiect de reglementare asistența reciprocă dintre autoritățile competente în domeniul securității cibernetice din statele membre ale Uniunii Europene pe chestiuni care vizează exercitarea supravegherii modului în care sunt respectate prevederile legislației în domeniul respectiv. Asistența respectivă este guvernată de principiul reciprocității și cel al proporționalității. **Alineatul (2)** lit. c) reflectă principiul proporționalității asistenței cu resursele de care dispune autoritatea competentă. **Alineatul (4)** determină exhaustiv cazurile când autoritatea competentă poate refuza o cerere de asistență: lipsa competenței legale, disproporționalitatea asistenței, afectarea securității naționale. Alineatul (7) transpune prevederile art. 26 alin. (5) din Directiva NIS2.

Punctul 17 al art. II propune revizuirea redacției articolului 20. Revizuirea este determinată de necesitatea transpunerii alin. (14) al art. 2 din Directiva NIS2.

Articolul I din proiectul de lege cuprinde propuneri de completare a Codului Contravențional cu art. Articolul 259³ *Încălcarea legislației în domeniul securității cibernetice* și Articolul 259⁴ *Împiedicarea activității Agenției Naționale pentru Securitate Cibernetică*. De asemenea, completarea vizează și introducerea articolului **Articolul 410¹** *Agenția pentru Securitate Cibernetică* în cartea a doua care reglementează chestiunile de procedură ale procesului contravențional. Propunerile de completare a codului vizează incriminarea faptelor de încălcare a cerințelor stabilite de art. 11 alin. (1), (2), (2²), (2³) sau (3) ori de art. 12 alin. (1), (3), (3¹), (4), (6), (7¹), (8) sau (8¹) din Legea nr. 48/2023 privind securitatea cibernetică. Subiecți ai contravențiilor respective sunt persoanele fizice și persoanele cu funcție de răspundere angajați ai furnizorului de servicii.

Art. III din proiectul de lege vizează modificări la Legea nr. 72/2026 comunicațiilor electronice adoptată recent. Punctele 1 și 2 cuprind modificări ale art. 3 din legea respectivă care au ca obiectiv transpunerea prevederilor art. 28 din Directiva NIS2. Acesta articol reglementează aspectele fundamentale privind Baza de date europeană pentru datele de înregistrare a numelor de domenii. Cerința actului UE este ca statele membre să asigure ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să colecteze și să mențină date exacte și complete privind înregistrarea numelor de domenii într-o bază de date dedicată, cu diligența necesară, în conformitate cu dreptul Uniunii în materie de protecție a datelor cu caracter personal. Deși Legea nr. 72/2026 actele²⁵ de punere a acestora în aplicare reglementează într-o anumită măsură aspectele

²⁵ Hotărârea ANRCETI nr. 42 /2020 privind aprobarea Regulamentului cu privire la gestionarea domeniului de nivel superior .md

respective, totuși acestea sunt destul de generale și nu abordează toate problematicile abordate în art. 28 al Directivei NIS2. Având în vedere natura obligațiilor impuse de art. 28 din directivă obiectul de reglementare a modificărilor propuse în proiect se încadrează mai degrabă în obiectul mai larg de reglementare a Legii nr. 72/2026. Din aceste rațiuni modificările respective sunt propuse la acest act și nu în Legea nr. 48/2023.

În ce privește propunerea de **abrogare a literei i) din alin. (2) al art.8**, menționăm că din punct de vedere al terminologiei utilizate - „*politici privind securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice accesibile publicului*” – se creează confuzia existenței unei arii de intervenție distinctă de cea a domeniului securității cibernetice sau a domeniului comunicațiilor electronice . Acest termen este absorbit de noțiunile de *rețea și sistem informatic* și noțiunea de securitate a rețelelor și sistemelor informatice prevăzute de art. 2 din Legea nr. 48/2023. Domeniile reglementate sunt cel al securității cibernetice, dat de Legea nr.48/2023, și cel al comunicațiilor electronice, dat de Legea nr. 72/2026. Anume aceste domenii ca arii determinate legal-juridic și obiectiv, delimitează competența de intervenție a autorităților publice corespunzătoare pe eșichierul realizării politicii statului în aceste domenii: elaborare-implementare-monitorizare-evaluare. Utilizarea unor construcții diferite va crea confuzii și inconsistențe nu doar în înțelegerea ariei de intervenție și a autorității competente, dar și a modului de aplicare a normei juridice materiale.

Art. IV din proiectul de lege cuprinde dispozițiile finale. Alineatul (1) stabilește termenul de intrare în vigoare la data publicării, cu excepția prevederilor ale căror aplicare este condiționată de obținerea calității de stat membru a Uniunii Europene de către Republica Moldova. **Alineatul (2)** face clarificări cu privire la inițierea realizării obligațiilor de informare stabilite de art. 7¹ alin. (1). În textul Directivei NIS2 sunt stabilite termene specifice pentru autoritățile competente ale statelor membre ale UE de realizare a acestor obligații pentru prima dată. În cazul Republicii Moldova această situație trebuie reglementată într-un mod diferit, având în vedere că data aderării este ulterioară termenelor stabilite de directivă. Alineatul (3) stabilește un termen de 3 luni pentru realizarea inițială a obligației de informare prevăzută la art. 4³ alin. (1), pentru categoria respectivă de furnizori de servicii. termenul de 3 luni a fost stabilit similar termenului de 3 luni pentru prezentarea modificărilor acestor informații stabilit de art. 27 alin. (3) din Directiva NIS2. Alineatul (4) stabilește în sarcina Guvernului aducerea legislației sale în conformitate cu prevederile legii. În context, notăm că modificările respective vor avea un caracter tehnic, având în vedere că proiectul de lege, deși cuprinde multiple modificări și completări nu afectează conceptul modelului de guvernanță în domeniul securității cibernetice, instituit inițial prin Legea nr. 48/2023.

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

Proiectul de lege are ca obiectiv principal finalizarea procesului de armonizare a legislației naționale la prevederile Directivei NIS2. Modificările și completările care sunt propuse să fie operate în Legea nr. 48/2023 privind securitatea cibernetică nu intervin cu schimbări conceptuale sau structurale a mecanismelor și soluțiilor introduse inițial în sistemul legislativ național prin adoptarea Legii nr 48/2023. Din aceste considerente, prin prisma prevederilor alineatului patru din pct. 3.2 din Instrucțiunea privind efectuarea analizei impactului de reglementare și modul de reflectare a rezultatelor acesteia în nota de fundamentare (anexa la Metodologia de analiză a impactului de reglementare, aprobată prin Hotărârea Guvernului nr. 574/2024), nu au fost examinate opțiuni alternative dat fiind faptul că Directiva NIS2 stabilește în mod clar mecanismele prin care această directivă urmează a fi implementată la nivel național.

