Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE

nr._____din_____2023

Chişinău

privind aprobarea proiectului de lege privind securitatea cibernetică

Guvernul HOTĂRĂŞTE:

Se aprobă şi se prezintă Parlamentului spre examinare proiectul de lege privind securitatea cibernetică.

PRIM-MINISTRU **Natalia GAVRILIȚA**

Contrasemnează:

Viceprim-ministru Iurie ȚURCANU

Ministrul Economiei Dumitru ALAIBA

Ministrul Justiției Sergiu LITVINENCO

proiect

Lege privind securitatea cibernetică

Capitolul I. Dispoziții generale

Articolul 1. Obiectul de reglementare al legii

Prezenta lege reglementează cadrul juridic, organizațional și de cooperare în domeniul securității cibernetice, stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică, determină cadrul național general de gestionare a crizelor în domeniul securității cibernetice, instituie cerințe, măsuri și mecanisme pentru asigurarea securității rețelelor și sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și gestionarea incidentelor cibernetice.

Articolul 2. Principalele noțiuni și definițiile lor

În sensul prezentei legi, următoarele noțiuni înseamnă:

1) ***amenințare cibernetică*** – orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora;

2) ***amenințare cibernetică semnificativă*** - amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor sale tehnice, că are potențialul de a afecta grav rețeaua și sistemele informatice ale unei persoane juridice care prestează servicii sau utilizatorii serviciilor furnizate de aceasta, cauzând prejudicii materiale sau morale considerabile;

3) ***divulgarea coordonată a vulnerabilităților*** – proces structurat prin care informații privind vulnerabilitățile sunt transmise producătorului sau furnizorului de produse TIC sau de servicii TIC potențial vulnerabile într-o manieră care să îi permită acestuia să diagnosticheze și să remedieze vulnerabilitatea înainte ca informațiile detaliate privind vulnerabilitatea să fie dezvăluite unor terțe părți sau publicului;

4) ***furnizor de servicii*** – persoană juridică de drept public sau de drept privat, înregistrată în Republica Moldova, care prestează servicii în unul sau mai multe sectoare și/sau subsectoare, stabilite de Guvern, și care este identificată de autoritatea competentă în conformitate cu prevederile prezentei legi și a cadrului normativ aprobat pentru punerea acesteia în aplicare;

5) ***gestionarea incidentului cibernetic*** – toate acțiunile și procedurile care vizează prevenirea, detectarea, analizarea, limitarea și izolarea unui incident cibernetic, sau vizează răspunsul la acesta și redresarea în urma acestui incident;

6) ***incident cibernetic*** **-** orice eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor conexe oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora;

7) ***incident cibernetic evitat la limită*** **–** un eveniment care ar fi putut compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora, dar care a fost împiedicat cu succes să se materializeze sau care nu s-a materializat;

8) ***măsuri de securitate*** - operațiuni și/sau resurse organizaționale, fizice și de tehnologie a informației aplicate în scopul obținerii și menținerea securității rețelelor și sistemelor informatice și a datelor procesate prin acestea;

9) ***proces TIC*** – un set de activități desfășurate pentru a concepe, a dezvolta, a furniza sau a întreține un produs TIC sau un serviciu TIC;

10) ***produs TIC*** - un element sau un grup de elemente al unei rețele sau al unui sistem informatic;

11) ***rețea și sistem informatic*** :

a) rețea de comunicații electronice în sensul prevederilor Legii comunicațiilor electronice nr. 241/2007 sau

b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale sau

c) date digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la lit. a) și b) în vederea funcționării, utilizării, protejării și întreținerii lor.

12) ***risc*** – potențialul de pierderi sau de perturbări cauzate de un incident cibernetic și trebuie exprimat ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului cibernetic;

13) ***securitate cibernetică*** - activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice;

14) ***securitatea rețelelor și a sistemelor informatice*** – capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

15) ***serviciu TIC*** - un serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice;

16) specificație tehnică – o specificație tehnică în sensul Legii nr. nr. 20/2016 cu privire la standardizarea națională;

17) ***standard*** – un standard în sensul Legii nr. 20/2016 cu privire la standardizarea națională;

18) ***vulnerabilitate*** - un punct slab, o susceptibilitate sau o deficiență a unor produse TIC sau a unor servicii TIC care poate fi exploatată de o amenințare cibernetică.

Articolul 3. Domeniul de aplicare

(1) Prezenta lege se aplică persoanelor juridice de drept privat care se califică drept întreprinderi mijlocii, potrivit clasificării prevăzute de legislația cu privire la întreprinderile

mici și mijlocii, și persoanelor juridice de drept privat care depășesc plafoanele pentru întreprinderile mijlocii, care furnizează servicii în unul sau mai multe dintre sectoarele sau subsectoarele stabilite de către Guvern, și care sunt identificate ca furnizori de servicii de către autoritatea competentă, desemnată conform articolului 7, în conformitate cu prevederile prezentei legi și a actelor normative de punere a acesteia în aplicare.

(2) Indiferent de dimensiunea lor, prezenta lege se aplică și persoanelor juridice, de tipul stabilit de Guvern, dacă acestea îndeplinesc cel puțin una dintre următoarele condiții:

a) sunt furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului în sensul legislației privind comunicațiile electronice;

b) sunt prestatori de servicii de încredere în sensul legislației privind identificarea electronică și serviciile de încredere;

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

d) furnizează servicii de înregistrare a numelor de domenii;

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

f) 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 sau ar putea genera un risc sistemic semnificativ, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier;

g) este critică din cauza importanței sale specifice la nivel național sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente;

h) furnizează un serviciu dependent de o rețea și/sau de un sistem informatic și de un obiectiv al infrastructurii critice și este identificată în conformitate cu cadrul normativ național relevant ca fiind operator al unei astfel de infrastructuri;

i) sunt persoanele juridice de drept public.

(3) Prezenta lege se aplică rețelelor și sistemelor informatice care sunt destinate prelucrării informațiilor atribuite la secretul de stat în măsura în care prevederile acesteia nu contravin prevederilor legislației care reglementează prelucrarea unor astfel de informații.

(4) Prezenta lege se aplică rețelelor și sistemelor informatice necesare pentru cooperarea militară internațională și pentru pregătirea pentru apărarea națională în domeniul de competență al Ministerului Apărării în măsura în care prevederile acesteia nu contravin legislației privind apărarea națională.

(5) 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.

(6) În cazul în care legile sectoriale specifice stabilesc implementarea unor măsuri de gestionare a riscurilor sau obligații de notificare a incidentelor semnificative, ale căror efecte sunt cel puțin echivalente cu efectele obligațiilor stabilite de prezenta lege, prevederile legilor respective au caracter special în raport cu prevederile prezentei legi.

(7) În cazul în care obligațiile, prevăzute la alineatul (6), stabilite de legile sectoriale specifice, sunt aplicabile unui cerc mai restrâns de persoane juridice decât cel prevăzut de

prezenta lege și de actele normative de pune în aplicare a acesteia, prevederile prezentei legi se aplică persoanelor juridice care nu cad sub incidența obligațiilor impuse de legile sectoriale specifice.

(8) Prevederile alineatelor (6) și (7) se aplică de către autoritatea competentă pentru fiecare caz în parte în procesul de identificare a furnizorilor de servicii în conformitate cu prevederile actului normativ stabilit la articolul 4 alineatul (2).

(9) Prevederile Codului administrativ se aplică procedurilor administrative prevăzute în prezenta lege, în măsura în care nu contravin acestora.

Articolul 4. Identificarea furnizorilor de servicii

(1) Autoritatea competentă întocmește și ține o listă a furnizorilor de servicii, care cuprinde cel puțin tipul, categoria furnizorului de servicii și sectorul și subsectorul în care prestează serviciul respectiv și asigură ori de câte ori este necesar, însă nu mai rar decât o dată la doi ani, actualizarea acesteia.

(2) Guvernul aprobă lista sectoarelor, subsectoarelor și, corespunzător, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și subsectoare, precum și stabilește cadrul metodologic privind identificarea persoanelor juridice de drept public și celor de drept privat ca fiind furnizori de servicii.

(3) La solicitarea autorității competente, Serviciul de Informații și Securitatea furnizează acesteia informația privind operatorii de infrastructură critică identificați ca atare în conformitate cu legislația privind protecția infrastructurii critice.

Articolul 5. Principiile de asigurare a securității cibernetice

În procesul asigurării securității cibernetice, inclusiv a implementării prevederilor prezentei legi, persoanele responsabile trebuie să acționeze luând în considerare următoarele principii:

1) principiul personalității - asigurarea securității rețelelor și a sistemelor informatice este organizată de către furnizorii de servicii;

2) principiul protecției integrale – furnizorii de servicii verifică riscurile potențiale pe care le prezintă rețelele și sistemele informatice pe care le dețin și aplică măsuri organizatorice și tehnice adecvate pentru protecția acestora;

3) principiul reducerii la minimum a efectelor negative - în cazul unui incident cibernetic, furnizorul de servicii aplică măsurile necesare pentru a evita escaladarea efectului incidentului cibernetic și posibila răspândire a acestuia la o altă rețea sau un alt sistem informatic și notifică incidentul cibernetic autorității competente conform prezentei legi;

4) principiul proporționalității - constă în asigurarea unui echilibru între riscurile la care rețelele și sistemele informatice sunt supuse și cerințele de securitate implementate;

5) principiul cooperării - în asigurarea securității cibernetice și în soluționarea incidentelor cibernetice, persoanele responsabile cooperează și, dacă este necesar, iau în considerare conexiunea mutuală dintre sisteme și servicii și dependența acestora.

Capitolul II. Cadrul instituțional, cooperarea și coordonarea strategică la nivel național

Articolul 6. Planificarea și coordonarea strategică în domeniul securității cibernetice la nivel național

(1) Coordonarea strategică la nivel național în domeniul securității cibernetice se realizează de Guvern prin intermediul autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

(2) Pentru asigurarea funcției de coordonare strategică, Guvernul instituie și stabilește modul de organizare și funcționare a Consiliului coordonator în domeniul securității cibernetice, organ colegial fără personalitate juridică, a cărui funcție de bază este promovarea și coordonarea, la nivel strategic și operațional, a politicilor în domeniul securității cibernetice.

(3) Strategia națională de securitate cibernetică este un document de politici care definește obiectivele strategice și măsurile de politică și de reglementare care au ca scop atingerea și menținerea unui nivel ridicat de securitate cibernetică. Strategia națională de securitate cibernetică se aprobă de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

Articolul 7. Autoritatea competentă

(1) Guvernul desemnează autoritatea competentă la nivel național în domeniul securității cibernetice și stabilește modul de organizare și funcționare a acesteia.

(2) Autoritatea competentă exercită funcțiile de punct național unic de contact și echipă de răspuns la incidentele cibernetice la nivel național.

(3) Autoritatea competentă exercită următoarele atribuții principale:

a) identifică și ține evidența furnizorilor de servicii pe teritoriul Republicii Moldova;

b) elaborează și asigură promovarea celor mai bune practici pentru gestionarea incidentelor cibernetice și a riscurilor;

c) asigură interacțiunea strategică la nivel internațional și schimbul de experiență cu alte state, organizații internaționale sau entități create de acestea privind aspecte legate de securitatea cibernetică;

d) asigură interacțiunea cu autoritățile și instituțiile publice naționale și cu furnizorii de servicii;

e) exercită supravegherea și controlul respectării de către furnizorii de servicii a obligațiilor ce le revin conform prezentei legi;

f) emite acte cu caracter obligatoriu, recomandări și orientări metodologice pentru furnizorii de servicii în vederea conformării și remedierii deficiențelor constatate și stabilește termenul până la care aceștia trebuie să se conformeze;

g) examinează sesizări cu privire la neîndeplinirea obligațiilor de către furnizorii de servicii;

h) exercită, atribuțiile organului constatator pentru cauze contravenționale în domeniul securității rețelelor și sistemelor informatice în conformitate cu prevederile Codului contravențional;

i) alte atribuții care decurg din prevederile prezentei legi.

(4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale:

a) monitorizează și analizează amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național, precum și acordă asistență furnizorilor de servicii, la solicitarea acestora, în procesul de monitorizare de către aceștia a rețelei lor și a sistemelor lor informatice*;*

b) emite avertizări timpurii, alerte, anunțuri și diseminează informații privind amenințările cibernetice, vulnerabilitățile, riscurile și incidentele cibernetice;

c) recepționează notificări privind incidentele cibernetice care afectează rețelele și sistemele informatice ale furnizorilor de servicii;

d) asigură răspunsul la incidente cibernetice, în conformitate cu procedurile stabilite de prezenta lege și actele normative de punere în aplicare a acesteia, inclusiv acordă asistență în acest sens furnizorilor de servicii;

e) colectează și analizează date criminalistice și furnizează analize dinamice de risc și de incident și conștientizare a situației în materie de securitate cibernetică;

f) cooperează, la nivel național și internațional, cu echipele de răspuns la incidentele cibernetice în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații;

g) efectuează, la cererea unui furnizor de servicii, scanări proactive a rețelelor și a sistemelor informatice ale solicitantului pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, în conformitate cu actul normativ aprobat de Guvern în temeiul articolului 17 alineatul (5);

h) implementează în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate;

i) exercită atribuțiile de coordonator al procesului de divulgare coordonată a vulnerabilităților conform cadrului normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, inclusiv:

- intermedierea și facilitarea interacțiunii dintre persoana fizică sau juridică care raportează o vulnerabilitate și producătorul sau furnizorul de produse TIC sau servicii TIC potențial vulnerabile, la cererea oricăreia dintre aceste entități;
- identificarea și contactarea persoanelor fizice sau juridice implicate;
- acordarea asistenței persoanelor fizice sau juridice care raportează o vulnerabilitate;
- negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități;
- asigurarea anonimatului persoanelor fizice sau juridice care raportează o vulnerabilitate, atunci când acestea o solicită.

(5) În exercitarea funcției de punct național unic de contact, autoritatea competentă exercită următoarele atribuții principale:

a) asigură o legătură a autorităților și instituțiilor publice naționale cu autoritățile similare din alte state și/sau cu organizații internaționale sau entități constituite de către acestea;

b) transmite, la cererea autorităților și instituțiilor publice sau a echipelor de răspuns la incidente cibernetice către punctele unice de contact din alte state notificări și solicitări privind incidentele cibernetice;

c) transmite autorităților și instituțiilor publice naționale, conform competenței acestora, notificări și cereri primite din alte state sau de la organizații internaționale ori de la entitățile constituite de către acestea.

Articolul 8. Centrul guvernamental de răspuns la incidentele de securitate cibernetică

(1) Pentru asigurarea securității cibernetice la nivel guvernamental, Guvernul instituie centrul de răspuns la incidentele cibernetice la nivelul rețelelor și sistemelor informatice ale căror proprietar este statul, desemnează persoana juridică de drept public responsabilă de exercitarea funcțiilor respective și stabilește modul de organizare și funcționare al centrului respectiv.

(2) Guvernul este responsabil de asigurarea cu resursele necesare a centrului de răspuns la incidentele de securitate cibernetică la nivel guvernamental pentru prevenirea, analiza, identificarea şi răspunsul la incidentele cibernetice la nivel guvernamental.

(3) Centrul de răspuns la incidentele cibernetice la nivel guvernamental, menționată în alineatul (1), este responsabilă de asigurarea securității rețelelor și sistemelor informatice ale căror proprietar este statul și de facilitarea realizării de către furnizorii de servicii – persoane juridice de drept public a obligațiilor de asigurare a securității cibernetice prevăzute de prezenta lege, inclusiv a celor de notificare, și a interacțiunii acestora cu autoritatea competentă și echipa de răspuns la incidente cibernetice la nivel național.

Articolul 9. Cadrul național de gestionare a crizelor în domeniul securității cibernetice

(1) Autoritatea competentă este responsabilă de gestionarea incidentelor cibernetice și a crizelor în domeniul securității cibernetice la nivel național.

(2) În acest scop autoritatea competentă aprobă planul național de răspuns la incidentele cibernetice și crizele de securitate cibernetică în care sunt stabilite obiectivele și modalitățile de gestionare a incidentelor cibernetice și a crizelor de securitate cibernetică la nivel național.

(3) Planul național de răspuns la incidente cibernetice și crize de securitate cibernetică trebuie să includă cel puțin însă fără să se limiteze la acestea:

a) obiectivele măsurilor și ale activităților naționale de pregătire;

b) sarcinile și responsabilitățile autorităților naționale competente;

c) procedurile de gestionare a crizelor și canalele de schimb de informații;

d) măsurile de pregătire, inclusiv exerciții și activități de formare;

e) furnizorii de servicii, interacțiunea dintre aceștia și autoritățile sau instituțiile publice responsabile, precum și infrastructura implicată;

f) procedurile și mecanismele de interacțiune dintre autoritățile și instituțiile publice responsabile la nivel național, precum și de interacțiune coordonată a acestora în gestionarea incidentelor și a crizelor de securitate cibernetică de mare amploare, inclusiv a celor la nivel european și internațional.

(4) Guvernul aprobă cadrul metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidente cibernetice și crize de securitate cibernetică, interacțiunea dintre autoritățile și instituțiile publice cu atribuții în procesul de elaborare și actualizare, precum și interacțiunea acestora cu sectorul privat.