În ce privește riscurile lipsei de intervenție, menționăm că lipsa de intervenție, cu alte cuvinte opțiunea de a nu face nimic ar presupune de a nu finaliza procesul de armonizare a legislației naționale

la prevederile Directivei NIS2. Aceasta implică riscuri legate de procesul de integrare europeană a Republicii Moldova, în particular în ce privește angajamentele de aliniere a cadrului normativ la aquis-ul comunitar. În acest caz prin prisma principiului proporționalității efortului, stabilit de pct. 6.6. din Metodologia de analiză a impactului de reglementare considerăm inutilă analizarea acestei problematice, având în veder caracterul eminentamente formal al unei astfel de analize.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Proiectul de lege nu are impacturi structurale și/sau instituționale asupra sistemului administrației publice și, prin urmare, adoptarea modificărilor propuse în acesta nu implică acțiuni de reformă structurală sau instituțională. Modelul de guvernanta în domeniul securității cibernetice, reflectat actualmente în Legea nr. 48/2023 nu va suferi modificări de ordin structural sau instituțional. ASC păstrează rolurile determinate de legea actuală și cadrul normativ guvernamental subsidiar exercitând în continuare atribuțiile de autoritate competentă în domeniul securității cibernetice (în sensul art.8, și 11 din Directiva NIS2) inclusiv de echipă națională de răspuns la incidente cibernetice și punct național unic de contact, precum și de autoritate de gestionare a crizelor cibernetice (în sensul art.9 din Directiva NIS2).

Sub aspect funcțional, proiectul de lege vine cu o dezvoltare a atribuțiilor ASC din perspectiva cooperării și schimbului de informații a acesteia cu autoritățile relevante ale Uniunii Europene și cu statele membre ale acesteia. Actualmente Legea 48/2023 la art. 7 alin. (3) lit. c) deja prevede o atribuție distinctă de a asigura interacțiunea strategică la nivel internațional și schimbul de experiență cu alte state, organizații internaționale sau entități create de acestea privind aspectele legate de securitatea cibernetică.

De asemenea, în prezent ASC desfășoară procesul de identificare a furnizorilor de servicii care vor cădea sub incidența prevederilor legii. Extinderea domeniului de aplicare a prevederilor legii și la persoanele fizice care desfășoară activitatea de întreprinzător ar putea sugera un efort suplimentar din partea ASC și, prin urmare necesitatea suplimentării statelor de personal cu unități suplimentare. Totuși acest aspect este contrabalansat de faptul că persoanele juridice de drept public urmează a fi identificate prin efectul legii fără a desfășura procedura de identificare clasică stabilită de regulamentul, aprobat prin Hotărârea nr. 860/2024.

4.2. Impactul financiar și argumentarea costurilor estimative

Modificările propuse în proiectul de lege nu necesită alocarea unor mijloace financiare suplimentare în bugetul autorităților responsabile de implementarea legii. Mijloacele financiare ce au fost alocate sau urmau a fi alocate pentru implementarea prevederilor Legii nr. 43/2023 privind securitatea cibernetică nu ar trebui să crească nici din perspectiva furnizorilor de servicii persoane juridice de drept public nici din perspectiva autorităților publice competente și responsabile de asigurarea punerii în aplicare a legii. Cu alte cuvinte persoanele juridice de drept public, în calitatea lor de furnizori de servicii, nu sunt supuse unor obligații legale suplimentare (în ce privește măsurile de securitate sau obligațiile de notificare) și, prin urmare, nici costuri suplimentare pentru realizarea acestor obligații nu sunt preconizate. O estimare inițială a impactului financiar din acest punct de vedere a fost realizat în contextul promovării proiectului de lege privind securitatea cibernetică²⁶ și a actelor normative de implementare a acesteia, în mod special impactul financiar estimat în nota de

²⁶ Dosarul de însoțire al proiectului respectiv de lege poate fi consultat aici:

<https://old.parlament.md/ProcesulLegislativ/Proiectedeactenormative/tabid/61/LegislativId/6386/language/ro-RO/Default.aspx>

fundamentare²⁷ la proiectul de hotărâre a Guvernului „Cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice” (Hotărârea Guvernului nr. 562/2025). Considerăm oportun de relevat aici că în nota respectivă în ce privește costurile de implementare a măsurilor de securitate pentru furnizorii de servicii din sectorul public, au fost relevate unele aspecte abordate de către Comisia Europeană în Analiza²⁸ 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%....”*

În ce privește impactul financiar al realizării de către ASC a activităților de implementare, menționăm că prevederile proiectului de lege nu implică cheltuieli suplimentare la cele care sunt deja prevăzute în bugetul de stat. Aceste cheltuieli sunt asociate realizării de către ASC a competenței sale în ce privește implementarea politicii de stat în domeniul securității cibernetice, inclusiv cele care derivă din exercitarea funcțiilor de cooperare și schimb de informații cu instituțiile Uniunii Europene și cu statele membre ale acesteia.

4.3. Impactul asupra sectorului privat

Impactul asupra sectorului privat din perspectiva Legii cu privire la securitatea cibernetică a fost expus în analiza de impact la proiectul de lege privind securitatea cibernetică și în analizele de impact la actele normative secundare, cuprinse în notele de fundamentare la proiectele respective de acte normative guvernamentale. Informațiile respective rămân valabile pentru aprecierea impactului, inclusiv și în mod special al celui financiar, asupra sectorului privat, pe care îl vor avea prevederile legale.

Deși propunerile de modificare a legii cuprinse în proiectul de față nu implică noi costuri de conformare din partea titularilor de obligații, totuși având în vedere că domeniul de aplicare al legii se extinde, în limita sectoarelor critice și tipurilor de întreprinderi, și la persoanele fizice care practică activitate de întreprinzător, considerăm oportun de reiterat unele informații relevante expuse în analizele anterioarei.

Astfel din punctul de vedere a asigurării conformității furnizorilor de servicii cu obligațiile impuse de lege, relevăm potrivit Raportului²⁹ 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

²⁷ Pct. 8 din ordinea de zi a ședinței Guvernului din 3 septembrie 2025: <https://gov.md/ro/sedinte-de-guvern/sedinta-guvernului-din-3-septembrie-2025-ora-1000>.

²⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52020SC0345>

²⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020SC0345>, pag. 71

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 ASC 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 acestea, 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)³⁰ 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”.

În analiza de impact³¹ 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 întreprinderile, cât și economia europeană vor fi bine poziționate pentru a profita de avantajele pieței globale a securității cibernetică, 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 cibernetică valora 63,7 miliarde de dolari și se preconizează că va crește între 80 și 120,1 miliarde de dolari până în 2017.”

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:

³⁰ <https://www.enisa.europa.eu/publications/nis-investments-2024>

³¹ <https://old.parlament.md/ProcesulLegislativ/Proiectedeactenormative/tabid/61/LegislativId/6386/language/ro-RO/Default.aspx>

- 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.
- 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

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.

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 parte, 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

Analiza impacturilor prevăzute în compartimentul 4 se finalizează cu concluzii privind necesitatea/oportunitatea sau lipsa necesității/oportunității intervenției statului pentru soluționarea unor probleme și privind identificarea celei mai bune soluții. Concluziile sunt formulate conform următoarelor criterii:

- eficacitatea opțiunii preferate în atingerea obiectivelor urmărite, inclusiv în comparație cu opțiunile alternative, după caz;

- măsura în care opțiunea preferată ar putea genera beneficii care justifică costurile asociate, inclusiv în comparație cu opțiunile alternative, după caz;
- măsura în care opțiunea preferată ar asigura cel mai mic nivel posibil al costurilor pentru cei afectați.