Articolul 10. Registrul de stat al incidentelor cibernetice

(1) În scopul evidenței datelor privind apariția, evoluția și soluționarea incidentelor cibernetice, precum și a automatizării proceselor de identificare, înregistrare, documentare, clasificare, analiză și gestionare a astfel de incidente, a monitorizării și evidenței alertelor, amenințărilor cibernetice și vulnerabilităților de securitate cibernetică, Guvernul, la propunerea autorității competente instituie și reglementează modul de organizare și funcționare a Registrului de stat al incidentelor cibernetice și, corespunzător, a sistemului informațional.

(2) Accesul la registru este limitat, iar datele din registru sunt destinate utilizării interne, cu excepția cazului în care de cadrul normativ prevede expres altfel.

Capitolul III. Obligații privind asigurarea securității cibernetice

Articolul 11. Măsurile de securitate ale rețelelor și sistemelor informatice ale furnizorilor de servicii

(1) Furnizorul de servicii este obligat să aplice continuu măsuri de securitate în scopul:

a) prevenirii incidentelor cibernetice;

b) soluționării incidentelor cibernetice;

c) prevenirii și atenuării impactului asupra continuității serviciului sau a securității rețelei și/sau a sistemului informatic cauzat de un incident cibernetic;

d) prevenirii și atenuării unui posibil impact asupra continuității unui serviciu ori rețea sau sistem informatic dependente de cele ale furnizorului de servicii.

(2) În procesul aplicării măsurilor de securitate, furnizorul de servicii este obligat:

a) să evalueze vulnerabilitățile și riscurile rețelei și sistemului informatic, să determine severitatea impactului unui eventual incident cibernetic survenit urmare a materializării riscurilor, să descrie măsurile pentru soluționarea unui incident cibernetic, precum și să întocmească un raport de evaluare în acest sens.

b) să ia măsuri tehnice și organizatorice corespunzătoare și proporționale, în conformitate cu standardul descris la alineatul (4) litera (a), pentru a gestiona riscurile legate de securitatea rețelelor și a sistemelor informatice pe care le utilizează în activitatea sa, inclusiv să aplice:

- politici referitoare la analiza riscurilor și securitatea rețelelor și sistemelor informatice;

- gestionarea incidentelor (prevenire, detectare și răspuns la incidente)
- politici și proceduri privind utilizarea criptografiei și a criptării,
- politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor de securitate cibernetică,
- măsuri privind continuitatea activității, inclusiv gestionarea copiilor de rezervă și recuperarea în caz de dezastru, precum și gestionarea crizelor;
- măsuri de securitate aplicate în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice, inclusiv gestionarea vulnerabilităților și divulgarea acestora,
- măsuri de securitate a resurselor umane, politici de control al accesului și gestionarea activelor,
- măsuri privind securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile dintre fiecare entitate și prestatorii sau furnizorii săi direcți de servicii,
- practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice,
- după caz, utilizarea de soluții de autentificare multifactor sau de autentificare continuă, de comunicații securizate voce, video și text și de sisteme securizate de comunicații de urgență în cadrul furnizorului de servicii,;

c) să mențină în stare de actualitate documentația privind măsurile de securitate;

d) să asigure monitorizarea în scopul detectării serviciilor TIC, proceselor TIC sau produselor TIC care compromit securitatea rețelei sau sistemului informatic;

e) să întreprindă măsuri orientate spre reducerea impactului și a răspândirii unui incident cibernetic, inclusiv, dacă este necesar, restricționarea utilizării sau accesului la rețeaua sau sistemul informatic.

(3) În cazul în care furnizorul de servicii autorizează un terț să administreze rețeaua și/sau sistemul informatic ori utilizează serviciile unui terț pentru găzduirea sistemului informatic, acesta este responsabil pentru aplicarea măsurilor de securitate a rețelei și/sau sistemului informatic de către terț.

(4) În vederea asigurării îndeplinirii obligațiilor prevăzute în prezentul articol și a securității rețelelor și sistemelor informatice ale furnizorilor de servicii, Guvernul:

a) prin intermediul organismului național de standardizare, asigură aprobarea standardelor naționale în domeniul securității informațiilor, securității cibernetice și protecția confidențialității în baza standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice;

b) la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, aprobă cerințele specifice de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.

Articolul 12. Obligațiile furnizorilor de servicii de a notifica incidentele cibernetice

(1) Furnizorul de servicii informează imediat autoritatea competentă, dar nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre un incident cibernetic:

a) care are un impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului;

b) al cărui impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului nu este evident, dar poate fi presupus în mod rezonabil.

(2) Furnizorul de servicii, prezintă autorității competente, imediat, dar nu mai târziu de 72 de ore din momentul în care a luat cunoștință despre incidentul cibernetic, o actualizare a informațiilor prezentate în conformitate cu alineatul (1) și o evaluare inițială a incidentului cibernetic cu impact semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili.

(3) În cazul în care rețeaua sau sistemul informatic al furnizorului de servicii este administrat și/sau găzduit de un terț, furnizorul de servicii trebuie să se asigure că terțul îl informează în termenii stabiliți la alineatele (1) și (2) despre un incident cibernetic, specificat în alineatul (1) sau că terțul informează concomitent în aceiași termeni autoritatea competentă despre faptul producerii unui astfel de incident cibernetic.

(4) Un incident cibernetic are un impact semnificativ dacă este îndeplinită cel puțin una dintre următoarele condiții:

a) impactul incidentului cibernetic este sever conform gradului de consecințe determinat în raportul de evaluare a riscurilor rețelei și sistemului informatic întocmit în conformitate cu prevederile articolul 11 alineatului (2) literele a) - c) și a cerințelor prevăzute de actele menționate la articolul 11 alineatul (4);

b) din cauza incidentului cibernetic prestarea serviciului este întreruptă pentru o perioadă mai mare decât perioada maximă de timp permisă pentru întrerupere, prevăzută în acordul corespunzător privind nivelul agreat al serviciilor, stabilit în cadrul relațiilor contractuale ale furnizorului de servicii, sau cerințele privind continuitatea serviciului stabilite în documentația prevăzută la articolul 11 alineatul (2) litere a) - c);

c) continuitatea serviciului unui terț este perturbată de incidentul cibernetic;

d) furnizorului de servicii, furnizorului altui serviciu sau utilizatorilor serviciilor le-au fost cauzate sau le-ar putea fi cauzate prejudicii materiale sau non-materiale considerabile din cauza incidentului cibernetic.

(5) Furnizorul de servicii este obligat să notifice într-o perioadă rezonabilă de timp, însă nu mai mult de 3 zile:

a) persoanele potențial afectate de incidentul cibernetic cu impact semnificativ sau publicul, dacă persoanele afectate nu pot fi notificate individual;

b) destinatarii serviciilor lor care ar putea fi afectați de o amenințare cibernetică semnificativă și orice măsuri sau măsuri corective pe care destinatarii respectivi le pot lua ca răspuns la amenințarea respectivă. Dacă este cazul, furnizorii de servicii informează, de asemenea, destinatarii în cauză despre amenințarea semnificativă propriu-zisă.

(6) În cazul în care furnizorul de servicii nu realizează obligațiunile de notificare prevăzute de alineatul (5) în termenul respectiv, autoritatea competentă își poate aroga obligația de notificare a persoanelor posibil afectate sau publicul, informând despre aceasta furnizorul de servicii.

(7) În cazul soluționării unui incident cibernetic cu impact semnificativ, furnizorul de servicii este obligat, în termen de 30 zile, să transmită autorității competente un raport

care să includă cel puțin informații despre cauzele producerii incidentului cibernetic, timpul de soluționare a acestuia, măsurile aplicate și impactul incidentului cibernetic.

(8) Procedura de notificare a incidentelor cibernetice, inclusiv interacțiunea dintre furnizorul de servicii și autoritatea competentă, modul de stabilire a impactului unui incident cibernetic și formatul informațiilor evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic sunt stabilite de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

(9) Furnizorul de servicii este obligat imediat, însă nu mai târziu de 24 de ore, să notifice autoritatea competentă despre impactul semnificativ al unui incident cibernetic, care a afectat un terț, asupra continuității serviciului său dacă prestarea acestui serviciu depinde de serviciile prestate de acest terț.

Articolul 13. Notificarea voluntară

(1) Furnizorii de servicii pot notifica autoritatea competentă cu privire la incidente cibernetice, amenințări cibernetice și incidente evitate la limită.

(2) Persoanele juridice de drept public sau de drept privat care nu sunt identificate de autoritatea competentă ca furnizori de servicii pot transmite acesteia notificări cu privire la incidente cibernetice semnificative, amenințări cibernetice și incidente evitate la limită.

(3) Notificările menționate la alineatele (1) și (2) din prezentul articol, sunt soluționate de către autoritatea competentă conform procedurilor stabilite de prezenta lege și a actului aprobat în temeiul articolului 12 alineatului (8), acordând prioritate examinării și soluționării notificărilor obligatorii conform prevederilor prezentei legi și asigurând confidențialitatea și protecția adecvată a informațiilor furnizate de către persoana care a notificat.

(4) Notificarea voluntară nu impune persoanelor menționate la alineatele (1) și (2) nicio obligație suplimentară care nu le-ar fi revenit dacă nu ar fi transmis notificarea, exceptând obligațiile care le revin sau le-ar putea reveni conform legislației corespunzătoare în contextul desfășurării acțiunilor de prevenire, investigare, depistare și urmărire penală a infracțiunilor.

Articolul 14. Măsurile de securitate ale rețelelor și sistemelor informatice ale persoanelor juridice de drept public

(1) Persoane juridice de drept public sunt obligate să aplice măsurile stabilite la articolului 11 alineatele (1)-(3) și cerințele de notificare obligatorie a unui incident cibernetic prevăzute la articolul 12.

(2) Cerințele minime de securitate a rețelelor și sistemelor informatice, ale căror proprietar este statul, sunt stabilite de Guvern la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

Articolul 15. Gestionarea incidentelor cibernetice

(1) Autoritatea competentă coordonează procesul de asigurare a securității cibernetice, de prevenire și de soluționare a incidentelor cibernetice în conformitate cu prevederile prezentei legi și actele normative aprobate în scopul punerii acesteia în aplicare.

(2) În scopul asigurării securității cibernetice, autoritatea competentă monitorizează activitatea privind gestionarea domeniului de nivel superior .md, analizează riscurile asupra securității sistemelor informatice, precum și impactul acestora asupra statului, societății și securității rețelelor și sistemelor informatice.

(3) În scopul prevenirii și soluționării unui incident cibernetic, autoritatea competentă emite alerte populației în scopul luării măsurilor pentru evitarea sau reducerea impactului incidentului cibernetic.

(4) În contextul realizării atribuțiilor funcționale prevăzute de prezenta lege, sau în temeiul unei obligații care decurge dintr-un acord internațional, autoritatea competentă are dreptul de a transmite unui alt stat sau unei organizații internaționale informații privind prevenirea și soluționarea unui incident cibernetic, în cazul în care nu există riscul ca informațiile transmise să prejudicieze securitatea națională sau desfășurarea procedurilor penale.

(5) În cazul transmiterii informațiilor conform alineatului (4), autoritatea competentă este obligată să țină cont de interesele de afaceri ale furnizorului de servicii și să asigure păstrarea secretului comercial în condițiile legislației speciale relevante.

Articolul 16. Schimbul de informații

(1) Furnizorii de servicii și, după caz, alte persoane juridice care nu intră în domeniul de aplicare al prezentei legi pot face schimb reciproc de informații relevante în materie de securitate cibernetică, în mod voluntar, inclusiv schimb de informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice entității care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice, în cazul în care un astfel de schimb de informații:

a) vizează prevenirea și detectarea incidentelor, răspunsul la incidente sau redresarea în urma acestora sau atenuarea impactului lor;

b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de limitare și prevenire a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare sau promovarea colaborării dintre persoanele juridice de drept public și cel de drept privat în domeniul cercetării amenințărilor cibernetice.

(2) Autoritatea competentă intermediază schimbul de informații între persoanele juridice menționate la alineatul (1) prin crearea și gestionarea unor platforme, inclusiv tehnico-tehnologice, și comunități de încredere. Pentru a asigura protecția informațiilor ce au un caracter potențial sensibil, autoritatea competentă facilitează semnarea acordurilor de schimb de informații între participanții la astfel de platforme și comunități. Modul de

semnare, conținutul și alte aspecte privind acordurile de schimb de informații se stabilesc de autoritatea competentă.

(3) Persoanele juridice de drept public pot semna acorduri de schimb de informații în materie de securitate cibernetică în condițiile stabilite de regulamentul aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii statului în domeniul securității cibernetice.

(4) Furnizorii de servicii sunt obligați să informeze autoritatea competentă despre semnarea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) sau retragerea din astfel de acorduri, în termen de 3 zile din data semnării sau, după caz, a retragerii.

Capitolul IV. Supraveghere și control de stat

Articolul 17. Supravegherea de stat în domeniul securității cibernetice

(1) Autoritatea competentă exercită funcția de supraveghere a respectării prevederilor prezentei legi de către furnizorii de servicii prin monitorizarea continuă a modului în care aceștia realizează obligațiile ce le revin conform prevederilor prezentei legi și a actelor normative de punere în aplicare a acesteia.

(2) În cazul în care un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluționeze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluționarea incidentului cibernetic utilizând, dacă este necesar, asistență profesionistă terță.

(3) Pentru contracararea unei amenințări grave imediate asupra securității rețelelor și sistemelor informatice sau pentru eliminarea unei perturbări grave în cazul unui incident cibernetic, autoritatea competentă poate restricționa utilizarea sau accesul la un sistem informatic, dacă sunt îndeplinite cumulativ următoarele condiții:

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

b) administratorul sistemului nu este în măsură sau nu poate în timp util să contracareze amenințarea gravă sau să elimine perturbarea gravă provocată de incidentul cibernetic;

c) nu este posibilă contracararea amenințării grave sau eliminarea perturbării grave provocate de incidentul cibernetic prin aplicarea unei alte măsuri;

d) nu se provoacă un prejudiciu disproporționat prin contracararea amenințării grave sau prin eliminarea perturbării provenite din incidentul cibernetic.

(4) Destinatarul și, în cazul unui furnizor de servicii, autoritatea publică care realizează politica de stat în domeniul respectiv și, dacă e cazul, autoritatea cu funcții regulatorii pe piața din domeniul în care se prestează serviciul respectiv, sunt notificați în cel mai scurt timp însă nu mai târziu de 24 de ore, referitor la aplicarea măsurilor prevăzute la alineatul (3).

(5) Modul de aplicare a măsurilor de supraveghere se stabilesc de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

Articolul 18. Controlul

(1) Autoritatea competentă exercită controlul respectării prezentei legi, aplicând următoarele principii:

a) legalitatea și respectarea competenței stabilite de lege;

b) aplicării doar a sancțiunilor care sunt stabilite de lege;

c) tratarea dubiilor în favoarea furnizorului de servicii;

d) efectuarea controlului pe cheltuiala statului;

e) prescrierea recomandărilor pentru înlăturarea încălcărilor constatate în urma controlului;

f) dreptul furnizorului de servicii de a contesta acțiunile autorității competente, inclusiv în instanța judecătorească.

(2) Autoritatea competentă realizează controlul respectării prevederilor prezentei legi exclusiv în baza unui act motivat emis în acest scop, în baza evaluării riscurilor pentru securitatea rețelelor și sistemelor informaționale ale furnizorilor de servicii, precum și cu înștiințarea în prealabil a furnizorului de servicii despre controlul preconizat.

(3) În vederea efectuării controlului, autoritatea competentă are dreptul să beneficieze de acces la informațiile, bunurile și încăperile deținute de furnizorul de servicii supus controlului, care sunt necesare realizării obiectivelor controlului.

(4) Autoritatea competentă efectuează controale numai în cazul în care:

a) a depistat și, urmare a unei investigații preliminare, a confirmat fapte de încălcare a prevederilor prezentei legi; și/sau

b) a fost sesizată cu privire la încălcări sau îndeplinirea necorespunzătoare a obligațiilor prevăzute de prezenta lege de către furnizorul de servicii.

(5) Modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform prezentei legi, se stabilește de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

Articolul 19. Protecția datelor cu caracter personal

În cazul în care, procesul exercitării funcției de supraveghere și control autoritatea competentă ia cunoștință de faptul că o încălcare de către un furnizor de servicii a obligațiilor prevăzute de prezenta lege poate atrage după sine o încălcare a legislației privind protecția datelor cu caracter personal, autoritatea competentă informează imediat organul de control al prelucrărilor de date cu caracter personal.

Capitolul V. Răspunderea

Articolul. 20 Răspunderea pentru încălcarea dispozițiilor prezentei legi

(1) Personalul autorității competente poartă răspundere, în conformitate cu legislația, pentru neîndeplinirea atribuțiilor funcționale stabilite de actele normative.

(2) Personalul autorităților/instituțiilor publice, furnizorilor de servicii care interacționează cu autoritatea competentă în condițiile prezentei legi, poartă răspundere, în

conformitate cu legislația, pentru neîndeplinirea atribuțiilor funcționale stabilite de actele normative.

(3) Persoanele fizice și juridice poartă răspundere penală, contravențională sau civilă, conform prevederilor actelor normative, pentru neîndeplinirea prevederilor prezentei legi.

(4) Autoritatea competentă constată contravențiile în domeniul securității cibernetice și întocmește procesele verbale corespunzătoare, examinează cauzele contravenționale și aplică sancțiunile contravenționale în conformitate cu prevederile Codului contravențional.

Capitolul VI. Dispoziții finale și tranzitorii

Articolul 21. Intrarea în vigoare a legii și măsuri de implementare

(1) Prezenta lege intră în vigoare pe data de 1 ianuarie 2025.

(2) Guvernul:

a) în termen de 9 luni din data publicării prezentei legi, va întreprinde măsurile necesare pentru instituirea/desemnarea autorității competente, reglementarea modului de organizare și funcționare a acesteia și dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite prin prezenta lege;

b) în termen de 9 luni din data publicării prezentei legi va prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege;

c) în termen de 12 luni din data publicării prezentei legi va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi, inclusiv va determina autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice;

d) în termen de 12 luni din data intrării în vigoare a prezentei legi va elabora și va aproba Strategia națională în domeniul securității cibernetice.

(3) Pentru realizarea eficientă a sarcinii stabilite la alineatul (2) litera a), Guvernul trebuie să asigure autoritatea competentă, astfel încât echipa de răspuns la incidente cibernetice la nivel național să corespundă următoarelor cerințe:

a) să asigure o disponibilitate ridicată a canalelor lor de comunicare evitând punctele unice de defecțiune;

b) să dispună de mai multe mijloace pentru a fi contactată și pentru a contacta alte entități în orice moment;

c) să specifice în mod clar canalele de comunicare și să le aducă la cunoștința bazei de utilizatori și a partenerilor de cooperare;

d) să dispună de sediu/sedii și sistemele informatice de suport, situate în amplasamente securizate;

e) să dispună de un sistem adecvat de gestionare și direcționare a solicitărilor, în special pentru a facilita preluarea, prelucrarea și transmiterea acestora întru-un mod efectiv și eficient;

f) să asigure confidențialitatea și credibilitatea operațiunilor lor;

g) să dispună de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor sale și se asigură că personalul său este format în mod corespunzător;

h) să dispună de sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor sale.

(4) Autoritatea competentă:

în termen de 3 luni de la data intrării în vigoare a actelor normative prevăzute la articolul 4 alineatul (2), în cooperare cu autoritățile publice responsabile de realizarea politicii de stat în sectoarele sau subsectoarele stabilite de Guvern în temeiul prevederilor articolului 4 alineatul (2), precum și, dacă e cazul, cu cele de reglementare a acestor domenii, va identifica furnizorii de servicii, îi va notifica în modul stabilit și îi va include în Lista furnizorilor de servicii, întocmită în condițiile prezentei legi;

va aproba actele normative necesare punerii în aplicare a prevederilor prezentei legi.

(5) Autoritățile publice responsabile de realizarea politicii de stat în sectoarele sau subsectoarele stabilite de Guvern, instituțiile publice responsabile de gestionarea unor domenii conexe sectoarelor și subsectoarelor respective, precum și, dacă e cazul, autoritățile publice de reglementare a acestor sectoare sau subsectoare, vor acorda suportul necesar autorității competente, la solicitarea acesteia, în procesul de identificare a furnizorilor de servicii.

Notă informativă
la proiectul de lege privind securitatea cibernetică

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului
Proiectul a fost elaborat de Ministerul Economiei în comun cu Echipa proiectului Moldova Cybersecurity Rapid Assistance, în coordonarea viceprim-ministrului pentru digitalizare.
2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite
1. Condițiile ce au impus elaborarea proiectului de act normativ (*documentele de politici din care rezultă necesitatea elaborării proiectului de lege)* Cadrul politicii de securitate cibernetică este oferit de un set de documente de politici adoptate de Parlament sau Guvern și care oferă viziunea strategică pentru țară cu privire la modul de înființare, consolidare și asigurare a rezilienței sistemului de securitate cibernetică în Republica Moldova. Astfel, ***Concepția securității informaționale***[1]***,*** aprobată prin Legea nr. 299/2017, reprezintă o viziune de ansamblu asupra scopului, obiectivelor, principiilor și direcțiilor de bază ale activității de asigurare a unui nivel înalt al securității informaționale a Republicii Moldova, 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. Concepția a constituit baza pentru elaborarea ***Strategia securității informaționale***[2] a Republicii Moldova pentru anii 2019-2024 și ***Planul de acțiuni*** pentru implementarea acesteia, aprobate prin Hotărârea Parlamentului nr. 257/2018. Scopul principal al acestei Strategii este de a lega și integra din punct de vedere juridic domeniile prioritare cu responsabilități și competențe de asigurare a securității informațiilor la nivel național, bazată inclusiv pe reziliența cibernetică. Problemele abordate de Strategie, într-un context mai larg al securității informaționale, se referă la cinci componente de bază: securitate cibernetică și investigarea criminalității cibernetice, securitatea spațiului mediatic, contrainformații și securitate, probleme de natură legală și, în final, probleme de conștientizare a maselor. Dintre acestea, cu referire la componenta securității cibernetice, Strategia evidențiază ca cele mai proeminente probleme lipsa unui CERT național (Centrul de răspuns la incidente de securitate cibernetică), responsabil de prevenirea și răspunsul la incidente din domeniul securității cibernetice la scară largă, lipsa unui sistem integrat de management al securității cibernetice și un mecanism viabil de audit al securității cibernetice. În acest context, Strategia stabilește un set de obiective de diferită natură, dintre care evidențiem în mod special următoarele: - crearea/desemnarea entității care va exercita rolul de Centru național de reacție la incidente de securitate cibernetică și care va constitui punctul unic de raportare a incidentelor de securitate cibernetică pentru autoritățile publice competente și persoanele fizice și juridice – cu termen limită de realizare în anul 2021 *(Obiectivul 1, acțiunea 1) din Planul de acțiuni de implementare a Strategiei)*; - elaborarea cadrului normativ pentru asigurarea unui nivel înalt de securitate a rețelelor și a sistemelor informatice la nivel național în baza bunelor practici ale UE cu termen limită de realizare în anul 2024 *(Obiectivul 1, acțiunea 5) din Planul de acțiuni de implementare a Strategiei)*. Diverse aspecte ale securității cibernetice sunt abordate și în alte documente de politici, interconectate cu Strategia securității informaționale, cum sunt:

[1] https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro
[2] https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro

- Strategia de securitate națională, aprobată prin Hotărârea Parlamentului nr. 153/2011[3] (pct. 4.7)
- Strategia Națională de Apărare și Planul de Acțiuni privind implementarea Strategiei Naționale de Apărare 2018–2022, aprobate prin Hotărârea Parlamentului nr. 134/2018[4] (pct. 2.8.2)
- Planul individual de acțiuni de parteneriat Republica Moldova – NATO pentru anii 2022–2023, aprobat prin Hotărârea Guvernului nr. 26/2022[5] (obiectivul 1.7, partea II).

Conform ***Programul de activitate al Guvernului „Moldova vremurilor bune”***[6] una dintre principalele provocări de dezvoltare a Republicii Moldova este vulnerabilitatea la amenințările și riscurile de securitate a statului. Conform acestui Program, ținând cont de obiectivul de extindere a gradului de digitalizare a economiei, a serviciilor și instituțiilor publice, de introducere a opțiunilor de vot electronic, devin imperative și măsurile de contracarare a riscurilor și amenințărilor de tip cibernetic. Printre acțiunile prioritare ale domeniilor transformării digitale, politicii externe și securității și apărării sunt, corespunzător:

- implementarea unui cadru eficient de securitate cibernetică pe modelul statelor cu experiență în acest domeniu;
- consolidarea, extinderea și fortificarea infrastructurilor digitale din sectorul public, inclusiv a centrelor de date și rețelelor informaționale cu aplicarea măsurilor de defensivă cibernetică, dezvoltarea capacităților de asigurare a securității informaționale, cibernetice și de comunicare strategică;
- intensificarea acțiunilor în vederea identificării unor direcții noi de cooperare cu UE și statele sale membre care ar completa și dezvolta prevederile Acordului de asociere în domenii ca securitatea statului, securitatea cibernetică, digitalizarea economiei și liberalizarea continuă a comerțului cu UE în sfera serviciilor și telecomunicațiilor ….
- dezvoltarea capacităților de asigurare a securității informaționale, cibernetice și de comunicare strategică.

În acest context în ***Planul de acțiuni al Guvernului pentru anii 2021-2022***[7], aprobat prin Hotărârea Guvernului nr. 235/2021, Guvernul și-a propus ca obiectiv implementarea unui cadru eficient de securitate cibernetică după modelul statelor cu experiență în acest domeniu (p.2.7) prin elaborarea proiectului de lege privind securitatea rețelelor și sistemelor informaționale (p. 2.7.1) cu termen de realizare decembrie 2022, stabilind ca responsabil principal de realizarea acestei acțiuni Ministerul Economiei

2. Finalitățile urmărite

Proiectul de lege are scopul ca prin implementarea cerințelor, măsurilor și mecanismelor instituite să se asigure un nivel suficient de ridicat de securitate a rețelelor și sistemelor informaționale în Republica Moldova, capabil să asigure protecția intereselor vitale ale persoanelor fizice și juridice, ale societății și ale statului, precum și a intereselor naționale ale Republicii Moldova. Un nivel ridicat de protecție a rețelelor și sistemelor informatice în prestarea unor servicii critice în ambele domenii, public și privat, poate fi atins prin asigurarea unui nivel de reziliență cibernetică adecvată provocărilor și amenințărilor atât din mediul cibernetic, cât și din cel non-cibernetic.

În acest context, urmare a implementării prevederilor proiectului de lege Guvernul își propune următoarele:

- desemnarea unei autorități competente în domeniul securității cibernetice cu funcții de identificare a persoanelor juridice care vor intra în cercul de subiecți asupra cărora se vor răsfrânge

---

[3] https://www.legis.md/cautare/getResults?doc_id=105346&lang=ro

[4] https://www.legis.md/cautare/getResults?doc_id=110013&lang=ro

[5] https://www.legis.md/cautare/getResults?doc_id=129865&lang=ro

[6] https://gov.md/sites/default/files/document/attachments/programul_de_activitate_al_guvernului_moldova_vremurilor_bune.pdf

[7] https://www.legis.md/cautare/getResults?doc_id=128407&lang=ro

prevederile proiectului (furnizori de servicii) și menținere în stare de actualitate a acesteia; de supraveghere și control a modului în care furnizorii de servicii îndeplinesc obligațiile impuse de lege, de stabilire a unor practici comune în gestionarea incidentelor cibernetice și de coordonare operațională a situațiilor de criză, de cooperare și interacțiune la nivel național și internațional și de schimb de experiență cu organizații, state sau alte entități relevante la nivel european în primul rând. În context ținem să evidențiem faptul că Guvernului i se acordă marja discreționară ca, în contextul exercitării prerogativei de desemnare a autorității competente, să decidă fie să desemneze o autoritate publică existentă, fie să instituie o autoritate publică nouă în structura sa administrativă și să o desemneze în calitate de autoritate competentă conform proiectului de lege.

- instituirea unei echipe de răspuns la incidentele de securitate cibernetică (CSIRT) cu competențe la nivel național, asigurarea recunoașterii internaționale a acesteia, în mod special la nivel european, care să exercite atribuții de monitorizare și analiză a amenințărilor cibernetice, vulnerabilităților și incidentelor cibernetice, de răspuns la incidente cibernetice, de asigurare a schimbului de informații și coordonare a procesului de divulgare a vulnerabilităților. Potrivit proiectului de lege se propune ca la nivel național CSIRT să fie stabilit în cadrul autorității competente;
- definirea cadrului general strategic și operațional de coordonare și cooperare dintre sectorul public și privat în domeniul securității cibernetice, inclusiv în ce privește gestionarea crizelor și aprobarea unui plan național de răspuns care să asigurare pregătirii, a capacității de reacție și a recuperării în caz de incidente cibernetice. În același context, proiectului de lege cuprinde norme juridice primare care vor avea ca efect aprobarea de către Guvern a Strategiei naționale privind securitatea cibernetică și instituirea Consiliului coordonator în domeniul securității cibernetice;
- stabilirea obligativității de a implementa măsuri de securitate de către entitățile ale căror servicii sunt critice pentru funcționarea economiei și a societății care să asigure atingerea unui nivel minim comun de securitate a rețelelor și sistemelor informaționale și reziliența serviciilor, ceea ce implicit va avea ca efect creșterea nivelului de pregătire și de răspuns la incidentele cibernetice și amenințările de acest fel;
- instituirea unui mecanism obligatoriu de raportare a incidentelor cibernetice semnificative de către furnizorii de servicii, și a posibilității de notificare voluntară a incidentelor cibernetice de orice categorie atât de către furnizorii de servicii, cât și de persoanele juridice care nu intră în categoria acestora;
- crearea și asigurarea funcționării adecvate a mecanismelor de cooperare eficiente la nivel național și internațional, prin difuzarea de către autoritatea competentă întregii societăți și în mod deosebit entităților ce furnizează servicii în domenii critice, a informațiilor relevante, a avertizărilor și alertelor, precum și a celor mai bune practici internaționale;
- dezvoltarea unor capabilități înalte de reacție la incidentele semnificative sau care ar putea avea impacturi cu potențiale prejudicii considerabile, atât a autorităților responsabile de implementarea politicii de stat în domeniul securității cibernetice, cât și a furnizorilor de servicii.

În conformitate cu prevederile art. 25 din Legea nr.100/2017 privind actele normative și ale Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărârea Guvernului nr. 23/2019, pentru a estima efectele și consecințele adoptării și implementării actului normativ în speță, a fost elaborată ***analiza de impact.*** Conform concluziilor relevate de analiza de impact, opțiunea reglementării problematicii securității cibernetice printr-o lege cadru s-a dovedit, din perspectiva raportului pozitiv dintre beneficii și costuri, a fi opțiunea cea mai plauzibilă, inclusiv din punctul de vedere al necesității de a transpune legislația Uniunii Europene în legislația națională. Este de remarcat stringența soluționării chestiunilor ce vizează aspectele instituționale și organizaționale ale acestui domeniu, prin desemnarea unei autorități competente și a unui CSIRT național cu capacități suficiente și necesare pentru a preveni, detecta și răspunde adecvat amenințărilor și incidentelor de securitate cibernetică. Prin intervenția propusă vor fi instituite premisele fundamentale necesare pentru stabilirea clară a responsabilităților și a răspunderii, precum și a mecanismelor orientate spre promovarea unei mai mari încrederi atât la nivel de autorități, cât și la nivel

de întreprinderi, stimulând schimbul de informații și asigurând o asistența reciprocă bazată pe încredere și diligență.

Implementarea proiectului de lege bineînțeles va presupune costuri de implementare atât pentru sectorul public, a căror sinteză este prevăzută în capitolul 5 din prezenta notă, cât și pentru cel privat, dar în rezultatul implementării măsurilor și cerințelor propuse se va asigura o creștere consecventă a nivelului de reziliență cibernetică a entităților-cheie din Republica Moldova, vor fi generate, economii de costuri atât pentru sectorul privat, cât și pentru societate.

Pe termen mediu și lung, atingerea unei creșteri a capacităților în materie de securitate cibernetică la nivel național ar aduce beneficii substanțiale printr-o cooperare la nivel operațional, stimulare și asistență reciprocă și o mai bună interacțiune cu mediul privat.

Elaborarea proiectului de lege a fost precedată de ***analiza informațiilor conținute în diferitele studii de cercetare și rapoarte de evaluare***, recomandări metodologice, dedicate atât nemijlocit contextului actual de securitate cibernetică în Republica Moldova, cât și contextului european și internațional în acest domeniu.

Astfel, potrivit *Analizei*[8] *modelelor de guvernanță națională în domeniul securității cibernetice și recomandări pentru Moldova*, efectuat de proiectul Asistență Rapidă în domeniul Securității Cibernetice pentru Republica Moldova au fost analizate modelele de guvernanță a 6 state membre ale UE (Republica Cehă, Estonia, Finlanda, Grecia, Regatul Țărilor de Jos și România) și furnizate recomandări ce au vizat în special:

necesitatea adoptării unei Strategii dedicată exclusiv domeniului securității cibernetice, aliniată la cerințele prevăzute în legislația europeană (Directiva NIS2), cu o mai bună coordonare a implementării și corelată cu alte documente de politici relevante;

modelul de guvernanță pentru securitatea cibernetică la nivel național ar trebui să fie mai degrabă unul centralizat, adică să concentreze funcțiile de autoritate competentă, CSIRT național și punct național unic de contact într-o singură autoritate, model caracteristic pentru statele cu resurse limitate;

inițierea în paralel cu o nouă lege privind securitatea cibernetică și a modificărilor în legislația relevantă, inclusiv cea privind infrastructura critică.

elaborarea, aprobarea și dezvoltarea continuă a legislației în domeniul respectiv trebuie însoțită de un amplu proces de consultare publică cu toate părțile interesate, precum și de instruiri și dialog constant pentru implementarea legii, dar și pentru conștientizarea sancțiunilor ce urmează a fi aplicate pentru nerespectare.