În cazul actelor normative cu relevanță UE, pentru prevederile care sunt expres reglementate în actul juridic european, acest subcompartiment se completează simplificat, fiind obligatoriu de expus doar concluziile privind măsura în care proiectul de act normativ ar asigura cel mai mic nivel posibil al costurilor pentru cei afectați.

5. Compatibilitatea proiectului actului normativ cu legislația UE

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

Proiectul de lege propus spre examinarea are ca scop transpunerea integrală a Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr.910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), publicată în Jurnalul Oficial al Uniunii Europene seria L nr.333 din 27 decembrie 2022.

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

Legea nr. 48/2023 privind securitatea cibernetică, actualmente în vigoare, transpune în mare parte prevederile Directivei NIS 2, la nivelul cadrului normativ primar. Totodată, un set de acte normative au fost adoptate la nivel guvernamental în vederea implementării prevederilor primare ale legii, dar și transpunerea directă a unor prevederi din Directiva NIS2 și ale unor acte juridice ale UE subsidiare acestei Directive. Setul de acte normative care transpun prevederile directivei sunt enumerate și descrise succint în punctul 2.2 din prezenta notă de fundamentare.

Următoarele acte juridice ale UE au fost transpuse prin actele normative guvernamentale respective, și anume prin Hotărârea Guvernului nr. 860/2024 *privind identificarea furnizorilor de servicii* și Hotărârea Guvernului nr. 562/2025 *cu privire la modul de realizare a obligațiilor de asigurare a securității ciberetice de către furnizorii de servicii în sectoarele critice*:

- **Regulamentul de punere în aplicare (UE) 2024/2690³² 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, publicat în Jurnalul Oficial al Uniunii Europene L din 18 octombrie 2024, CELEX: 32024R2690;

- Comunicarea Comisiei **Orientările Comisiei³³ privind aplicarea articolului 4 alineatele (1) și (2)** din Directiva (UE) 2022/2555 (Directiva NIS 2);

³² <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R2690;>

³³ [https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918\(01\);](https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918(01);)

- Comunicarea Comisiei ***Orientările Comisiei³⁴ privind aplicarea articolului 3 alineatul (4)*** din Directiva (UE) 2022/2555 (Directiva NIS 2).

Actele normative naționale deja adoptate împreună cu prevederile proiectului de lege propus spre examinare vor asigura transpunerea integrală, la nivel juridico-normativ, a prevederilor Directivei NIS2.

În principiu prevederile proiectului de lege asigură o armonizare minimă, inclusiv din perspectiva art. 5 al Directivei NIS2 și nu instituie cerințe care ar depăși această minimă armonizare, inclusiv impunerea unor obligații mai stricte persoanelor fizice și juridice care cad sub incidența legii. 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.

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 MDED mded.gov.md și pe platforma de consultare particip.gov.md, la data de 11.02.2026 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de lege, link: https://particip.gov.md/ro/document/stages/*/16150

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

Cadrul normativ necesar punerii în aplicare a prevederilor normelor legale primare în domeniul securității cibernetice a fost aprobat integral, cu excepția regulamentului privind condițiile în care persoanele juridice de drept public pot semna acorduri de schimb de informații în materie de securitate cibernetică, care urmează a fi elaborat și aprobat prin hotărâre de Guvern până la finele anului 2026.

Proiectul de lege propune ajustări ale procesului de identificare a furnizorilor de servicii, îmbunătățiri a prevederilor care vizează măsurile de securitate pe care furnizorii de servicii urmează să le implementeze și obligațiile de notificare a incidentelor semnificative de către aceștia, precum și revizuirea normelor care reglementează la nivel primar supravegherea și controlul de stat pentru a le armoniza integral cu prevederile Directivei NIS2. Având în vedere acest fapt, precum și ținând cont de faptul că modificările propuse nu revizuiesc fundamental nici modelul de guvernanță în acest domeniu și nici spectrul de obligații deja stabilite în Legea privind securitatea cibernetică, cadrul normativ guvernamental nu va necesita modificări substanțiale..

Totodată, adoptarea modificărilor propuse în proiectul de lege ar putea suscita necesitatea aprobării unor acte administrative departamentale comune în vederea reglementării la nivel operațional a modului de cooperare a ASC cu alte autorități publice cu competențe tangente domeniului, cu ar fi Banca Națională a Moldovei, Comisia Națională a Pieței Financiare, Agenția Națională pentru Reglementare în Comunicații, Ministerul Afacerilor Interne, Serviciul de Informații și Securitate, etc.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Autoritățile publice principale responsabile de organizarea procesului de implementare a propunerilor conținute în proiectul de lege, sunt MDED și ASC.

MDED urmează să asigure coordonarea procesului de implementare a politicilor în domeniul securității cibernetice. În acest context, MDED urmează să organizeze procesul de revizuire a actelor

³⁴ https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=oj:JOC_2023_324_R_0002;

normative secundare în domeniul securității cibernetice în vederea aducerii acestora în concordanță cu noile reglementări ale legii. De asemenea MDED va fi responsabil de monitorizarea și evaluarea modul de implementare a noilor prevederi legale în conformitate art. 75 din Legea nr. 100/2017 privind actele normative.

În acest context relevăm că Legea privind securitatea cibernetică este o lege cadru care determină principalele concepte și mecanisme de ordin juridic, organizatoric și instituțional orientate spre asigurarea unui nivel înalt de securitate a rețelelor și sistemelor informatice, parte a infrastructurii informaționale critice a țării. Legea respectivă și actele normative de punere a acestora în aplicare constituie principalele instrumente juridice pentru realizarea politicii de stat în acest domeniu. Din perspectiva planificării strategice în acest domeniu, principalul instrument decizional orientat spre realizarea politicii de stat în domeniul securității cibernetice este Programul național de securitate cibernetică pentru anii 2026-2030, aprobat prin Hotărârea Guvernului nr. 821/2025. Acest document de politici însumează acțiuni, realizarea cărora este orientată spre atingerea unor obiective generale și specifice similare obiectivelor urmărite prin punerea în aplicare a Legii nr.48/2023. Cu alte cuvinte, Programul este o continuare logică la nivelul planificării strategice de implementare și operaționalizare a instrumentelor și mecanismelor reglementate prin Legea nr. 48/2023. Reieșind din aceasta, atât mecanismul de monitorizare și evaluare a Programului, stabilit în capitolul VIII, cât și indicatorii de monitorizare stabiliți în capitolul III, tabelul 1, urmează a fi utilizate în procesul de monitorizare și evaluare a modului în care sunt implementate noile prevederi ale Legii nr. 48/2023. Astfel, unul din principalii indicatori de performanță îl constituie scorul de țară conform Indicelui global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor la toate cele 5 grupuri de măsuri: juridice; tehnice; organizaționale; dezvoltare a capacităților; cooperare.

ASC îi revine rolul de implementator al prevederilor legale noi. În acest sens ASC trebuie să finalizeze operaționalizarea în volum deplin a subdiviziunilor responsabile de exercitarea atribuțiilor menționate în proiectul de lege.

Secretar de Stat

Michelle ILIEV

SINTEZA

obiecțiilor și propunerilor SEIR la proiectul de lege pentru modificarea unor acte normative (armonizarea legislației naționale la prevederile Directivei NIS2)

Nr./ ord.	Textul prevederii proiectului de lege pe marginea căruia s-a formulat obiecția	Conținutul obiecțiilor	Rezultatul examinării obiecțiilor (<i>inclusiv textul prevederii în cazul definitivării</i>)
1.			
2.	La pct. 2.2 din nota de fundamentare	Nu se descriu părțile interesate care sunt afectate de probleme și cele care participă la apariția acestora.	Se acceptă. Nota a fost completată corespunzător.
3.	La punctul 3.2. din nota de fundamentare	Nu se expun opțiuni alternative sau motivul de ce acestea nu au fost luate în considerare.	Se acceptă în partea argumentării motivelor de neexaminare a unei opțiuni alternative. Punctul 3.2 din nota de fundamentare a fost completat cu informații privind argumentarea neexpunerii unor opțiuni alternative.
4.		Nu se analizează riscul neintervenției - a păstra situația și reglementarea curentă.	În ce privește riscurile lipsei de intervenție, menționăm că lipsa de intervenție, cu alte cuvinte opțiunea de a nu face nimic ar presupune de a nu finaliza procesul de armonizare a legislației naționale la prevederile Directivei NIS2. Aceasta implică riscuri legate de procesul de integrare europeană a Republicii Moldova, în particular în ce privește angajamentele de aliniere a cadrului normativ la aquis-ul comunitar. În acest caz prin prisma principiului proporționalității efortului, stabilit de pct. 6.6. din Metodologia de analiză a impactului de reglementare, considerăm inutilă analizarea acestei problematice, având

			în vedere caracterul eminamente formal al unei astfel de analize.
5.		Nu se examinează costurile și beneficiile opțiunilor alternative (dacă este cazul)	Pentru aceste compartimente nu este aplicabilă cerința de a evalua costurile și beneficiile opțiunii alternative, având în vedere că o astfel de opțiune nu a fost examinată (vezi argumentarea de la pct.3 din prezentul tabel și completările operate la pct. 3.2 din nota de fundamentare).
6.	La pct. 4.6 din nota de fundamentare	Nu se expune concluzia argumentată în baza beneficiilor nete sau celui mai mic impact negativ	
7.		Nu au fost desfășurate consultări cu principalele părți care vor fi afectate de proiect	Proiectul a fost supus consultărilor publice fiind plasat spre consultare pe portalul particip.gov.md în perioada 24.06.2026 - 09.07.2026, link: https://particip.gov.md/ro/document/stages/*/16150
8.	La pct. 9 din nota de fundamentare	Nu se stabilesc indicatorii de performanță pentru a efectua monitorizarea	Se acceptă. Compartimentul 9 al notei de fundamentare a fost completat.
9.		Nu se stabilește cum va fi monitorizat și evaluat impactul opțiunii recomandate și peste cât timp se va evalua performanța actului normativ propus	Se acceptă. Compartimentul 9 din nota de fundamentare a fost completat.
10.	(2 ¹) Conducerea furnizorului de servicii este obligată:	La art.11 alin.2/1 din Legea nr.48/2023 se impune obligația pentru „conducerea” furnizorilor	Se acceptă în principiu. Pentru claritate cuvântul „conducere” fost substituit cu cuvântul administrator conform prevederilor Codului civil. În orice caz, nu putem accepta interpretarea conform căreia aceste noțiuni ar

	a) să urmeze cursuri de formare pentru a dobândi suficiente cunoștințe și competențe pentru a putea identifica riscurile și a evalua practicile de gestionare a riscurilor de securitate cibernetică și impactul acestora asupra serviciilor pe care le prestează furnizorul de servicii, b) să aprobe măsurile de securitate a rețelelor și a sistemelor informatice, c) să supravegheze modul în care aceste măsuri sunt implementate. Atunci când organul de conducere al furnizorului de servicii este unul colegial, acesta desemnează un membru responsabil de realizarea obligațiilor de asigurare a securității cibernetică, care este obligat să urmeze cursurile de formare prevăzute la lit. a).	de a urma cursuri de formare în domeniul securității cibernetică. Nu este clar la care „conducere” se referă obligația și dacă ține de toate persoanele cu funcții de conducere în toată întreprinderea sau, totuși, este suficient o singură persoană responsabilă de domeniul în cauză din cadrul întreprinderii. Deși obligația conducerii furnizorului de servicii de a urma cursuri de formare este compatibilă cu art. 20 alin. (2) din Directiva (UE) 2022/2555, formularea propusă nu îndeplinește exigențele de claritate și previzibilitate ale normei juridice, întrucât nu stabilește elementele esențiale ale acestei obligații.	incorporează orice persoană cu funcție de răspundere din cadrul furnizorului de servicii. Propoziția a doua din acest alineat stabilește expres că atunci când conducere/ administrarea furnizorului de servicii se realizează de către un organ colegial acesta urmează să desemneze un membru care să îndeplinească obligațiile respective.
11.		Textul nu precizează natura și conținutul cursurilor, condițiile pe	Se acceptă parțial. Dispoziția acestui alineat a fost completată cu o propoziție care atribuie ASC sarcina de a oferi orientări metodologice furnizorilor de servicii în

		care trebuie să le îndeplinească furnizorii de instruire, modalitatea de confirmare a competențelor dobândite, periodicitatea instruirii și nici autoritatea competentă să stabilească sau să aprobe eventualele cerințe minime în privința programului de instruire. În lipsa unor asemenea repere normative, evaluarea conformării rămâne în mare măsură la aprecierea discreționară a autorității competente, ceea ce poate genera practici neuniforme și riscuri de aplicare arbitrară a legii.	realizarea acestei obligații. Totuși textul precizează natura și conținutul cursurilor. În primul rând într-un text de lege natura textului legal nu trebuie precizată. În al doilea rând litera a) stabilește clar care este conținutul obiectului acestei obligații: identificarea riscurilor și evaluarea practicilor de gestionare a riscurilor de securitate cibernetică și impactul acestora asupra serviciilor pe care le prestează furnizorul de servicii.
12.	(2) Autoritatea competentă prezintă, fără întârzieri nejustificate și, dacă e posibil , nu mai târziu de 24 de ore de la recepționarea informației indicate la alin.(1), furnizorului de servicii un răspuns inițial cu	La art.12 alin.(2) Legea nr.48/2023 completarea cu sintagma „dacă este posibil”, face ca termenul limită de 24 de ore, acordat pentru Agenție, să nu mai aibă sens din	Se acceptă parțial. Sintagma „dacă este posibil” a fost substituită cu sintagma „atunci când este posibil”, asigurând corespunderea absolută cu textul din Directiva NIS2. Totuși, considerăm că această remarcă trebuie păstrată în textul proiectului nu doar din considerente de armonizare textuală cu prevederile art. 23 alin. (5) din Directiva NIS2, ci mai ales din considerente practice: pe de o parte dinamica și evoluția situației în caz de incidente