De asemenea, *Raportul de evaluare*[9] *privind instituirea unei echipe de răspuns la incidente de securitate cibernetică din Republica Moldova*, efectuat de ITU în septembrie 2022 a înaintat mai multe recomandări, dintre care relevăm în mod deosebit recomandarea privind necesitatea unui CSIRT național, mandatat oficial și recunoscut clar ca entitatea competentă să răspundă la incidente și să coordoneze acest proces, acționând ca punct focal în gestionarea incidentelor și ca centru de coordonare pentru a gestiona schimbul de informații și fluxurile de informații, astfel încât toate părțile relevante să poată raporta incidentele către acest punct central, precum și să dispună de capacitățile necesare pentru a furniza cunoștințe despre cele mai bune practici disponibile, etc.

De rând cu studiile menționate mai sus, în procesul elaborării proiectului de lege au fost luate în considerare următoarele:

Ghid de bune practici[10] al Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) privind modul de constituire și organizare a unui CSIRT;

Raportul[11] ENISA privind investițiile în rețele și sisteme informatice (NIS);

---

[8] Analysis of Cybersecurity National Governance Models and Recommendations to Moldova, efectuat de Moldova Cybersecurity Rapid Assistance Project, septembrie, 2022.

[9] Assessment Report of Moldova National Computer Incident Response Team (cirt-mdmd), efectuat de ITU, în septembrie 2022

[10] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

[11] Report on network and information systems (NIS) investments, ENISA, 2021 (https://www.enisa.europa.eu/publications/nis-investments-2021)

Evaluarea de impact[12], realizată de Comisia Europeană, la propunerea de Directivă a Parlamentului European și a Consiliului privind măsurile de asigurare a unui nivel ridicat de securitate a rețelelor și a informațiilor în întreaga Uniune (Directiva NIS1), etc.

Raport de evaluare a impactului[13] pentru 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 (propunerea de Directivă NIS2).

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

Potrivit Programului de Asociere[14] dintre Uniunea Europeană și Republica Moldova pentru perioada 2021-2027 (Recomandarea nr. 1/2022 a Consiliului de Asociere UE-Republica Moldova din 22 august 2022 privind Programul de asociere UE-Republica Moldova [2022/1997]), unul dintre obiectivele generale ale cooperării dintre UE și Republica Moldova este transformarea digitală rezilientă, ceea ce presupune și asigurarea unor cadre juridice, de politică și operaționale solide în materie de securitate cibernetică, pe baza legislației și a bunelor practici ale UE. În continuare acest document determină prioritățile pe termen scurt și lung ale programului în domeniul „Libertate, securitate și justiție", stabilind colaborarea părților în materie de securitate cibernetică prin implementarea următoarelor măsuri:

- asigurarea punerii în aplicare a măsurilor legate de componenta de securitate cibernetică a Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia;
- consolidarea securității cibernetice prin ***transpunerea în dreptul intern a Directivei (UE) 2016/1148*** a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune („Directiva NIS");
- identificarea și desemnarea în mod oficial a unei echipe naționale de răspuns la urgențe cibernetice (CERT) și stabilirea unei diviziuni clare a muncii și a competențelor între agențiile implicate în asigurarea securității cibernetice;
- elaborarea unei abordări în vederea consolidării cooperării în domeniul securității cibernetice prin intermediul schimbului de informații și de bune practici, în special cu privire la utilizarea setului de instrumente pentru securitatea rețelelor 5G, elaborat de UE.

În același context, una dintre acțiunile, prevăzute de *Planul de acțiuni pentru implementarea măsurilor propuse de către Comisia Europeană în Avizul său privind cererea de aderare a Republicii Moldova la Uniunea Europeană, aprobat de către Comisia Națională pentru Integrare Europeană pe data de 4 august 2022*, ce urmează a fi realizată de Republica Moldova pentru implementarea măsurii de *consolidare a luptei împotriva criminalității organizate, pe baza unor evaluări detaliate ale amenințărilor, a unei cooperări sporite cu partenerii regionali ai UE și internaționali și a unei mai bune coordonări a autorităților de aplicare a legii*, propuse de Comisia Europeană, este *adoptarea Legii privind securitatea rețelelor și a sistemelor informatice, în conformitate cu Directiva UE privind securitatea rețelelor și a informației (NIS), în vederea stabilirii unui cadru eficient de securitate cibernetică.*

La data de 29 decembrie 2022, în Jurnalul Oficial al Uniunii Europene a fost publicată 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). Această Directivă vine să înlocuiască Directiva NIS1 și, potrivit art. 45 al primei, urmează să intre în vigoare în a douăzecea zi de la data publicării. În același timp Directiva NIS2, în art. 41, prevede obligativitatea statelor membre ale UE ca până la 17 octombrie 2024 să adopte și să publice măsurile necesare pentru a se conforma acestei directive, iar de la 18 octombrie să le pună în aplicare. Până la

[12] https://data.consilium.europa.eu/doc/document/ST-6342-2013-ADD-2/en/pdf

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

[14] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22022D1997&from=EN

această data Directiva NIS1 continuă să rămână în vigoare urmând a fi abrogată la data de 18 octombrie 2024 (art.44).

În comparație cu Directiva NIS1, Directiva NIS2:

- extinde cercul de entități și sectoare/subsectoare care sunt vizate de normele de securitate cibernetică;
- elimină diferențierea dintre operatorii de servicii esențiale și furnizorii de servicii digitale, care s-a dovedit a fi caducă;
- instituie o uniformizare mai aprofundată a normelor de securitate cibernetică în statele membre ale UE;
- stabilește aplicarea unor norme care prevăd cerințe mai stricte în materie de securitate cibernetică.
- stabilește un cadru pentru o mai bună cooperare cibernetică și un schimb de informații între diferitele state membre ale UE și creează o bază de date europeană privind vulnerabilitățile, etc.

Obiectivul Directivei NIS2 este de a atinge un nivel mai ridicat de securitate cibernetică în UE decât cel atins până acum prin implementarea Directivei NIS. Cu alte cuvinte Directiva NIS2 este o nouă treaptă în procesul de asigurare a securității rețelelor și sistemelor informatice în statele membre ale UE. Necesitatea unei astfel de îmbunătățiri a fost determinată de deficiențele constatate în procesul reexaminării Directivei NIS1, care o împiedică să soluționeze în mod eficace provocările actuale și cele emergente în materie de securitate cibernetică.[15]

În context, pentru exercițiul nostru este important de relevat că, spre deosebire de contextul Republicii Moldova, contextul european de implementare a Directivei NIS2 este dat în primul rând de faptul că statele membre au atins deja un anumit nivel de securitate cibernetică implementând prevederile Directivei NIS1, ceea ce nu este caracteristic pentru Republica Moldova. După cum deja s-a menționat mai sus, anumite progrese în acest domeniu au fost realizate, însă acestea nicidecum nu pot fi catalogate ca fiind în armonie cu cele existente în Uniunea Europeană.

Din această perspectivă transpunerea în dreptul intern a Directivei NIS2 va fi una parțială și nu doar din perspectiva 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 substanțială a nivelului de reziliență cibernetică a serviciilor critice, iar pe de altă parte să nu constituie o povară insurmontabilă pentru persoanele juridice, în special pentru cele din sectorul privat, dar și pentru bugetul de stat.

În acest context, proiectul de lege cuprinde reglementări care, din punctul de vedere al armonizării legislației naționale cu cea europeană, au ca obiectiv general de a transpune Directiva NIS2. Totuși, proiectul legii asigură o armonizare parțială, creând în principiu doar premisele legale primare pentru acțiuni viitoare cu caracter unic sau permanent, care vor asigura transpunerea într-un volum mai mare a Directivei NIS2. Adițional, este extrem de important de a lua în considerare și alte acte legislative europene, în paralel cu NIS2, care sunt relevante în dezvoltarea domeniului securității cibernetice în Moldova și sunt aplicabile în statele membre ale UE. Într-o etapă imediat următoare publicării proiectului, Guvernul, în comun cu autoritățile responsabile, urmează să aprobe un set de acte normative de punere în aplicare a prevederilor legii, precum și să asigure desemnarea/instituirea, organizarea, dotarea cu resurse necesare și asigurarea funcționalității autorității competente.

Astfel, ținem să evidențiem că Directiva NIS2, ca de altfel și Directiva NIS, sunt acte cu un efect orizontal fundamental, nefiind un instrument de sine stătător. Concomitent cu Directiva NIS2 au fost aprobate alte două acte fundamentale din perspectiva rezilienței cibernetice, și anume:

- 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 (Directiva CER);

[15] Considerentul (2) din Directiva NIS2: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555

- 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 (Regulamentul DORA).

Prin urmare, transpunerea Directivei NIS2 în legislația națională nu poate fi concepută fără demararea imediată a proceselor de transpunere și a celorlalte două acte, parte a pachetului legislativ european direcționat spre creșterea și îmbunătățirea rezilienței sectoarelor de o importanță critică fundamentală pentru funcționarea economiei și a statului. Importanța acestui exercițiu este determinată și de interconexiunile dintre cele trei documente. Regulamentul DORA are un caracter de lex specialis față de prevederile conținute în Directiva NIS2[16], iar interconexiunile[17] 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. Desincronizarea acestor procese la nivel național, de transpunere a celor trei acte europene, constituie un risc serios de implementare a prevederilor proiectului de lege.

De asemenea, autoritățile administrației publice centrale de specialitate responsabile de realizarea politicii de stat în sectoarele și subsectoarele enumerate în anexele II și III ale directivei NIS2 urmează să efectueze o evaluare a gradului de transpunere a legislației UE la care se face referire în aceste anexe, și după caz, să inițieze modificarea legislației sectoriale relevante.

Rezultatele procesului de transpunere în proiectul de lege a prevederilor Directivei NIS2, gradul de transpunere a acesteia și explicațiile de rigoare privind relația dintre componentele acestei directive și părțile corespunzătoare ale proiectului de lege sunt reflectate în tabelul de concordanță, care este parte a dosarului de însoțire a proiectului.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

Domeniul protecției și asigurării securității rețelelor și sistemelor informatice în Republica Moldova nu a constituit până în prezent obiectul unei legi cadru care să reglementeze sistemic problemele de securitate cibernetică. Norme juridice care reglementează aspectele organizatorice, instituționale și funcționale în domeniul asigurării protecției și securității rețelelor și sistemelor informaționale sunt dispersate în câteva legi, principalele dintre acestea fiind:

Legea nr. nr 467/2003[18] cu privire la informatizare si resursele informaționale de stat (art.23) și **Legea nr. 71/2007[19] cu privire la registre** (art.24) reglementează, pe de o parte, responsabilitățile autorităților publice în asigurarea securității cibernetice a sistemelor și resurselor informaționale ale statului, iar pe de altă parte, responsabilitățile entităților, inclusiv private, în protecția informațiilor conținute de resursele și prelucrate de sistemele informaționale pe care le creează.

În același timp, cerințele de securitate pentru rețelele publice de comunicații electronice și serviciile de comunicații electronice accesibile publicului sunt prevăzute la articolele 21 și 22 din ***Legea comunicațiilor electronice nr. 241/2007***[20]. Această lege reglementează activitatea în domeniul comunicațiilor electronice civile a tuturor furnizorilor de rețele sau servicii de comunicații electronice, fie din sectorul public sau privat, și stabilește drepturile și obligațiile utilizatorilor. Legea nu se extinde la rețelele de comunicații speciale. Din punct de vedere al securității rețelelor și serviciilor de comunicații electronice, Agenția Națională pentru Reglementare în Comunicațiile Electronice și Tehnologia Informației este responsabilă de implementarea măsurilor minime de securitate pe care toți

[16] Considerentul (28) din Directiva NIS2: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555
[17] Considerentul (30) din Directiva NIS2: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555
[18] https://www.legis.md/cautare/getResults?doc_id=132933&lang=ro
[19] https://www.legis.md/cautare/getResults?doc_id=131038&lang=ro
[20] https://www.legis.md/cautare/getResults?doc_id=133262&lang=ro

furnizorii ar trebui să le implementeze. Agenția poate verifica și evalua măsurile stabilite de furnizori pentru a garanta securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

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

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

- **Hotărârea Guvernului nr. 201/2017**[21] privind aprobarea cerințelor minime obligatorii de securitate cibernetică, care se adresează atât autorităților guvernamentale, cât și autorităților care nu intră în structura administrativă a Guvernului. Obiectul de reglementare al acestei hotărâri se limitează la aspecte de organizare a sistemului intern de securitate cibernetică, documentația ce necesită a fi aprobată și actualizată periodic, a responsabilităților angajaților entităților care intră în cercul de subiecți ai reglementărilor, a cerințelor propriu-zise ce urmează a fi aplicate atunci când în activitatea instituțiilor respective sunt utilizate soluții de tehnologie a informației și comunicațiilor și, respectiv, de prestare a serviciilor bazate pe astfel de soluții, a cerințelor specifice la achiziția sistemelor informaționale noi sau actualizarea celor existente, precum și a celor ce urmează a fi aplicate la externalizarea administrării/mentenanței sistemelor**.**
- **Hotărârea Guvernului nr. 482/2020**[22] privind aprobarea măsurilor necesare asigurării securității cibernetice la nivel guvernamental, prin care Guvernul reglementează din punct de vedere instituțional, organizatoric, procedural și funcțional sistemul de asigurare a securității cibernetice la nivelul structurii sale administrative, inclusiv desemnează Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică în calitate de Centru guvernamental de reacție la incidente de securitate cibernetică, care constituie și punctul unic de contact și de raportare a incidentelor de securitate cibernetică pentru structurile de tip CERT (echipă de răspuns la incidentele cibernetice) departamentale ale Guvernului.
- **Hotărârea Guvernului nr. 388/2022**[23] privind aprobarea Concepției Sistemului Informațional „Registrul de Stat al Incidentelor de Securitate Cibernetică”, este una dintre măsurile preliminare pentru stabilirea unei platforme informaționale pentru comunicarea strategică cu entitățile publice, precum și pentru asigurarea evidenței amenințărilor, vulnerabilităților în spațiul cibernetic și a incidentelor de securitate cibernetică identificate sau raportate.

Cu toate că actele normative sus-menționate abordează problematica protecției rețelelor și sistemelor informatice, normele conținute de acestea au un caracter disparat și îngust, limitat la obiectivul de a legifera anumite aspecte ale securității cibernetice doar din perspectiva necesităților de reglementare a domeniului care constituie obiectul actului normativ respectiv, în detrimentul unei abordări sistemice, care să coaguleze din punct de vedere normativ la nivel național întregul spectru de măsuri de ordin organizatoric, instituțional, funcțional, procedural și coercitiv în acest domeniu.

Deși la nivel guvernamental anumite mecanisme coordonate de interacțiune sunt deja instituite în art. 23 din Legea nr. 467/2003 și, subsidiar în Hotărârea Guvernului 482/2020 și reflectă o anumită maturitate în gestionarea incidentelor, riscurilor, vulnerabilităților și amenințărilor cibernetice la rețelele și sistemele informaționale, ale căror proprietar este statul, totuși în sectorul public există anumite lacune și inconsistențe referitoare în mod special la aplicabilitatea prevederilor normative asupra autorităților administrației publice locale și la cooperarea CERT-Gov cu autoritățile publice care sunt plasate în afara structurii administrative guvernamentale.

În ce privește sectorul privat, problematica asigurării securității cibernetice este abordată într-o formă limitată în contextul realizării prevederilor Legii nr. 120/2017 cu privire la prevenirea și combaterea terorismului și a actelor de punere în aplicare a acesteia (*Regulamentului privind protecția antiteroristă a infrastructurii critice, aprobat prin Hotărârea Guvernului nr. 701/2018, Regulamentului*

[21] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro

[22] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro

[23] https://www.legis.md/cautare/getResults?doc_id=132011&lang=ro

privind organizarea și desfășurarea testelor antiteroriste, aprobat prin Hotărârea Guvernului nr. 996 /2018 și Ordinul SIS cu privire la aprobarea modelului Pașaportului antiterorist), din perspectiva protecției antiteroriste a infrastructurii critice.

Această situație are ca efect un nivel general insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor legate de securitatea rețelelor și a sistemelor informatice, ceea ce poate submina sau subminează buna funcționare, pe de o parte, a activității administrative, în mod special prestarea serviciilor publice, de către administrația publică centrală și locală, iar pe de altă parte buna funcționare a activității economice desfășurată de către întreprinderile din mediul privat, ceea ce afectează în consecință întreaga economie națională și, implicit, activitatea socială.

Proiectul de lege are ca ***obiect reglementarea*** cadrului juridic, organizațional și de cooperare în domeniul securității cibernetice a persoanelor juridice, competenței autorităților și instituțiilor publice în materie de securitate cibernetică, cadrului național general de gestionare a crizelor în domeniul securității cibernetice, cerințelor, măsurilor și mecanismelor pentru asigurarea securității rețelelor și sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și modul de gestionare a incidentelor cibernetice. Proiectul este structurat în 6 capitole după cum urmează:

În ***capitolul I – Dispoziții generale*** sunt reglementate aspecte ce țin de domeniul de aplicare al legii, principalele noțiuni utilizate și definițiile acestora, aspecte generale privind procesul de identificare a persoanelor juridice asupra cărora prevederile legii urmează să fie aplicate, precum și principiile generale conform cărora subiecții legii urmează să le aplice în procesul de asigurare a securității cibernetice.