	privire la incidentul cibernetic cu impact semnificativ și, la solicitarea furnizorului de servicii, recomandări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de soluționare a incidentului respectiv, inclusiv de atenuare a impactului acestuia și de continuitate a activității.	perspectiva rigorilor de reglementare juridică.	cibernetice este de cele mai multe ori imprevizibilă, iar informațiile ar putea să nu fie disponibile în cele 24 de ore. Totuși, atunci când ele sunt disponibile acestea trebuie livrate furnizorului de servicii, iar păstrarea acestui termen de 24 de ore este un reper temporal obligatoriu pentru ASC, din perspectiva responsabilității generale pentru monitorizarea spațiului cibernetic național și a misiunii sale de coordonare a procesului de răspuns la incidente, în caz de solicitare și de acordare a suportului furnizorilor de servicii.
13.	Art. 19: (12) În privința furnizorilor importanți de servicii, autoritatea competentă exercită împuternicirile prevăzute la alin. (5), cu excepția literei b) în ce privește caracterul periodic al auditurilor de securitate specifice, precum și aplică măsurile de asigurare a respectării legii prevăzute la alin. (7), cu excepția celor de la lit. b) pct. 2) și lit. d), doar atunci când dispune de dovezi, indicii sau informații, inclusiv rezultate din alte activități	Proiectul de lege instituie un regim uniform al competențelor de supraveghere și al măsurilor administrative aplicabile în majoritatea cazurilor tuturor categoriilor de furnizori de servicii, fără a diferenția între furnizorii „esențiali” și cei „importanți” (așa cum este diferențiat în Directivă) în funcție de nivelul de risc și de importanța serviciilor prestate. O asemenea abordare ridică probleme din perspectiva	Această afirmație nu corespunde realității. Proiectul reflectă abordarea conceptuală propusă în Directiva NIS2. Alineatul (12) din art. 19 propus în proiectul de lege determină condițiile de aplicare a prevederilor art. 19 în privința furnizorilor importanți de servicii. Față de această categorie de furnizori de servicii urmează a fi aplicată o procedură simplificată de supraveghere și control (ex-post) care în principal se caracterizează prin faptul că măsurile de control de stat și cele de asigurare a respectării legii pot fi aplicate doar post factum, adică doar dacă există anumite dovezi din diverse surse care ar putea oferi suficiente temeiuri de a suspecta o potențială încălcare a legii.

	desfășurate de autoritatea competentă în exercitarea competenței sale, furnizate de alte autorități și instituții publice, de persoane fizice sau juridice ori disponibile în surse publice, care ar sugera potențiale încălcări ale prezentei legi (exercitarea ex-post al controlului de stat).	principiului proporționalității, întrucât permite exercitarea aceluiași atribuții de control și intervenție față de entități aflate în situații juridice și factuale diferite, generând o sarcină administrativă și de conformare potențial excesivă pentru operatorii economici. În același timp, proiectul diferențiază regimul sancționator prin stabilirea unor limite distincte ale amenzilor pentru furnizorii esențiali și cei importanți, ceea ce demonstrează recunoașterea de către legiuitor a existenței unor grade diferite de risc și de impact. În aceste condiții, se impune asigurarea unei reglementări coerente și proporționale, prin corelarea competențelor de supraveghere și control cu nivelul de criticitate al	
--	--	--	--

		entităților vizate și de separat entitățile esențiale de cele importante, conform modelului din Directivă.	
14.	Art. 19: (1) Controlul de stat privind respectarea de către furnizorii de servicii a prezentei legi și a actelor normative adoptate în temeiul acesteia se exercită de către autoritatea competentă în conformitate cu prezenta lege și Legea nr.131/2012 privind controlul de stat. (2) Prevederile prezentei legi care reglementează controlul de stat exercitat de autoritatea competentă se completează cu prevederile Legii nr.131/2012 privind controlul de stat. Dacă Legea 131/2012 privind controlul de stat nu conține prevederi aplicabile activităților desfășurate de autoritatea competentă în	În privința aspectelor de supraveghere și control exercitate de Agenție, propuse la art.19 în Legea nr.48/2023, atenționăm: - La alineatul (5) lit. c) se admite inițierea controalelor inopinate în cazul oricărei încălcări a legii. Ceea ce nu corespunde cu principiile prevăzute de Directivă în privința proporționalității intervenției, dar nici cu rigorile Legii nr.131/2012 care prevede clar și exhaustiv la art.19 temeiurile pentru inițierea unui control inopinat, cu luare în calcul a gravității încălcării și riscului;	Această prevedere trebuie examinată în coroborare cu prevederile alineatelor anterioare, ea nu trebuie interpretată izolat ci în contextul general al normelor acestui articol. Acest context este dat de faptul că activitățile de control se exercită în conformitate cu Legea nr. 131/2012. Alineatul (5) enumeră doar competența ASC, din perspectiva Directivei NIS2, fără a afecta sistemul juridic și mecanismele instituite prin Legea nr. 131/2012, în exercitarea controlului și enumeră activitățile pe care le poate realiza în acest sens. În același timp aceste activități de control urmează a fi realizate în limitele stabilite de Legea nr. 131/2012 privind controlul de stat, care, având în vedere că în sens mai larg , sunt activități administrative, urmează a fi completată cu prevederile Codului administrativ.

	exercitarea controlului de stat și asigurarea respectării legii sau prevederile acesteia sunt insuficiente, prevederile prezentei legi se completează cu prevederile Codului administrativ. (3) Prevederile Legii nr.131/2012 privind controlul de stat se aplică în măsura în care nu contravin prevederilor prezentei legi. (5) În exercitarea funcției de control de stat în privința furnizorilor de servicii, autoritatea competentă este împuternicită: ... c) să efectueze controale inopinate, inclusiv în cazurile justificate de un incident cibernetic cu impact semnificativ sau de o încălcare a prezentei legi de către furnizorul de servicii în cauză;		
15.	Art. 19:	- La același articol se atribuie Agenției	Se acceptă.

	(5) În exercitarea funcției de control de stat în privința furnizorilor de servicii, autoritatea competentă este împuternicită: ... b) să dispună efectuarea unor audituri de securitate periodice și specifice în privința furnizorului de servicii de către un organism independent; ... (6) Auditurile de securitate specifice, menționate la alin. (5) litera b), trebuie să se bazeze pe evaluări ale riscurilor efectuate de autoritatea competentă sau de furnizorul de servicii auditat sau pe alte informații disponibile legate de riscuri. Raportul auditului de securitate specific se remite fără întârzieri nejustificate autorității competente. Costurile auditului de securitate specific sunt suportate de furnizorul de servicii, dacă autoritatea	competența de a impune efectuarea unui audit de securitate cibernetică, preluând în acest sens formularea generală prevăzută de Directiva (UE) 2022/2555, fără a stabili însă condițiile și circumstanțele concrete în care o asemenea măsură poate fi dispusă. În lipsa unor criterii obiective privind temeiurile declanșării auditului, frecvența acestuia, proporționalitatea în raport cu nivelul de risc identificat sau existența unor indicii de neconformitate, această competență poate conferi autorității o marjă excesiv de largă de apreciere, cu impact direct asupra activității și costurilor suportate de operatorii economici. Se impune reglementarea unor garanții procedurale și a unor criterii clare de	Alineatul (6) din articolul 19 a fost completat cu o propoziție nouă cu următorul cuprins: „Condițiile și cazurile în care autoritatea competentă poate dispune efectuarea unor audituri de securitate specifice, situațiile în care autoritatea competentă rambursează furnizorului de servicii costurile auditului de securitate specific, precum și modul de rambursare a acestor costurilor se stabilesc de Guvern.”
--	---	--	--

	competentă nu decide altfel în cazurile justificate corespunzător.	aplicare, astfel încât auditul să reprezinte o măsură necesară, adecvată și proporțională în raport cu scopul urmărit, aplicată în funcție de riscurile concrete identificate și nu ca o obligație generală susceptibilă de a fi impusă discreționar.	
16.		Totodată, se remarcă faptul că proiectul extinde această competență asupra tuturor categoriilor de furnizori de servicii, în timp ce Directiva (UE) 2022/2555 integrează această măsură în principal în cadrul regimului de supraveghere aplicabil entităților esențiale, ceea ce este o abordare disproporționată în raport cu entitățile care nu prezintă același nivel de criticitate sau risc;	Precizare. Proiectul de lege face distincție între cele două categorii de furnizori de servicii în aplicarea auditurilor specifice. Alineatul (12) di art. 19 în redacția propusă în proiect determină clar că în privința furnizorilor importanți de servicii, autoritatea competentă exercită împuternicirile prevăzute la alin. (5), cu excepția literei b) în ce privește caracterul periodic al auditurilor de securitate specifice. Aceasta corespunde conceptului propus în Directiva NIS2.

17.		- Din perspectiva controlului de stat, un astfel de audit poate fi calificat drept o expertiză dispusă în cadrul procedurii de control, care trebuie să fie strict conexă cu procedura prevăzute de lege și să urmeze rigorile procedurale ale Legii nr.131/2012, în caz contrar auditul în cauză ar putea fi utilizat ca o formă camuflată de control de stat sau ca și modalitate de prelungire nejustificată a procedurii de control;	Se acceptă. Vezi rezultatul examinării de la pct. 15 din prezentul tabel.
18.		- Se prevede ca auditul să fie achitat de către persoana auditată, ceea ce este contrar cu principiul prevăzut de Legea nr.235/2006 (și detaliat în Legea nr.131/2012), conform căruia toate cheltuielile în privința controlul de stat se suportă din contul statului. În același timp, însăși formularea „dacă	Se acceptă parțial. Vezi rezultatul examinării de la pct. 15 din prezentul tabel. Totodată, ținem să relevăm că aceste norme transpun prevederile Directivei NIS2. Prevederile Directivei NIS2 la acest aspect nu sunt opționale și stabilesc expres condițiile și regulile generale care trebuie reflectate în legislația națională a statelor membre. Una din aceste reguli generale este că furnizorul de servicii suportă costurile auditului de securitate specific, dispus de autoritatea competentă. Excepția de la această regulă sunt situațiile în care autoritatea competentă poate decide în mod justificat că aceste costuri trebuie suportate de către bugetul de stat. Această normă obligatorie spre

		autoritatea competentă nu decide altfel în cazurile justificate corespunzător” este una extrem de vagă, încalcă principiul previzibilității aplicării normei și lasă o marjă prea mare de discreție pentru Agenție.	transpunere din actul UE constituie în esență opusul conceptului de suportare a costurilor în cazul unui control de stat, stabilit de legea respectivă. Trebuie să luăm în considerare faptul că în raport cu relația autoritatea competentă – furnizor de servicii, auditurile de securitate specifice vor fi efectuate de organisme independente.
19.	Art. 19: ...(9) În ce privește furnizorii esențiali de servicii, dacă măsurile prevăzute la alin. (7) lit. a) și lit. b) punctele 1) – 3) și 5) sunt ineficiente, autoritatea competentă stabilește un termen suplimentar în care furnizorul esențial de servicii este obligat să remedieze deficiențele sau să se conformeze cerințelor stabilite în prescripția emisă de autoritatea competentă. Dacă furnizorul esențial de servicii nu remediază deficiențele sau nu se conformează cerințelor în termenul suplimentar	La art.19 alin.(9) și 19/1 din Legea nr.48/2023 suspendarea sau retragerea actelor permissive se reglementează ca și categorii de sancțiuni, ceea ce contravine principial cu prevederile din Legea nr.160/2011 care prevăd că „autoritatea emitentă nu are dreptul de a suspenda și/sau de a retrage actul permisiv în scopul sancționării solicitantului în cazul în care acesta nu respectă unele condiții sau nu onorează unele obligații care nu se încadrează în lista	Se acceptă. Proiectul a fost modificat după cum urmează: 1. Litera a) a fost expusă într-o redacție nouă: „a) în cazul încălcărilor foarte grave și de riscuri iminente , poate emite o prescripție în calitate de măsură restrictivă în sensul art. 30 din Legea nr. 131/2012 privind controlul de stat, de suspendare a activității furnizorului respectiv de servicii, în parte sau, dacă nu e posibilă disjungerea activităților respective, în totalitate în conformitate și în condițiile stabilite de Legea ne. 131/2012 privind controlul de stat, până la remedierea deficienței și/sau asigurarea conformității cu cerințele prescrise; 2. litera b) a fost completată la început cu textul „în cazul încălcărilor grave și foarte grave, poate”.

	stabilit în temeiul prezentului alineat, autoritatea competentă: a) solicită autorităților sau instituțiilor publice competente să suspende actul/actele permissive în privința furnizorului respectiv de servicii până la remediarea deficienței și/sau asigurarea conformității cu cerințele prescise; b) solicită organelor de conducere ale furnizorului esențial de servicii suspendarea contractului individual de muncă cu persoana fizică care exercită responsabilități de conducere la nivel de director executiv sau de reprezentant legal al furnizorului de servicii sau impunerea unor interdicții acestor persoane în exercitarea responsabilităților respective, până la remediarea deficienței și/sau asigurarea	expresă de cerințe și/sau condiții stabilite de lege în privința actului permisiv în cauză”. Din altă perspectivă, Directiva la art.32 vine cu formulări suficient de generale în privința modului de suspendare a activității economice, lăsînd spațiu pentru a selecta metoda care corespunde cu cadrul normativ național. Ori nu este clar din ce cauză autorii au optat anume pentru „suspendarea actelor permissive”, care în practică se dovedește mai anevoioasă și mai birocratică decît o măsură restrictivă în cadrul controlului de stat. Astfel, dacă este necesar de aplicat măsura de suspendare totală sau parțială a activității de întreprinzător pentru a asigura înlăturarea încălcărilor admise, doar	
--	--	--	--