Acest capitol de asemenea stabilește principalele criterii în baza cărora autoritatea competentă urmează să identifice persoanele juridice ca furnizori de servicii, criterii ce au la bază regula principală a dimensiunii organizației, dar și criterii specifice precum categoria de servicii prestate (ex. prestatorii de servicii de încredere, furnizorii de rețele și servicii de comunicații electronice accesibile publicului, etc), calitatea prestatorului de servicii (operator al obiectivelor infrastructurii critice), impactul pe care l-ar putea avea perturbarea prestării serviciului, dependența serviciului de rețelele și sistemele informatice, importanța și interconexiunile cu alte servicii sau sectoare și subsectoare.

Capitolul II „Cadrul instituțional, cooperarea și coordonarea strategică la nivel național” cuprinde norme juridice ce reglementează problematici generale ale raporturilor juridice instituite în procesul de planificare și coordonare strategică în domeniul securității cibernetice la nivel național, inclusiv competența Guvernului de aprobare a Strategiei naționale de securitate cibernetică, misiunea Consiliului coordonator în domeniul securității cibernetice, aspecte funcționale ale Autorității competente în domeniul reglementat de prevederile legii, modul de desemnare, atribuții specifice funcției de CSIRT național și de punct unic de contact la nivel național. De asemenea capitolul vizat stabilește norme legale primare de reglementare a cadrului național general de gestionare a crizelor în materie de securitate cibernetică, inclusiv responsabilitatea autorității competente de a elabora și aproba Planul național de răspuns la incidentele și crizele de securitate cibernetică, în baza cadrului metodologic aprobat de Guvern în ce privește elaborarea, actualizarea și implementarea prevederilor acestui plan. În același context, în acest capitol sunt propuse reglementări fundamentale ce vizează instituirea, organizarea și funcționarea Registrului de stat al incidentelor cibernetice și a sistemului informațional ce-l formează. De notat că Guvernul a aprobat deja Conceptul acestui Registru de stat și sistem informațional ce-l formează prin Hotărârea sa nr. **nr. 388/2022, menționată mai sus.**

Capitolul III – Obligații privind asigurarea securității cibernetice – cuprinde reglementări privind măsurile obligatorii de securitate ce urmează a fi întreprinse de către persoanele juridice, identificate de autoritatea competentă ca furnizorii de servicii, pentru a asigura un nivel înalt de securitate a rețelelor și sistemelor informatice proprii, responsabilitățile acestora în legătură cu măsurile respective, aspecte procedurale generale și obligațiile concrete în procesul de gestionare a incidentelor cibernetice semnificative, responsabilitățile în relațiile cu persoanele juridice terțe care nu cad sub incidența prevederilor legii.

De asemenea, capitolul cuprinde reglementări generale privind asigurarea de către autoritatea competentă prin intermediul echipei de răspuns la incidente cibernetice a procesului de gestionare a

acțiunilor orientate spre prevenirea și soluționarea a incidentelor, dar și spre prevenirea și atenuarea impactului asupra continuității serviciului sau a securității rețelei și/sau a sistemului informatic cauzat de un incident cibernetic.

De rând cu acestea, acest capitol include și prevederi privind notificarea voluntară, ceea ce presupune dreptul furnizorilor de servicii să notifice autoritatea competentă cu privire la incidente cibernetice, amenințări cibernetice și incidente evitate la limită, iar persoanele juridice de drept public sau de drept privat care nu sunt identificate de autoritatea competentă ca furnizori de servicii – să transmită acesteia notificări cu privire la incidente cibernetice semnificative, amenințările cibernetice și incidentele evitate la limită.

În contextul acestor reglementări, capitolul în speță abordează și problematica schimbului de informații voluntar, prin instituirea contextului juridico-normativ suficient pentru crearea unor comunități și platforme de schimb de informații, între furnizorii de servicii și dintre aceștia și alte persoane juridice care nu intră în domeniul de aplicare al prezentei legi. Astfel subiecții respectivi pot face schimb reciproc de informații relevante în materie de securitate cibernetică, în mod voluntar, inclusiv de informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice. Conform proiectului de act normativ autoritatea competentă trebuie să intermedieze acest schimb de informații prin crearea și gestionarea unor platforme, inclusiv tehnico-tehnologice, și comunități de încredere, iar pentru a asigura protecția informațiilor ce au un caracter potențial sensibil, autoritatea competentă urmează să-și aroge funcția de a facilita semnarea acordurilor de schimb de informații între participanții la astfel de platforme și comunități.

În ***Capitolul IV – Supraveghere și control de stat*** sunt cuprinse normele juridice ce reglementează aspectele privind exercitarea de către autoritatea competentă a funcțiilor de supraveghere și control de stat. Aceste funcții urmează a fi realizate prin monitorizarea continuă a modului în care aceștia realizează obligațiile ce le revin conform prevederilor legii și a actelor normative de punere în aplicare a acesteia. Atunci când un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluționeze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluționarea incidentului cibernetic utilizând, dacă este necesar, asistență profesionistă terță.

În același context, pentru a contracara o amenințare gravă imediată asupra securității rețelelor și sistemelor informatice sau pentru a elimina o perturbare gravă în cazul unui incident cibernetic sunt stabilite expres condițiile în care autoritatea competentă poate restricționa utilizarea sau accesul la un sistem informatic. În ce privește controlul sunt stabilite reglementările primare minime necesare pentru asigurarea legalității intervenției autorității competente pe această dimensiune.

În ambele cazuri, ale supravegherii și controlului de stat, pentru implementarea prevederilor legii conform articolelor corespunzătoare din capitolul respectiv al proiectului de lege, Guvernul urmează să adopte acte normative care să reglementeze mai detaliat modul de aplicare a măsurilor de supraveghere și modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin.

Capitolul V – Răspunderea – abordează generic, în scop de interconexiune cu legislația cadru din domeniul administrativ, contravențional, penal și de altă natură, problematica răspunderii, pe de o parte a autorității competente inclusiv a personalului acesteia, iar pe de altă parte a persoanelor juridice care cad sub incidența prevederilor legii în calitate de furnizori de servicii, inclusiv angajații acestora. Aici este necesar de evidențiat că o etapă importantă în procesul de implementare a proiectului de lege va constitui elaborarea și aprobarea proiectului de lege pentru modificarea legilor existente astfel încât intercalarea noilor norme legale să evite coliziuni sau lacune ale normelor juridice primare și, implicit, deficiențe de implementare ale prevederilor proiectului de lege în speță.

Capitolul VI – Dispoziții finale și tranzitorii – prevede termenul de intrare în vigoare al legii – 1 an din data publicării, precum și termenele concrete și sarcinile stabilite:

Guvernului: de a întreprinde măsurile necesare pentru instituirea/desemnarea autorității competente, reglementarea modului de organizare și funcționare a acesteia și dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege, de a prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege și de a aduce în concordanță actele proprii;

Autorității competente: de a identifica furnizorii de servicii, îi va notifica în modul stabilit și îi va include în Lista furnizorilor de servicii, întocmită în condițiile legii și de a aproba actele normative necesare punerii în aplicare a legii;

Autorităților și instituțiilor publice să acorde suportul necesar autorității competente în procesul de identificare a furnizorilor de servicii.

Totodată în acest capitol sunt stabilite cerințele față de CSIRT național din perspectiva obligării Guvernului de a dota autoritatea competentă astfel încât aceste cerințe să fie îndeplinite nu doar în faza inițială de înființare a acestei entități, ci și să fie aplicate într-o manieră continuă și permanentă.

5. Fundamentarea economico-financiară

În principiu, impactul economico-financiar al implementării proiectului de lege este detaliat descris în capitolul corespunzător al analizei de impact la proiectul respectiv. Totuși, rezumând cele expuse în analiza de impact, implementarea acestei inițiative va implica costuri:

- pentru bugetul de stat, determinate de necesitatea instituirii/desemnării autorității competente, creării și dotării corespunzătoare cu resurse a unui CSIRT național sau, eventual, atribuirii competenței unui astfel de CSIRT către CERT-Gov,
- pentru furnizorii de servicii din sectorul privat - privind necesitatea conformării cu cerințele noi stabilite de noul cadru legal în domeniul securității cibernetice.

În ce privește costurile privind autoritatea competentă și CSIRT național modelul[24] de cost estimat pentru înființarea acestora este în mare măsură determinat de obiectivele stabilite pentru această organizație, de poziția sa juridică și de grupul de interese (constituenții).

Pentru realizarea funcțiilor enunțate mai sus autoritatea competentă, în cazul în care va include în competența sa și realizarea funcției de CSIRT național va avea necesarul de **minim 25 de angajați**, fără a include aici conducătorii, personalul de suport (în cazul creării unei entități noi) și personalul dedicat realizării funcției de supraveghere (numărul acestuia este direct dependent de numărul furnizorilor de servicii). Având în vedere prevederile cadrului normativ național în domeniul salarizării**,** și presupunând că personalul respectiv este divizat în patru subdiviziuni (numărul funcțiilor fundamentale ce urmează a fi realizate de autoritatea competentă) remunerarea anuală a muncii acestui personal ar constitui:

- în cazul instituției publice: ***între 3,6 mil. lei și 8,5 mil lei anual*****;**
- în cazul unei autorități administrative centrale sau autorități administrative în subordinea unui minister**: *între 1,9 mil lei și 3,2 mil. lei anual*.**

La aceste cheltuieli de personal, urmează a fi adăugate cheltuieli investiționale unice inițiale de circa ***10 mil. lei (0,5 mil Euro)*** în echipamentul și instrumentarul tehnic al CSIRT.

De asemenea, o estimare a costurilor ce țin de asigurarea cu sediu ce corespunde cerințelor Directivei NIS2 urmează a fi efectuat atunci când Guvernul, în temeiul prevederilor legale propuse în proiect va exercita dreptul său discreționar de a decide înființarea unei noi entități sau atribuirea competențelor unei autorități existente.

În analiza de impact la Directiva NIS1, experții Comisiei Europene au stabilit că „*Pentru cele trei state membre care nu au înființat încă CERT-uri naționale/guvernamentale (Cipru, Irlanda și Polonia), costul estimat al punerii în funcțiune a infrastructurii și serviciilor aferente, pe baza interviurilor realizate cu CERT-uri care sunt deja operaționale, ar fi de* ***aproximativ 2,5 milioane EUR pentru fiecare CERT*****.”.**

[24] The cost model of Competent Cyber Authority, Moldova Cybersecurity Rapid Assistance Project, October 2022;

În același context, Agenția Europeană pentru Securitate Cibernetică a publicat un ghid[25] privind modul de creare și asigurare a funcționalității unui CSIRT care oferă informații și privind costurile estimative la nivelul țărilor membre, necesare pentru instituirea unui CSIRT național.

În ce privește costurile de conformare pentru persoanele juridice din sectorul privat, estimarea costurilor de implementare a legii pentru întreprinderile care vor cădea sub incidența obligațiilor stabilite de lege actualmente este o provocare în condițiile unei lipse acute a datelor statistice primare în domeniu securității cibernetice, precum și lipsei unor evaluări și analize financiare bazate pe astfel de date la nivel național. Totuși anumite orientări pe această dimensiune sunt acordate de Comisia Europeană în procesul de evaluare[26] 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***.”

În ce privește costurile pentru entitățile administrației publice și furnizorii de servicii asociați cu raportarea obligatorie a unui incident semnificativ, Comisia Europeană a estimat în aceeași analiză de impact că *costul preconizat pentru fiecare notificare de încălcare ar fi de **125 EUR**….., iar în ceea ce privește posibilele investigații care pot fi inițiate de către autoritățile competente de securitatea rețelelor și informațiilor (NIS) cu privire la respectarea obligațiilor de gestionare a riscurilor și de notificare a incidentelor NIS….. costul maxim pentru entitatea afectată ar fi de maximum **25 000 EUR** pe investigație.*

Totodată, ținem să relevăm că Planul de acțiuni privind implementarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărârea Guvernului 811/2015[27], a estimat costurile de creare, dotare și asigurare a funcționalității unui centru de reacție la incidente cibernetice la nivel național la circa 49,6 mil. lei, dintre care 29,7 mil lei urmau a fi dedicate în anul 2016 exclusiv acțiunilor de creare a acestui centru.

6. Modul de încorporare a actului în cadrul normativ în vigoare

1. Cadrul juridic ce necesită a fi modificat și/sau elaborat și aprobat

În conformitate cu prevederile art. 20 alin (2) din proiectul de lege, Guvernul urmează, în termen de cel mult 6 luni din data publicării Legii privind securitatea cibernetică să asigure elaborarea și să prezinte Parlamentului propuneri de modificare a legilor în vigoare care sunt conexe domeniului reglementat de actul normativ în speță. Astfel, deși la momentul actual este destul de ambițios de a identifica prevederile specifice ale unor legi-cadru ce reglementează alte domenii și care cu certitudine necesită a fi modificate în contextul aducerii în concordanță cu prevederile legii în speță, totuși ar putea fi anticipată necesitatea, cel puțin a examinării, în contextul realizării acestui obiectiv, a următoarelor legi care cuprind reglementări privind securitatea și protecția rețelelor și sistemelor informatice:

- Legea nr. 1069/2000 cu privire la informatică;
- Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat;
- Legea nr.71/2007 cu privire la registre;
- Legea nr. 241/2007 comunicațiilor electronice;
- Legea nr.133/2011 privind protecția datelor cu caracter personal;
- Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;

În același context, unei examinări aprofundate urmează a fi supuse legile cadru care reglementează sectoarele, subsectoarele și tipurile de entități ce prestează servicii în acestea, enumerate în anexele I și II la Directiva NIS2, în contextul în care Guvernul urmează să aprobe lista acestor sectoare și subsectoare de rând cu tipurile persoanelor juridice. Examinarea acestei categorii de acte normative naționale urmează a fi efectuată în primul rând din perspectiva armonizării acestora cu actele sectoriale relevante ale Uniunii Europene, menționate de altfel în anexele respective ale Directivei NIS2.

[25] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc.
[26] https://data.consilium.europa.eu/doc/document/ST-6342-2013-ADD-2/en/pdf
[27] https://www.legis.md/cautare/getResults?doc_id=110324&lang=ro

În continuare pentru a asigura implementarea prevederilor legale noi, urmează a fi supuse dacă nu unei revizuiri, cel puțin unei examinări aprofundate în scopul confirmării conformității cu prevederile noii legi a următoarelor acte normative guvernamentale:

- Hotărârea Guvernului nr. 201/2017 privind aprobarea cerințelor minime obligatorii de securitate cibernetică;
- Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental;
- Hotărârea Guvernului nr. 388/2022 cu privire la aprobarea Concepției Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică".

În același context, Guvernul urmează să aprobe un set de acte normative de punere în aplicare a noului cadru normativ în domeniul securității cibernetice, prevăzute de proiectul de lege:

a) lista sectoarelor, subsectoarelor și, respectiv, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și/sau subsectoare (art. 5 alin. (3));

b) cadrul metodologic privind identificarea persoanelor juridice de drept public sau privat ca fiind furnizori de servicii (art. 5 alin. (3));

c) instituirea și reglementarea modului de organizare și funcționare a Consiliului coordonator în domeniul securității cibernetice (art.6 alin. (2));

d) Strategia națională de securitate cibernetică (art.6 alin. (3)), având la bază pe de o parte rezultatele și concluziile procesului de analiză a modului de implementare a Strategiei naționale de securitate informațională, aprobată prin Hotărârea Parlamentului nr. 257/2018, și pe de altă parte prevederile articolului 7 al Directivei NIS 2;

e) modul de organizare și funcționare a entității care va exercita funcțiile autorității competente (art. 7 alin. (1));

f) modul de coordonare de către autoritatea competentă a procesului de divulgare a vulnerabilităților (art. 7 alin. (4) lit. i));

g) cadrul metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidente cibernetice și crize de securitate cibernetică, interacțiunea dintre autoritățile și instituțiile publice cu atribuții în procesul de elaborare și actualizare, precum și interacțiunea acestora cu sectorul privat (art. 9 alin. (4));

h) modul de organizare și funcționare a Registrului de stat al incidentelor cibernetice și a sistemului informațional corespunzător art. 10 alin. (1));

i) asigurarea, prin intermediul organismului național de standardizare și în cooperare cu autoritatea competentă, aprobarea Standardului Moldovenesc în domeniul securității informațiilor, securității cibernetice și protecția confidențialității în baza standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice art. 11 alin. (4));

j) cerințele specifice privind măsurile de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii (art. 10 alin. (4);

k) procedura de notificare a incidentelor cibernetice, inclusiv interacțiunea dintre furnizorul de servicii și autoritatea competentă, modul de stabilire a impactului unui incident cibernetic și formatul informațiilor evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic (art. 12 alin. (8)).

l) regulamentul privind condițiile și cerințele în care sunt semnate de către autoritățile și instituțiile publice acordurile de schimb de informații în materie de securitate cibernetică (art. 16 alin. (3));

m) modul de aplicare a măsurilor de supraveghere de către autoritatea competentă (art. 17 alin. (5));

n) modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii privind securitatea cibernetică (art. 18 alin. (5)).

2. Schimbările instituționale preconizate prin aprobarea proiectului de act normativ

În temeiul art. 7 alin. (1) din proiectul de act normativ Guvernul urmează să desemneze autoritatea competentă la nivel național în domeniul securității cibernetice. De asemenea, potrivit prevederilor art. 20 alin. (2) Guvernul urmează să asigure dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege.