	conformității cu cerințele prescrise. Măsurile prevăzute la prezentul alineat nu se aplică persoanelor juridice de drept public. ... Art. 19/1: (1) Autoritatea competentă aplică amenzile în completare față de oricare dintre măsurile prevăzute la art. 19 alin. (7) literele (a) și b) și alin. (9).	în cazuri de încălcări foarte grave și riscuri iminente, este suficient de indicat posibilitatea Agenției de a emite o astfel de prescripție și aplica o astfel de măsură în cadrul procedurii de control de stat, în limitele și condițiile Legii nr.131/2012. În același timp, este important ca cel puțin orientativ proiectul să concretizeze în raport cu ce categorii de încălcări și gravitatea acestora pot fi aplicate astfel de măsuri, inclusiv când se aplică măsura de la litera a) și când cea de la litera b). Însă dacă se dorește ca să fie aplicată o sancțiune (post-factum) complementară, pe lângă amendă, în formă de lipsire de dreptul de a desfășura o anumită activitate sau de a ocupa o anumită funcție, aceasta se realizează în	
--	---	--	--

		cadrul procedurii contravenționale în temeiul hotărârii instanței de judecată.	
20.	Art. I – Codul Contravențional nr. 218/2008 (Republicat: Monitorul Oficial al Republicii Moldova, 2017, nr.78-84, art.100), cu modificările ulterioare, se modifică după cum urmează: 1. Se completează cu articolele 259³ și 259⁴, cu următorul cuprins: „Articolul 259³. Încălcarea legislației în domeniul securității cibernetice (1) Încălcarea cerințelor stabilite de art. 11 alin. (1), (2), (2²), (2³) sau (3) ori de art. 12 alin. (1), (3), (3¹), (4), (6), (7¹), (8) sau (8¹) din Legea nr. 48/2023 privind securitatea cibernetică de către furnizorul esențial de servicii,	Proiectul de lege instituie, pe lângă amenzile administrative preluate din modelul Directivei (UE) 2022/2555, și sancțiuni contravenționale cu un quantum semnificativ pentru încălcarea unor obligații similare, fără o argumentare temeinică în privința oportunității și necesității. Ori sancțiunile din Directivă au deja un caracter substanțial represiv, prin quantumurile ridicate raportate la cifra de afaceri, astfel încât suprapunerea lor cu amenzi contravenționale considerabile poate crea un efect disproporționat asupra agenților economici, contrar principiului unei	Precizare. Abordarea propusă în proiect prevede două regimuri de sancționare diferite unul, cel prevăzut în modificările la Codul contravențional, cu amendă contravențională având ca subiecți ai răspunderi contravenționale persoanele fizice și cele cu funcție de răspundere din cadrul furnizorilor de servicii și al doilea cel prevăzut în art. 19/1 cu care se propune completarea Legii nr. 48/2023. În al doilea caz este vorba de amenzile administrative aplicate furnizorilor de servicii ca subiecți speciali persoane juridice. Opțiunea respectivă este optimă și unica posibilă în contextul în care este necesar, pe de o parte să se asigure transpunerea integrală a Directivei NIS2, inclusiv și în mod special quantumul amenzilor administrative, iar pe de altă parte să nu se intervină aleatoriu în sisteme juridice complexe precum este legislația contravențională. În context menționăm că soluționarea problematicilor respective urmează a fi realizată în mod sistemic prin corectarea și ajustarea politicilor de stat în domeniile respective. Din perspectiva promovării proiectului în speță, autorii au operat cu instrumentarul juridic disponibil și au evitat distorsionarea unor instituții juridice deja consolidate.

	se sancționează cu amendă de la 100 la 1000 de unități convenționale aplicată persoanei fizice, cu amendă de la 500 la 1500 de unități convenționale aplicată persoanei cu funcție de răspundere. (2) Încălcarea cerințelor stabilite de art. 11 alin. (1), (2), (2²), (2³) sau (3) ori de art. 12 alin. (1), (3), (3¹), (4), (6), (7¹), (8) sau (8¹) din Legea nr. 48/2023 privind securitatea cibernetică de către furnizorul important de servicii, se sancționează cu amendă de la 50 la 500 de unități convenționale aplicată persoanei fizice, cu amendă de la 100 la 1000 de unități convenționale aplicată persoanei cu funcție de răspundere. (3) Neexecutarea obligației prevăzute de articolul 17 alin. (4) din Legea nr. 48/2023 privind securitatea cibernetică,	intervenții administrative necesare și echilibrate. În lipsa unor norme de delimitare a domeniului de aplicare al sancțiunilor și a unor garanții împotriva cumulului acestora pentru aceeași faptă, există riscul aplicării unor sancțiuni multiple pentru aceeași încălcare, ceea ce poate conduce la o intervenție excesivă asupra activității operatorilor economici și poate contraveni principiilor proporționalității. Se recomandă revizuirea necesității sancțiunilor contravenționale sau, cel puțin, clarificarea suplimentară a condițiilor de aplicare a sancțiunilor administrative și contravenționale, inclusiv prin stabilirea unor criterii de delimitare, a priorității aplicării unui anumit tip de sancțiune sau a interdicției cumulului	
--	--	---	--

	se sancționează cu amendă de la 50 la 150 de unități convenționale aplicată persoanei cu funcție de răspundere, cu amendă de la 100 la 500 de unități convenționale aplicată persoanei juridice. Articolul 259⁴. Împiedicarea activității Agenției pentru Securitate Cibernetică Refuzul neîntemeiat de a prezenta informațiile sau documentele solicitate de Agenția pentru Securitate Cibernetică în procesul exercitării atribuțiilor sau prezentarea informației neautentice sau incomplete sau împiedicarea accesului pentru personalul abilitat cu funcții de control al Agenției pentru Securitate Cibernetică în locurile unde sunt amplasate obiectele controlului, se sancționează cu amendă de la 50 la 150 de	sancționator atunci când există identitate de faptă, subiect și scop al sancțiunii.	
--	---	--	--

unități convenționale aplicată persoanei fizice, cu amendă de la 100 la 300 de unități convenționale aplicată persoanei cu funcție de răspundere, cu amendă de la 500 la 1500 de unități convenționale aplicată persoanei juridice.”. 2. Se completează cu articolul 410¹ cu următorul cuprins: „Articolul 410¹. Agenția pentru Securitate Cibernetică (1) Contravențiile prevăzute la articolele 259³ și 259⁴ se constată și se examinează de către Agenția pentru Securitate Cibernetică. (2) Sunt în drept să constate contravenții și să încheie procese-verbale șefii subdiviziunilor și funcționarii din cadrul Agenției pentru Securitate Cibernetică, împuterniciți de către directorul sau		
---	--	--