Potrivit proiectului de act normativ Guvernului i se conferă o marjă discreționară în procesul de desemnare a acestei autorități competente fie prin instituirea unei autorități/instituții publice noi fie prin identificarea și atribuirea competenței prevăzute de proiectul de act normativ unei entități publice existente. În oricare dintre cazurile menționate Guvernul urmează, după aprobarea sau, după caz, revizuirea modului de organizare a entității desemnate ca fiind autoritatea competentă în sensul prevederilor proiectului de lege, să inițieze procesul de ajustare a structurii, efectivului-limită și organigramei entității respective și să asigure aprobarea statelor de personal noi și a schemei de încadrare corespunzătoare.

De asemenea, Guvernul conform art. 20 alin. (2) lit. a) urmează să asigure dotarea autorității competente, inclusiv CSIRT național, cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege. Pentru realizarea acestei sarcini conform prevederilor art. 20 alin. (3) din proiectul legii, Guvernul trebuie să doteze autoritatea competentă, astfel încât CSIRT național să corespundă cerințelor stipulate la acest alineat, care sunt în principiu cerințele față de astfel de echipe stabilite de Directiva NIS2 la art. 11 alin. (1).

7. Avizarea și consultarea publică a proiectului

În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional pe pagina web oficială a Ministerului Economiei *me.gov.md* și pe platforma de consultare *particip.gov.md,* la data de 23 decembrie 2022 a fost publicat anunțul referitor la inițierea elaborării proiectului de lege la care au fost anexate analiza de impact la proiect și versiunea inițială a acestuia.

Proiectul urmează a fi plasat pentru consultări publice pe pagina web oficială a Ministerului Economiei *me.gov.md* și pe platforma de consultare *particip.gov.md.*

8. Constatările expertizei anticorupție

Proiectul urmează a fi supus expertizei anticorupție

9. Constatările expertizei de compatibilitate

Proiectul urmează a fi supus expertizei de compatibilitate

10. Constatările expertizei juridice

Proiectul urmează a fi supus expertizei juridice

11. Constatările altor expertize

Proiectul a fost examinat în prealabil de către Cancelaria de Stat și Ministerul Finanțelor.

În data de 17.01.2023 proiectul a fost examinat în cadrul ședinței Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător și a fost susținut condiționat.

Analiză de impact
la proiectul de lege privind securitatea cibernetică

Titlul analizei impactului (poate conţine titlul propunerii de act normativ):	Proiectul Legii privind securitatea cibernetică
Data:	
Autoritatea administraţiei publice (autor):	Ministerul Economiei
Subdiviziunea:	Direcția politici în domeniul tehnologiei informației și economiei digitale
Persoana responsabilă şi datele de contact:	Andrei CUȘCĂ, șef al Direcției politici în domeniul tehnologiei informației și economiei digitale, tel. 022 250 557, e-mail: andrei.cusca@me.gov.md

Compartimentele analizei impactului

1. Definirea problemei

a) Determinați clar şi concis problema şi/sau problemele care urmează să fie soluţionate

Problema principală care urmează a fi soluționată prin inițiativa de reglementare legală propusă poate fi descrisă ca fiind un nivel general insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor legate de securitatea rețelelor și a sistemelor informatice, ceea ce poate submina sau subminează buna funcționare, pe de o parte, a activității administrative, în mod special prestarea serviciilor publice, de către administrația publică centrală și locală, iar pe de altă parte buna funcționare a activității economice desfășurată de către întreprinderile din mediul privat, ceea ce afectează în consecință întreaga economie națională și, implicit, activitatea socială.

Această problemă fundamentală cuprinde un set de elemente componente specifice care necesită a fi puse în evidență pentru a releva importanța unei intervenții imediate pe dimensiunea instituirii consolidării și asigurării unei funcționalități adecvate a mecanismului de asigurare a securității cibernetice la nivel național, după cum urmează.

- disfuncționalități în activitatea economică a diferiților actori, de stat sau privați, activitate care e bazată din ce în ce mai mult pe producerea de bunuri și prestarea de servicii, prin utilizarea tot mai intensă a tehnologiilor informaționale;
- numărul, frecvența și complexitatea în creștere a incidentelor de securitate cibernetică;
- o percepere deficitară a întinderii fenomenului respectiv, a gravității impacturilor incidentelor de securitate cibernetică asupra vieții administrative, economice și sociale sau, cel puțin asupra gravității și complexității incidentelor;
- reziliența cibernetică scăzută a unor sectoare și domenii în care buna funcționare a securității rețelelor și sistemelor informatice este primordială pentru menținerea unei bune funcționări a activității economice, sociale, administrative sau de altă natură critică pentru întreaga țară

- un nivel scăzut de conștientizare comună a potențialului negativ pe care îl comportă contextul actual național și lipsa unor mecanisme viabile care să permită reacționarea comună, imediată și eficace în situații de criză.

b) Descrieți problema, persoanele/entitățile afectate și cele care contribuie la apariția problemei, cu justificarea necesității schimbării situației curente și viitoare, în baza dovezilor și datelor colectate și examinate

Potrivit documentului de concept al proiectului Strategiei naționale de transformare digitală[28] industria tehnologiei informației și comunicațiilor (TIC) din Moldova a cunoscut o creștere dinamică, datorită cererii ridicate de pe piață, concurenței și efortului consolidat al tuturor actorilor implicați. Acesta generează anual circa 7% din Produsul Intern Brut (PIB) al țării, apropiindu-se de o valoare totală a veniturilor de circa 15 miliarde MDL sau 900 milioane USD.

Pe parcursul ultimilor 5 ani, piața de comunicații electronice a avut o perioadă de concurență și creștere agilă, poziționând țara în destinații de top pe dimensiunea Internet de mare viteză, accesibilitate, iar recent – cu disponibilitatea Internetului Gigabit. În perioada 2015-2020, motorul creșterii industriei TIC în Moldova a devenit sectorul tehnologiei informației (IT), care a crescut de patru ori, depășind telecomunicațiile. O politică și un cadru legislativ dedicat pentru tehnologia informației și industriile digitale au jucat un rol central în evoluția sa remarcabilă și dinamică. Comparând ponderea în PIB a sectorului IT în 2020 de circa 3,6% cu cea de 0,8% în 2013, când sectorul IT a fost declarat ca prioritate de politică, dinamica este remarcabilă. Creșterea în industria IT a fost determinată de avantajele Moldovei ca destinație de externalizare a serviciilor IT, bazate pe cost, locație și competențe, precum și de un regim fiscal și administrativ facilitat pentru rezidenții Virtual Moldova IT Park. Rapoartele globale privind digitalizarea (Indicele UN DESA e-Guvernare, Indicele de dezvoltare în rețea NRI, Indicele de țară digitală, etc.), rapoartele ANRCETI și sondajele naționale anuale ale Agenției de Guvernare Electronică (AGE) atestă realizări considerabile ale Republicii Moldova în accesul la internet și dispozitive IT, precum și crearea platformelor de e-guvernare.

Totuși, dezvoltarea rapidă a tehnologiei informației și comunicațiilor electronice și a proceselor de transformare digitală deși au adus beneficii indiscutabile în toate domeniile, în același timp, au fost însoțite de creșterea semnificativă și continuă a numărului de amenințări la adresa securității cibernetice.

Intensificarea digitalizării a avut drept consecință evoluția semnificativă a acestor amenințări. Criza provocată de pandemia COVID-19 a demonstrat importanța serviciilor electronice pentru populație, sectorul public și privat. Totodată această criză ne-a demonstrat cât de rapid pot evolua amenințările la adresa securității cibernetice și cât de sensibile sunt serviciile electronice și economia digitală în fața acestor provocări cibernetice.

Spre exemplu raportul de evaluare[29] efectuat de ITU arată o imagine de ansamblu asupra amenințărilor cibernetice în Republica Moldova. La fel ca în alte țări, Moldova este afectată de diferite tipuri de atacuri cibernetice. Acestea vizează nu numai entitățile guvernamentale, ci și sectorul privat și populația în general. Deși autoritățile specializate urmăresc și monitorizează peisajul amenințărilor cibernetice legate de entitățile guvernamentale, lipsește o înțelegere holistică a atacurilor cibernetice care au loc în țară. Tipurile comune de incidente de securitate cibernetică sunt legate de: scams; phishing (including smishing and vishing); ransomware; web defacement; denial of service. Din 2015, țara s-a confruntat cu patru tipuri de atacuri, inclusiv DDOS, phishing, atacuri de forță brută care au încercat să

[28] https://particip.gov.md/ru/document/stages/anunt-privind-initierea-elaborarii-strategiei-de-transformare-digitala-a-republicii-moldova-pentru-anii-20232030-stdm-2030/9355

[29] Assessment Report of Moldova National Computer Incident Response Team (cirt-mdmd), ITU, septembrie 2022

obțină acces la sistemele informatice guvernamentale și deturnarea paginilor web oficiale. Sectorul privat este vizat în egală măsură de amenințările cibernetice. Între timp, IMM-urile se străduiesc să se apere și, prin urmare, reprezintă cea mai vulnerabilă parte a sectorului privat. Acest lucru ridică îngrijorări deosebite, deoarece în 2019 IMM-urile reprezentau aproximativ 98,6% din numărul total de întreprinderi[30], iar mai puțin de 17% dintre acestea au integrat cu succes tehnologiile digitale în activitatea lor. Acest lucru dezvăluie un potențial uriaș neexploatat, dar evidențiază și necesitatea urgentă a IMM-urilor de a-și transforma afacerile și de a adopta protocoale de securitate cibernetică.[31] IMM-urile sunt adesea victime ale atacurilor ransomware care au ca rezultat criptarea bazelor lor de date contabile. Cetățenii sunt, de asemenea, supuși atacurilor cibernetice, iar cele mai frecvente sunt vishingul și smishingul. Infractorii cibernetici au succes în aceste tipuri de atac datorită nivelului redus de cultură digitală și igiena cibernetică. Una dintre grupurile criminale prinse în 2021 pentru furt de bani din conturile bancare a folosit Viber pentru a contacta cetățenii și a se prezenta ca angajați ai băncii. Începând din 2020 și până în septembrie 2021 când au fost prinși, au făcut peste 40 de retrageri din conturile bancare ale mai multor persoane fizice.

Lipsa unor politici bine definite și reglementărilor naționale pune în pericol funcționarea economiei în Republica Moldova, în mod special a celei digitale. În acest sens, reziliența cibernetică a persoanelor juridice (publice și private), care sunt prestatorii de servicii esențiale și critice pentru funcționarea economiei naționale și a statului în ansamblu, devine un element de importanță majoră.

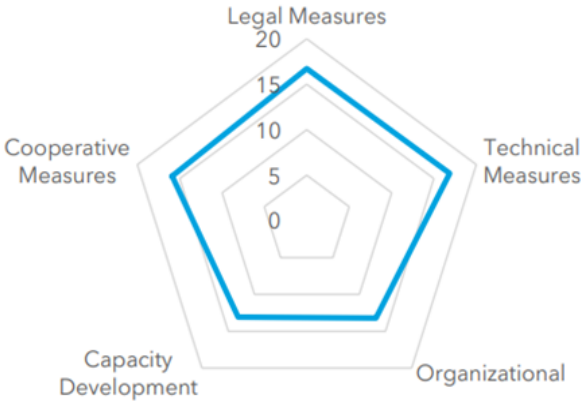
Republica Moldova nu dispune de proceduri mature între autoritățile guvernamentale competente și marile întreprinderi critice pentru a coopera și a face schimb de informații fără întârzieri nejustificate, în special în ceea ce privește identificarea entităților critice, a riscurilor, a amenințărilor cibernetice și a incidentelor, precum și în ceea ce privește riscurile, amenințările și incidentele necibernetice care afectează entitățile critice, inclusiv măsurile de securitate cibernetică și fizică luate de entitățile critice, precum și rezultatele activităților de supraveghere desfășurate cu privire la astfel de entități

Conform Indicelui global de securitate cibernetică (GCI) al ITU pentru 2020, Moldova ocupă locul 33 în regiunea Europei și locul 63 la nivel mondial. GCI este o referință de încredere care măsoară angajamentul a 194 de țări față de securitatea cibernetică la nivel mondial, sporind în același timp gradul de conștientizare a importanței și dimensiunilor problemelor de securitate cibernetică și evaluând rezistența și fiabilitatea sectorului TIC al țărilor. Metodologia de evaluare a GCI analizează modul în care fiecare țară abordează aspectele legate de securitatea cibernetică în cadrul politicilor sale naționale. Aceasta se realizează cu ajutorul unui chestionar care abordează principalii factori care contribuie la gradul de pregătire al unei țări în materie de securitate cibernetică. Potrivit raportului de evaluare[32] efectuat de ITU în vederea instituirii la nivel național a unei echipe de răspuns la incidentele de securitate cibernetică, în pofida îmbunătățirilor în domeniul TIC, performanța Moldovei în cadrul Indexului global de securitate cibernetică (GCI) 2020 a scăzut. Acest declin poate fi atribuit în principal eliminării și adăugării de noi întrebări, precum și modificărilor aduse metodologiei și ponderării GCI. Cu toate acestea, Republica Moldova a înregistrat progrese semnificative începând cu 2015 în ceea ce privește măsurile legate de elaborarea și punerea în aplicare a politicilor interne, a acordurilor internaționale și a obligațiilor pentru a proteja infrastructura informațională critică a țării.

Performanța Republicii Moldova în Indexul Global al Securității Cibernetice (GCI)[33] pentru anul 2020 este ilustrată în imaginea de mai jos:

[30] https://statistica.gov.md/newsview.php?l=ro&idc=168&id=6716
[31] https://www.odimm.md/ro/digitalizarea
[32] Assessment Report of Moldova National Computer Incident Response Team (cirt-mdmd), ITU, septembrie 2022
[33] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Moldova (Republic of)



Development Level:
Developed Country, Landlocked Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Organizational, Capacity Development Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.78	16.73	16.86	13.21	13.09	15.89

Source: ITU Global Cybersecurity Index v4, 2020

Acest grafic arată că Republica Moldova mai are loc pentru îmbunătățiri în anumiți piloni ai GCI. Printre aceștia se numără structurile de măsuri organizaționale și să adopte măsuri de evaluare a nivelului de dezvoltare a securității cibernetice la nivel național.

În același context, evaluarea maturității în domeniul securității cibernetice a Republicii Moldova este reflectată și de indicele național de securitate cibernetică (NCSI)[34]. Acesta este un indice global în timp real, care măsoară gradul de pregătire a țărilor pentru a preveni amenințările cibernetice și a gestiona incidentele cibernetice. NCSI este, de asemenea, o bază de date cu materiale de evidență disponibile publicului și un instrument pentru consolidarea capacităților naționale în domeniul securității cibernetice. În figura de mai jos este reflectată poziția Republicii Moldova și principalii indicatori care reflectă maturitatea țării în materie de securitate cibernetică.

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

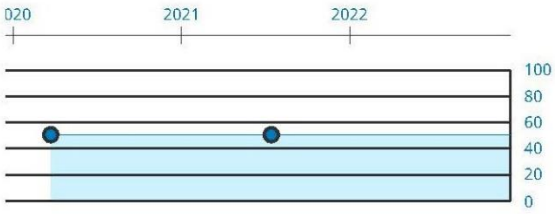
NCSI
national cyber security index

72. Moldova (Republic of) 50.65

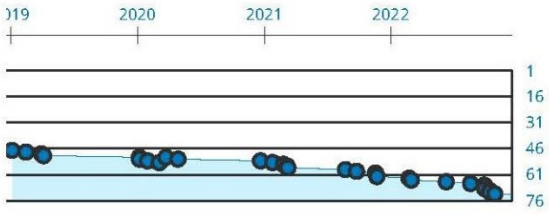
Population	3.6 million
Area (km²)	33.8 thousand
GDP per capita ($)	5.7 thousand

72nd	National Cyber Security Index	51 %
63rd	Global Cybersecurity Index	76 %
59th	ICT Development Index	65 %
69th	Networked Readiness Index	49 %

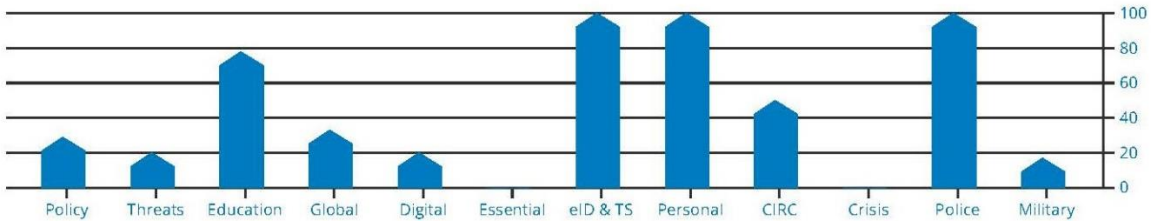
NCSI DEVELOPMENT TIMELINE



RANKING TIMELINE



NCSI FULFILMENT PERCENTAGE



Restanțele cele mai accentuate sunt dezvoltarea politicilor de securitate cibernetică, analiza amenințărilor cibernetice și a informațiilor, protecția serviciilor digitale, cooperarea militară în domeniul cibernetic, care sunt situate sub nivelul de 30%, iar protecția serviciilor esențiale și managementul crizelor de securitate cibernetică având valoarea 0%.

c) Expuneți clar cauzele care au dus la apariţia problemei

Problematica enunțată și descrisă în subcompartimentele anterioare, rezumată la reziliența cibernetică scăzută a actorilor esențiali, perturbarea activității cărora ar putea prejudicia considerabil viața economică și socială caracterizată în mod special printr-un nivel insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor la securitatea rețelelor și a sistemelor informatice ale acestora are la bază o serie de cauze, principalele dintre care constau în următoarele:

1. lipsa unui cadru instituțional și normativ care să stabilească în mod clar responsabilitățile și, implicit, acțiunile ce necesită a fi întreprinse în caz de incidente și crize de securitate cibernetică atât de autoritățile administrației publice cât și de către diverși actori din sectorul privat.
2. Absența unei echipe de răspuns la incidentele de securitate cibernetică la nivel național (CSIRT național), al cărui obiectiv principal este de a spori siguranța, securitatea și protecția digitală a țării și are un mandat oficial formal pentru a îndeplini o astfel de responsabilitate la nivel național.
3. măsuri de securitate a rețelelor și sistemelor informatice și cerințe față de astfel de măsuri insuficiente sau chiar lipsa acestora, ale unor actori din sectorul privat, a căror activitate poate fi calificată ca fiind esențială în prestarea unor servicii;

4. schimbul insuficient de informații cu privire la incidente, riscuri și amenințări de securitate cibernetică. Majoritatea breșelor de securitate nu sunt raportate și trec neobservate, în principal din cauza reticenței companiilor de a împărtăși aceste informații, de teama daunelor aduse reputației sau a răspunderii. De cele mai multe ori, persoanele responsabile de securitatea rețelelor și a sistemelor informatice împărtășesc informațiile relevante doar cu grupuri mici pe care le consideră de încredere, mai degrabă decât să treacă prin canalele oficiale. Schimbul insuficient de informații cu privire la amenințări și riscuri duce la o pregătire insuficientă, iar schimbul insuficient de informații cu privire la incidente duce la o reacție insuficientă. Indisponibilitatea unor date și informații fiabile privind amenințările și incidentele de securitate cibernetică împiedică autoritățile publice responsabile să elaboreze politici bazate pe date concrete și să reacționeze în timp util la incidentele care afectează rețelele guvernamentale.
5. De asemenea, nu există în prezent un cadru instituțional, procedural și normativ-juridic pentru schimbul de informații de încredere privind amenințările, riscurile și incidentele de securitate între sectorul public și cel privat.
6. lipsa unui cadru coerent de gestionare a crizelor de securitate cibernetică în caz de incidente cibernetice de mare amploare sau care ar putea sau au impact semnificativ asupra sectoarelor critice;
7. Lipsa unor norma legale primare privind obligativitatea implementării de către furnizorii de servicii esențiali a unor măsurilor de asigurare a securității cibernetice, precum și a unui mecanism, inclusiv a unei autorități competente în exercitarea funcției de supraveghere și control a modului de implementare a unor astfel de mecanisme.

d) Descrieți cum a evoluat problema şi cum va evolua fără o intervenție

Problematica asigurării securității informaționale a țării a constituit totdeauna o preocupare în legătură cu procesul de transformare digitală a țării. Această preocupare a fost reflectată de-a lungul anilor în documentele de politici, ca parte componentă a procesului de dezvoltare a societății informaționale în Republica Moldova, reflectată în documente de politici precum Strategia Națională de edificare a societății informaționale – "Moldova electronică", Strategia națională de dezvoltare a societății informaționale "Moldova Digitală 2020", Programul de modernizare tehnologică a Guvernării, etc.

Cu toate acestea o abordare oficială mai pronunțată față de domeniul securității cibernetice și problematicii acestuia a fost acordată odată cu adoptarea de către Parlament, în anul 2017 a Concepției securității informaționale a Republicii Moldova și, în anul 2018, de către Guvern, a Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, obiectivul de bază al căruia a constituit crearea unui sistem de management al securității cibernetice a Republicii Moldova prin securizarea serviciilor societăți informaționale, contribuind astfel la dezvoltarea unei economii bazate pe cunoaștere, ceea ce, la rândul său, va stimula creșterea gradului de competitivitate economică și de coeziune socială, precum și va asigura crearea de noi locuri noi de muncă.

Actualmente, aceleași obiective sunt consacrate și în Strategia securității informaționale una dintre problemele de bază identificate de aceasta fiind lipsa unei entități de tip CERT (Centru de reacție la incidente de securitate cibernetică), la nivel național, responsabile de prevenirea și reacția la incidente din domeniul securității cibernetice.

Deși un set de acțiuni în conformitate cu aceste documente de politici au fost întreprinse de către autoritățile responsabile totuși până în prezent, în Moldova nu s-a reușit crearea sau stabilirea unei autoritățile competente pe domeniul securității cibernetice la nivel național.

Această situație limitează autoritățile publice responsabile în realizarea misiunii de care sunt responsabile – realizarea politicii de stat în domeniul securității cibernetice. În cazul lipsei elementelor

menționate, sectorul public și privat, precum și societatea vor fi supuse în continuare unor riscuri majore aferente amenințărilor de securitate cibernetică.

Un element negativ este lipsa totală a sistemului de răspuns la incidentele de securitate cibernetică la nivel național, precum și lipsa suportului eficient pentru mediul de afaceri.

Lipsa unor reguli de protecție a rețelelor și sistemelor informatice și de prevenție a incidentelor va duce la devieri de la entitate la entitate. Respectiv schimbul de informații (cel voluntar) ar putea fi inutil din motivul perceperii diferite și neconcordanțelor între procedurile interne ale entităților.

În special este de menționat un alt element negativ prin prisma situației geopolitice în regiune, când sectorul public nu va dispune de instrumente de comunicare transparentă cu alte state și de asigurare a schimbului de informații privind incidentele și vulnerabilitățile, asigurând interesele sectorului public și mediului de afaceri din Moldova.

Lipsa reglementării domeniului securității cibernetice va vulnerabiliza autoritățile publice, persoane fizice și persoane juridice în față provocărilor de securitate cibernetică, care sunt permanent în creștere.

Pentru entitățile esențiale și importante, impactul monetar al unei încălcări a datelor este substanțial. Cel mai recent raport *IBM Cost of a Data Breach*[35] a stabilit că în anul 2022 costul mediu al unei încălcări a datelor la nivel global a atins un maxim istoric de 4,35 milioane USD. Această cifră reprezintă o creștere cu 2,6% față de anul precedent și o creștere cu 12,7% față de anul 2020.

Raportul respectiv evidențiază principalii factori care contribuie la costurile mai mari ale încălcării datelor, privite prin prisma sectoarelor și regiunilor geografice și detaliază măsurile pe care organizațiile le pot lua pentru a minimiza riscurile de încălcare a securității:

- Costurile suportate privind încălcarea datelor sunt cu 3,05 milioane USD mai mici pentru în cazul organizațiile care folosesc instrumente de inteligență artificială (AI) și automatizare;
- Organizațiile care au o echipă CSIRT și își testează în mod regulat planul de răspuns la incidente au economisit în medie 2,66 milioane USD;
- Organizațiile care au implementat o arhitectură de încredere zero au în medie cu 1 milion USD mai puțin în costuri de încălcare;
- Tehnologiile de detectare și răspuns extinse (XDR) au ajutat la economisirea în medie de 29 de zile în timpul de răspuns la încălcare.

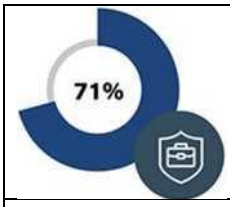
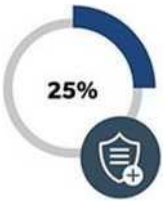
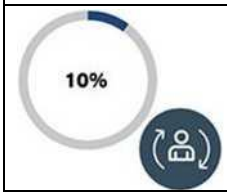
Raportul IBM din 2022 a citat mai multe componente contributive care afectează costurile de încălcare a datelor. Costul mediu al unei breșe de date pentru organizațiile cu infrastructură critică a fost în general de 4,82 milioane USD - cu 1 milion USD mai mult decât costul mediu pentru organizațiile din alte industrii. Costul mediu al unui atac de phishing în 2022 a fost calculat la 4,91 milioane USD, comparativ cu 4,54 milioane USD pentru ransomware și 4,50 milioane USD pentru acreditările furate sau compromise.

Potrivit raportului, în timp ce costurile de încălcare a datelor asociate cu reputația deteriorată, timpul de oprire a afacerii și reglementările/litigiile rămân semnificative, o tendință mai recentă este o creștere bruscă a costurilor primelor de asigurare cibernetică din cauza frecvenței și gravității încălcărilor, împreună cu plățile considerabile pentru ransomware. Pe tema ransomware-ului, dovezile sugerează că companiile sunt din ce în ce mai deschise să plătească răscumpărări ca parte a răspunsului lor la încălcare, chiar și alocă milioane de dolari în acest scop. Conform raportului IBM din 2022, 62% dintre cele 550 de

[35] https://www.ibm.com/downloads/cas/3R8N1DZJ

organizații care suferă de încălcări studiate au declarat că nu au suficient personal pentru a-și satisface nevoile de securitate.

Potrivit *Consultancy.eu*, care este o platformă online pentru industria de consultanță, costurile și cheltuielile asociate unui incident cibernetic pot fi clasificate în patru segmente de mai jos.

	**Asistență și măsuri de urgență** • Identificarea, evaluarea și limitarea evenimentului de securitate (IT Forensic) • Furnizarea de asistență juridică (Încălcarea confidențialității datelor) • Furnizarea de asistență pentru gestionarea crizelor sau comunicare
	**Costuri adiționale** • Restabilirea sistemului informatic la starea sa anterioară • Menținerea operabilității sistemului IT • Pregătirea cererii • Prevenirea sau limitarea răspunderii/detectarea și controlul oricărei utilizări necorespunzătoare a datelor cu caracter personal (încălcarea datelor). • Strategie de comunicare • Notificare către autoritate sau către persoane fizice (încălcarea datelor) • Răscumpărare • Costurile de apărare rezultate în urma unei investigații efectuate de o autoritate de reglementare • Amenzi din partea autorităților naționale, pentru încălcarea drepturilor de protecție a datelor cu caracter personal
	**Acoperire de răspundere** Cheltuieli de apărare și daune care decurg din pretenții formulate de terți: • Un eveniment de securitate • Încălcare a confidențialității datelor cu caracter personal • Defăimarea, deteriorarea reputației, încălcarea proprietății intelectuale, încălcarea vieții private etc
	**Pierderea cifrei de afaceri și creșterea costului muncii** • Întreruperea afacerii • Cheltuieli suplimentare

Incapacitatea întreprinderilor și a autorităților de a reacționa rapid la un incident și de a atenua impactul acestuia vor conduce, cel mai probabil, la o descreștere a încrederii generale a cetățenilor în economia digitală, ceea ce ar putea avea un impact negativ asupra creșterii economice și a investițiilor.

Situația poate, de asemenea, alimenta în continuare criminalitatea informatică, extremism, pericolul terorismului, alte fenomene negative, precum și război hibrid.

Situația existentă nu va preveni eventualele pierderi financiare cauzate de atacurile cibernetice, cum și nu va duce la prevenirea riscurilor/daunelor de mediu în cazul unui atac asupra unui serviciu esențial.

Respectiv, incidentele de securitate cibernetică vor provoca imediat sau vor avea potențialul de a provoca perturbări operaționale sau pierderi financiare substanțiale la diferite nivele ale oricărei entități și chiar la nivel de economie națională.

Ca urmare a incidentului vor fi afectate direct sau cel puțin indirect alte persoane fizice sau juridice, cauzând pierderi materiale sau morale considerabile.

Pentru mediul privat în continuare vor surveni daune din cauza perturbării serviciilor digitale drept rezultat al incidentelor de securitate cibernetică, fiind necesare investiții enorme pentru asigurarea securității cibernetice proprii din motivul lipsei suportului din partea autorităților.

Pentru mediul public, aceasta ar însemna, de asemenea, un risc de creștere a cheltuielilor bugetare pentru atenuarea ad-hoc a amenințărilor, precum și costuri suplimentare pentru soluționarea situațiilor de urgență legate de incidentele de securitate cibernetică.

Pentru societate, lipsa unei abordări a incidentelor de securitate cibernetică va duce la pierderii de venituri datorate perturbărilor economice potențiale.

e) Descrieți cadrul juridic actual aplicabil raporturilor analizate și identificați carențele prevederilor normative în vigoare, identificați documentele de politici și reglementările existente care condiționează intervenția statului

Cadrul de politici și cadrul normativ

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

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

Concepția securității informaționale[36], aprobată prin Legea nr. 299/2017

Concepția reprezintă o viziune de ansamblu asupra scopului, obiectivelor, principiilor și direcțiilor de bază ale activității de asigurare a unui nivel înalt al securității informaționale a Republicii Moldova, securitatea informațională fiind parte componentă a sistemului național de securitate.

Potrivit acestei concepții măsurile de prevenire, depistare și contracarare a amenințărilor complexe și persistente la adresa securității informaționale pot fi întreprinse doar cu condiția existenței și funcționării unui cadru normativ corespunzător în domeniu, a unor instrumente și metode bine definite, a unor mecanisme de colaborare la nivel național și internațional." Concepția securității informaționale a Republicii Moldova este determinată de necesitatea protejării intereselor statului, ale societății și ale persoanei, a obiectivelor vitale și de importanță strategică pentru securitatea națională, de necesitatea asigurării protecției informației atribuite la secret de stat, precum și de necesitatea prevenirii și combaterii criminalității informatice.

Concepția constituie baza pentru elaborarea Strategiei securității informaționale a Republicii Moldova și a Planului de acțiuni pentru implementarea strategiei respective. În primul capitol Concepția descrie situația în domeniu și definește problemele din acest sector, stabilește obiectivele de bază, amenințările la adresa securității informaționale, realizarea cărora are ca scop asigurarea protecției, în spațiul informațional, a drepturilor și libertăților fundamentale, a democrației și a statului de drept. În partea a doua Concepția descrie instrumentele și căile de soluționare a problemelor identificate, inclusiv direcțiile strategice și tactice de asigurare a securității informaționale, principiile și principalele sarcini ale autorităților competente, metodele de asigurare a securității informaționale (juridice, tehnico-

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

organizatorice, economice, contrainformative și de securitate), cooperarea internațională în acest domeniu și organizarea sistemului de asigurare a securității informaționale. În ce privește aspectul organizării sistemului respectiv, concepția desemnează Serviciul de Informații și Securitate ca fiind, în limitele competenței atribuite prin lege autoritatea națională de coordonare a activității autorităților publice desfășurate în domeniul securității informaționale.

Strategia securității informaționale[37] a Republicii Moldova pentru anii 2019-2024 și Planul de acțiuni pentru implementarea acesteia, aprobate prin Hotărârea Parlamentului nr. 257/2018

După cum s-a menționat mai sus, Concepția securității informaționale reprezintă documentul de bază pentru elaborarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și documentul de politici ce integrează domeniile centrale și asociate spațiului informațional, ce oferă noțiuni, definește principiile de organizare la nivel de stat, societate și persoană, precum și detaliază metodele juridice, tehnico-organizatorice, economice și contrainformative pentru asigurarea securității informaționale a Republicii Moldova..

În acest context, **scopul principal** al Strategiei securitate informațională este de a lega și integra din punct de vedere juridic domeniile prioritare cu responsabilități și competențe de asigurare a securității informațiilor la nivel național, bazată inclusiv pe reziliența cibernetică.

Scopul și obiectivele acestei Strategii se realizează în baza Planului de acțiuni pentru implementarea acesteia. Astfel, în contextul definirii problemelor și al descrierii situației la momentul adoptării strategiei, acest document evidențiază un spectru larg de probleme cu care se confruntă până acum Republica Moldova. Problemele abordate de Strategie se referă la cinci componente de bază ale securității cibernetice și investigației criminalității cibernetice, securitatea spațiului media, componenta de contrainformații și securitate, aspectele juridice și, în final, problemele de conștientizare a maselor.

Dintre acestea, Strategia evidențiază problemele cele mai proeminente cum ar fi lipsa unui CERT național (Centrul de răspuns la incidente de securitate cibernetică), responsabil de prevenirea și răspunsul la incidente din domeniul securității cibernetice la scară largă la nivel național, lipsa unui sistem integrat de management al securității cibernetice și un mecanism viabil de audit al securității cibernetice, precum și lipsa de specialiști calificați, programe de formare specializată adresate angajaților organelor de drept, dotarea insuficientă cu echipamente și software, finanțare redusă pentru participarea specialiștilor la proiecte internaționale și evenimente pentru consolidarea capacităților și schimbul de bune practici etc.

Strategia include mai multe cerințe fundamentale pentru a obține o mai bună guvernare a securității cibernetice la nivel național, precum și o listă de acțiuni propuse și indicatori de progres.

Diverse aspecte ale securității cibernetice sunt abordate și în alte documente de politici, interconectate cu Strategia securității informaționale, cum sunt:

- Strategia de securitate națională, aprobată prin Hotărârea Parlamentului nr. 153/2011[38]
- Strategia Națională de Apărare și Planul de Acțiuni privind implementarea Strategiei Naționale de Apărare 2018–2022, aprobate prin Hotărârea Parlamentului nr. 134/2018[39]

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

[38] https://www.legis.md/cautare/getResults?doc_id=105346&lang=ro

[39] https://www.legis.md/cautare/getResults?doc_id=110013&lang=ro

- Planul individual de acțiuni de parteneriat Republica Moldova – NATO pentru anii 2022–2023, aprobat prin Hotărârea Guvernului nr. 26/2022[40].