	directorul adjunct al Agenției. (3) Sunt în drept să examineze cauzele contravenționale și să aplice sancțiuni directorul sau directorul adjunct ai Agenției pentru Securitate Cibernetică.”.		
21.	Articolul 19¹. Amenda pentru încălcările prezentei legi (1) Autoritatea competentă aplică amenzi în completare față de oricare dintre măsurile prevăzute la art. 19 alin. (7) literele (a) și b) și alin. (9). (2) Atunci când decide aplicarea unei amenzi și cuantumul acesteia, în fiecare caz în parte autoritatea competentă ține cont în mod corespunzător cel puțin de elementele prevăzute la art.19 alin. (10). (3) Pentru încălcarea de către furnizorul esențial de servicii a cerințelor	Sanțiunile propuse la art.19/1 din Legea nr.48/2023 nu sunt corelate cu nici o procedură clară de constatare, aplicare și ispășire a pedepsei. Odată ce astfel de norme nu se regăsesc în proiect, decât unele prevederi de abordare generală, este strict necesar de clarificat care este cadrul normativ procesual care se aplică complementar. Totodată atenționăm că procedura prevăzută de Codul administrativ nu se recomandă a fi aplicată pentru emiterea deciziei pentru constatarea	Se acceptă de principiu. Art. 19/1 a fost completat cu două alienate noi cu următorul cuprins: „(6) Autoritatea competentă constată încălcările prevăzute de prezentul articol în conformitate cu procedura stabilită de Legea nr. 131/2012 privind controlul de stat și aplică amenzi în cuantumul prevăzut de alineatele (3) sau (4) prin procesul verbal cu privire la efectuarea controlului de stat doar pentru încălcările grave și foarte grave. (7) Furnizorii de servicii, în privința cărora au fost aplicate amenzi în conformitate cu prevederile prezentei legi pot contesta deciziile autorității competente de aplicare a amenzilor respective în conformitate cu prevederile art. 30 din Legea nr. 131/2012 privind controlul de stat. Totodată, ținem să relevăm următoarele. Conceptul propus în proiect are ca scop integrarea regimului sancționator al „amenzilor administrative”, caracteristic actelor normative ale UE, în sistemul moldovenesc. Directiva NIS2 lasă la latitudinea statelor membre modul de integrare a amenzilor administrative în sistemele

prevăzute la art. 11 alin. (1), (2), (2²), (2³) sau (3) ori la art. 12 alin. (1), (3), (3¹), (4), (6), (7¹), (8) sau (8¹), autoritatea competentă aplică amendă de până la 2000000 lei sau de până la 2% din cifra totală de afaceri realizată în anul anterior aplicării amenzii, luându-se în considerare valoarea cea mai mare dintre acestea. (4) Pentru încălcarea de către furnizorul important de servicii a cerințelor prevăzute la art. 11 alin. (1), (2), (2²), (2³) sau (3) ori la art. 12 alin. (1), (3), (3¹), (4), (6), (7¹), (8) sau (8¹), autoritatea competentă aplică amendă de până la 1400000 lei sau de până la 1,4% din cifra totală de afaceri realizată în anul anterior aplicării amenzii, luându-se în considerare valoarea cea mai mare dintre acestea. (5) În cazul în care cifra totală de afaceri realizată în anul anterior aplicării amenzii nu este	încălcărilor și aplicarea sancțiunilor odată ce Codul administrativ are cu totul alte obiective, nu neapărat cele de apărare a ordinii publice, drepturilor și valorilor ocrotite de lege și nu conține garanțiile necesare pentru învinuit pentru înfăptuirea corectă și echitabilă a dreptății sau pentru prevenirea comiterii noilor încălcări. În același timp, procedura administrativă nu conține reglementare clară cu privire la probatoriu, mijloacele de probă acceptabile și limita probării, dar și contestarea deciziei se petrece în cadrul procedurii contenciosului administrativ care efectiv impune învinuitul să-și demonstreze nevinovăția, ceea ce ar fi o încălcare a principiului prezumției nevinovăției. Odată ce în practică, factorul de	juridice proprii. Cu toate acestea, subiecții amenzii, quantumul amenzilor și însăși obligativitatea transpunerii prevederilor respective sunt obligatorii, inclusiv văzute prin prisma principiului minimeii armonizării. Sistemul juridic al Republicii Moldova nu cuprinde un set de norme substanțiale și procedurale specifice aplicării regimului amenzilor administrative, astfel cum acesta este reflectat în Directiva NIS2 în particular. Instrumentele juridice existente oferite de Codul penal sau/și Codul contravențional, deși sunt relevante din punctul de vedere al garanțiilor oferite „învinuitului”, cuprind limitări, în mod special din perspectiva quantumului sancțiunilor pecuniare. Extrapolarea, spre exemplu al prevederilor Codului contravențional, printr-o norma de blanchetă, la procedurile de aplicare a amenzii administrative prevăzute de proiect, ar contraveni principiului legalității (nu există pedeapsă fără lege), consacrat în art. 5 din Codul contravențional. Nu ar fi corect din punct de vedere juridic nici introducerea în Codul Contravențional a unor excepții, determinate de rațiuni proprii unui singur domeniu (cel al securității cibernetice), fără o abordare sistemică a reformării dreptului contravențional, astfel încât normele din actele UE să fie preluate păstrându-li-se esența și natura juridică a acestora, bazată pe rațiuni teoretice sau empirice ale legiuitorului european. Aceleași raționamente considerăm că pot fi aplicate și legislației penale. Unicul instrument care ar putea fi utilizat în asigurarea unor garanții procedurale minime persoanelor în privința cărora au fost aplicate amenzi administrative în viziunea noastră este Codul administrativ, acesta însă, după cum este reflectat și în proiectul de lege urmează a fi aplicat în
---	--	---

	înregistrată, se ia în considerare cea mai recentă cifră de afaceri anuală a întreprinderii, anterioară aplicării amenzii. (6) Amenzile prevăzute de prezentul articol nu se aplică persoanelor juridice de drept public.	decizie din cadrul autorității publice are o libertate destul de mare de a decide asupra vinovăției, aplicarea sancțiunii sau unei măsuri coercitive (nefiind restrîns de rigorile contravenționale sau penale ale probatorului ș.a. necesități de argumentare suplimentară), iar în cadrul contestării, reclamantul va fi obligat să demonstreze că sancțiunea/măsura i-a fost aplicată eronat sau disproportionat, ceea ce în esență, în majoritatea cazurilor va presupune că reclamantul trebuie deja să dovedească că nu a comis faptele imputate sau că faptele comise au fost calificate eronat.	completarea prevederilor Legii nr. 131/2012 privind controlul de stat. Aici trebuie relevat faptul că același algoritm juridic este utilizat și de art. 30 din Legea nr. 131/2023. De asemenea Aici este important de relevat referitor la sarcina probării în procesul administrativ, că regula generală conform căreia fiecare parte în probează pretențiile nu este una absolută. Alin. (2) din art. 93 al Codului administrativ stabilește o regulă specială derogatorie de la cea generală conform căreia fiecare participant probează faptele atribuite exclusiv sferei sale de activitate. Cu alte cuvinte, organul de control trebuie să probeze cel puțin existența faptei ilicite și cuantumul și proporționalitatea amenzii aplicate. De asemenea, în proiect s-a corectat o eroare tehnică, art. 19/1 fiind inclus în art. IV alin. (1) din proiectul de lege, ceea ce înseamnă că acest articol urmează să intre în vigoare la data intrării în vigoare a tratatului de aderare a Republicii Moldova la Uniunea Europeană. Sperăm că până la intrarea în vigoare a acestei prevederi, autoritățile publice responsabile vor soluționa în mod sistemic modul de încorporarea în sistemul legislativ și juridic național a regimului sancționator cuprins în actele Uniunii Europene.
--	---	--	--