Din perspectiva **cadrului normativ, l**a nivel național, Republica Moldova nu are o lege-cadru care să reglementeze sistemic problemele de securitate cibernetică. Normele juridice care reglementează aspectele organizatorice, instituționale și funcționale în domeniul asigurării protecției și securității rețelelor și sistemelor informaționale sunt dispersate în câteva în legi.

Legea nr. nr 467/2003[41] cu privire la informatizare si resursele informaționale de stat (art.23) și **Legea nr. 71/2007[42] cu privire la registre** (art.24) reglementează, pe de o parte, responsabilitățile autorităților publice în asigurarea securității cibernetice a sistemelor și resurselor informaționale ale statului, iar pe de altă parte, responsabilitățile entităților, inclusiv private, în protecția informațiilor conținute de resursele și prelucrate de sistemele informaționale pe care le creează.

În același timp, cerințele de securitate pentru rețelele publice de comunicații electronice și serviciile de comunicații electronice accesibile publicului sunt prevăzute la articolele 21 și 22 din ***Legea comunicațiilor electronice nr. 241/2007***[43]. Această lege reglementează activitatea în domeniul comunicațiilor electronice civile a tuturor furnizorilor de rețele sau servicii de comunicații electronice, fie din sectorul public sau privat, și stabilește drepturile și obligațiile utilizatorilor. Legea nu se extinde la rețelele de comunicații speciale. Din punct de vedere al securității rețelelor și serviciilor de comunicații electronice, Agenția Națională pentru Reglementare în Comunicațiile Electronice și Tehnologia Informației este responsabilă de implementarea măsurilor minime de securitate pe care toți furnizorii ar trebui să le implementeze. Agenția poate verifica și evalua măsurile stabilite de furnizori pentru a garanta securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

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

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

- **Hotărârea Guvernului nr. 201/2017**[44] privind aprobarea cerințelor minime obligatorii de securitate cibernetică, care se adresează atât autorităților guvernamentale, cât și autorităților care nu intră în structura administrativă a Guvernului;
- **Hotărârea Guvernului nr. 482/2020** [45]privind aprobarea măsurilor necesare asigurării securității cibernetice la nivel guvernamental, care completează, în special, cu măsuri organizatorice decizia sus-menționată, dar numai pentru autoritățile și instituțiile publice care fac parte din structura administrativă guvernamentală;

[40] https://www.legis.md/cautare/getResults?doc_id=129865&lang=ro

[41] https://www.legis.md/cautare/getResults?doc_id=132933&lang=ro

[42] https://www.legis.md/cautare/getResults?doc_id=131038&lang=ro

[43] https://www.legis.md/cautare/getResults?doc_id=133262&lang=ro

[44] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro

[45] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro

- **Hotărârea Guvernului nr. 388/2022**[46] privind aprobarea Concepției Sistemului Informațional „Registrul de Stat al Incidentelor de Securitate Cibernetică”, este una dintre măsurile preliminare pentru stabilirea unei platforme informaționale pentru comunicarea strategică cu entitățile publice, precum și pentru asigurarea evidenței amenințărilor, vulnerabilităților în spațiul cibernetic. și incidente de securitate cibernetică identificate sau raportate.

Modelul organizațional actual de securitate cibernetică în Republica Moldova este reprezentat de autorități și instituții publice, aflate în structura administrativă a Guvernului sau în afara acesteia, cu un spectru divers de responsabilități cu incidență pe întregul eșichier de realizare a politicii de stat în domeniul securității cibernetice.

Consiliul Coordonator pentru Asigurarea Securității Informaționale a fost înființat prin Hotărârea Guvernului nr. 467/2022[47]. Acest organism colectiv, cu atribuții consultative și operaționale, a fost instituit pentru integrarea sistemică a entităților participante în spațiul informațional și susținerea unui nivel înalt de securitate informațională, inclusiv securitate cibernetică. Activitatea Consiliului se concentrează pe patru niveluri: cibernetic; operațional; mass-media și civic -privat. Consiliul monitorizează activitatea persoanelor juridice de drept public și privat responsabile cu implementarea Planului de acțiuni pentru implementarea Strategiei securității informaționale. Activitatea consultativă se desfășoară la nivelul Consiliului între membrii constitutivi în cadrul ședințelor ordinare sau extraordinare, pe teme axate pe asigurarea securității informaționale și cibernetice. Activitatea operațională constă în finalizarea de către Consiliu a complexului de măsuri de reacție la pericole, riscuri și amenințări ale securității informaționale și cibernetice, implementarea acțiunilor necesare de către persoane juridice, atât publice, cât și private, la nivelul departamentului, interinstituțional. , sectorial, intersectorial sau național, conform cadrului normativ care reglementează activitatea componentelor societății informaționale. Secretariatul Consiliului este asigurat de Cancelaria de Stat.

Ministerul Economiei este autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul tehnologiei informației, societatea informațională, tehnologia informației, economia digitală, securitatea cibernetică și guvernanța internetului.

Ministerul Infrastructurii și Dezvoltării Regionale este autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul comunicațiilor electronice, inclusiv elaborarea, coordonarea și monitorizarea politicilor privind gestionarea domeniului de nivel superior .md, precum și asigurarea evaluării conformității echipamente de comunicații electronice.

Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (STISC), în subordinea Cancelariei de Stat, administrează, întreține și dezvoltă infrastructura informatică, sistemul de telecomunicații al autorităților administrației publice ca parte a rețelei speciale de comunicații și sistemele informaționale de stat, gestionează infrastructura cheilor publice (PKI) a Guvernului, precum și implementează politica de securitate cibernetică.[48] În cadrul STISC funcționează **CERT-Gov**[49] . CERT-Gov[50] este un CSIRT guvernamental, adică o echipă responsabilă numai pentru sisteme și rețele informatice de stat. Activitatea acestei entități se concentrează pe coordonare, formare și alte funcții administrative. Activitățile lor de răspuns la incidente sunt limitate din cauza lipsei de oameni cu

[46] https://www.legis.md/cautare/getResults?doc_id=132011&lang=ro

[47] https://www.legis.md/cautare/getResults?doc_id=132064&lang=ro

[48] https://www.legis.md/cautare/getResults?doc_id=128904&lang=ro

[49] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro

[50] https://stisc.gov.md/ro/cert-gov-md

cunoștințe tehnice de specialitate puternice, dar și din cauza insuficienței echipamentelor tehnice și a cadrului normativ deficitar. În principiu CERT-Gov acționează ca punct național de contact național „de facto", deoarece oficial la nivel juridico-normativ încă nu a fost stabilit un CERT național.

Agenția de Guvernare Electronică (Hotărârea de Guvern nr.760/2010 [51]privind organizarea și funcționarea Agenției de E-Guvernare) în subordinea Cancelariei de Stat este responsabilă pentru implementarea politicilor în domeniile de modernizare a serviciilor guvernamentale, și transformarea digitală a guvernării, gestionează platforma și servicii electronice guvernamentale (MConnect, MPass, MSign, MPay , etc). (anexa nr. 4 la Hotărârea Guvernului nr. 414/2018[52]). De asemenea, Agenția are și responsabilități ce țin de asigurarea securității informației în autoritățile și instituțiile din sectorul public. Agenția de e-Guvernare împreună cu partenerii săi ia măsuri juridice, organizatorice și tehnice complexe de garantare a securității informațiilor [53]. Conform regulamentului său de activitate, principalele responsabilități ale Agenției în domeniul securității cibernetice sunt auditul securității cibernetice în sectorul public, inclusiv monitorizarea implementării rezultatelor auditului securității cibernetice; cercetarea securității cibernetice, precum și supravegherea instituțiilor publice în ceea ce privește implementarea cerințelor minime de securitate.

Serviciul de Securitate și Informații (SIS) avea un rol important în protejarea infrastructurii critice din țară, precum și a sistemelor speciale de telecomunicații [54]. Cu toate acestea, în prezent, SIS se concentrează pe securitatea fizică și mai puțin pe aspectele de securitate cibernetică. Responsabilitățile diferitelor instituții sunt în discuție, întrucât SIS așteaptă legislația de la Ministerul Economiei privind CIIP. Potrivit informațiilor de la mai multe părți interesate, SIS nu a avut rolul de lider în dezvoltarea CIIP și armonizarea legislației moldovenești cu Directiva NIS. Potrivit pct. 115 din Strategia de securitate a informațiilor, Serviciul de Securitate și Informații are rolul principal în procesul de monitorizare și coordonare a implementării Strategiei de securitate a informațiilor și a Planului de acțiuni al acesteia.

Centrul pentru combaterea crimelor informatice al Inspectoratului Național de Investigații al **Inspectoratului General de Poliție** al Ministerului Afacerilor Interne este unitatea principală de investigare a criminalității informatice, însărcinată cu activități de investigație specială și de urmărire penală în materie de criminalitate informatică. Centrul este activ în furnizarea de asistență și îndrumare unităților de poliție locale în materie de criminalitate cibernetică și dovezi electronice. Centrul are un contract bilateral cu CERT-GOV pentru schimbul de informații privind incidentele cibernetice. Centrul cooperează, de asemenea, cu SIS și le oferă informații despre situația din spațiul cibernetic național.

Procuratura Generală are o secție specializată - Secția combaterea crimelor cibernetice. însărcinată cu investigarea și urmărirea penală a cazurile de criminalitate informatică, cu investigarea întregului spectru de infracțiuni prevăzute de articolul 2-10 Convenția de la Budapesta, precum și a infracțiunilor conexe împotriva sau cu utilizarea sistemelor informatice și a datelor.

Agenția Națională de Reglementare pentru Comunicații Electronice și Tehnologia Informației[55] (ANRCETI) este autoritatea publică centrală care reglementează activitatea în comunicațiile electronice, tehnologia informației și comunicațiile poștale, asigură implementarea

[51] https://www.legis.md/cautare/getResults?doc_id=130646&lang=ro

[52] https://www.legis.md/cautare/getResults?doc_id=128904&lang=ro

[53] http://www.egov.md/en/about

[54] https://www.legis.md/cautare/getResults?doc_id=129284&lang=ro

[55] https://en.anrceti.md/informatie_sumara

strategiilor de dezvoltare în aceste sectoare și supraveghează conformitatea furnizorilor de comunicații electronice și de servicii poștale cu legislația care reglementează aceste sectoare. Modul de organizare și funcționare a ANRCETI este stabilit de Guvern[56]. Cu toate acestea, această entitate este autonomă față de Guvern în activitatea sa de reglementare. Potrivit legii, Agenția aprobă regulile [57]de implementare a măsurilor minime de securitate și integritate a rețelelor publice de comunicații electronice și/sau a serviciilor de comunicații electronice accesibile publicului, precum și elaborează reglementări privind administrarea domeniului de nivel superior .md.[58]

Ministerul Apărării este implementatorul Strategiei Naționale de Apărare pentru anii 2018-2021. Strategia menționează și activități de apărare cibernetică. Armata moldovenească își dezvoltă, însă doar propriile capacități defensive și propriul CERT pentru a-și proteja propriile rețele.

2. Stabilirea obiectivelor

a) Expuneți obiectivele (care trebuie să fie legate direct de problemă și cauzele acesteia, formulate cuantificat, măsurabil, fixat în timp și realist)

Obiectivul general al intervenției preconizate este creșterea nivelului de reziliență cibernetică a serviciilor critice pentru întreaga societate, în ambele sectare privat sau public, asigurând un nivel ridicat de protecție a rețelelor și sistemelor informatice ale furnizorilor de servicii utilizate în procesul de prestare a serviciilor lor.

Ca **obiective specifice** care odată realizate vor asigura atingerea obiectivului general enunțat mai sus ținem să evidențiem următoarele:

- Instituirea/desemnarea unei autorități competente în domeniul securității cibernetice cu funcții de supravegherea și control, identificare și menținere în stare de actualitate a listei furnizorilor de servicii, interacțiune strategică la nivel internațional și schimb de experiență cu organizații, state sau alte entități relevante la nivel european în primul rând, uniformizare a practicilor în gestionarea incidentelor cibernetice și coordonarea operațională a situațiilor de criză
- Desemnarea/ instituirea unei CSIRT cu competențe la nivel național, asigurarea recunoașterii internaționale a acesteia, în mod special la nivel european, care să exercite monitorizează și analizează amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național răspunsul la incidente cibernetice, asigurarea schimbului de informații și coordonare a procesului de divulgare a vulnerabilităților; Pentru ca un CSIRT național să fie eficient în interiorul țării sale, acesta ar trebui să stabilească și să mențină relații bune cu părțile interesate naționale și transnaționale, inclusiv cooperarea cu alte echipe naționale și CSIRT - atât în regiunea sa geografică, cât și la nivel mondial;
- Implementarea unor măsuri de securitate de către furnizorii de servicii care să asigure atingerea unui nivel minim comun de securitate a rețelelor și sistemelor informaționale proprii ceea ce implicit va acea ca efect creșterea nivelului de pregătire și de răspuns la incidentele cibernetice și amenințările de acest fel.
- Asigurarea unei cooperări eficiente la nivel național și internațional, prin difuzarea de către autoritatea competentă întregii societăți și în mod deosebit entităților ce furnizează servicii în

[56] https://www.legis.md/cautare/getResults?doc_id=125209&lang=ro

[57] https://www.legis.md/cautare/getResults?doc_id=119924&lang=ro

[58] https://en.anrceti.md/node/35

domenii critice, a informațiilor relevante, a avertizărilor și alertelor, precum și a celor mai bune practici internaționale;
- Dezvoltarea unor capabilități înalte de reacție la incidentele semnificative sau care ar putea avea impacturi cu potențiale prejudicii considerabile, atât autorităților responsabile de implementarea politicii de stat în domeniul securității cibernetice, cât și furnizorilor de servicii.

În același context este necesar de evidențiat că un obiectiv convergent al contextului expus îl constituie necesitatea, având în vedere statutul de țară candidat pentru aderarea la Uniunea Europeană a Republicii Moldova, alinierii legislației naționale la legislația Uniunii Europene, transpunerea Directivei (UE) 2022/... a Parlamentului European și a Consiliului 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*) având un caracter de prioritate națională în domeniul securității cibernetice.

3. Identificarea opţiunilor

a) Expuneți succint opțiunea „a nu face nimic”, care presupune lipsa de intervenție

Opțiunea respectivă presupune păstrarea status-quo-ului actual, fără o intervenție la nivel normativ, instituțional și organizatoric. În această situație autoritățile responsabile de realizarea politicii de stat în domeniul securității cibernetice urmează să continue activitățile orientate spre asigurarea unui nivel adecvat de securitate a rețelelor și sistemelor informatice, astfel încât prestare serviciilor esențiale să aibă un caracter continuu. Schimbul de informații între diverși furnizori de servicii și actori statali urmează în continuare să aibă loc, în ce privește sectorul privat, pe baze preponderent de voluntariat. Din această perspectivă, în ce privește furnizorii de servicii esențiale din mediul privat, funcția de supraveghere și control al autorităților competente va fi afectată de lipsa unor reglementări legale coerente, care să constituie temeiul juridic primordial de exercitare a unor astfel de competențe.

Deși măsuri susținute au fost întreprinse pentru îmbunătățirea gestionarii riscurilor și incidentelor cibernetice în sectorul public, totuși având în vedere interconexiunile TIC din domeniul public cu cel privat și caracterul intersectorial și chiar transfrontalier al amenințărilor și incidentelor de securitate cibernetică, o creștere a nivelului de protecție cibernetică la nivel național este un obiectiv greu de realizat dacă nu chiar imposibil fără perfecționarea mecanismelor de interacțiune, de responsabilizare, de schimb de informații obligatoriu și, în ultimă instanță de supraveghere și control al acestora.

De asemenea, păstrarea situației actuale va influența credibilitatea țării pe plan internațional, în mod deosebit din punctul de vedere operațional ce ține de schimbul de informații cu partenerii europeni și internaționali în domeniul securității cibernetice.

b) Expuneți principalele prevederi ale proiectului, cu impact, explicînd cum acestea țintesc cauzele problemei, cu indicarea novațiilor și întregului spectru de soluţii/drepturi/obligaţii ce se doresc să fie aprobate

Aprobarea unei legi cadru care să reglementeze domeniul securității cibernetice are ca obiectiv principal ca prin implementarea cerințelor, măsurilor și mecanismelor legale instituite să se asigure un nivel înalt de securitate cibernetică a rețelelor și sistemelor informatice în Republica Moldova, capabil să asigure protecția intereselor vitale ale persoanelor fizice și juridice, ale societății și ale statului, precum și a intereselor naționale ale Republicii Moldova în spațiul cibernetic.

Proiectul de lege are ca ***obiect de reglementare*** cadrul juridic, organizațional și de cooperare în domeniul securității cibernetice a persoanelor juridice de drept public și a persoanelor juridice de drept privat, stabilește competența acestora în materie de securitate cibernetică, determină cadrul național general de gestionare a crizelor în domeniul securității cibernetice, instituie cerințe, măsuri și mecanisme pentru asigurarea securității rețelelor și sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și stabilește modul de gestionare a incidentelor cibernetice.

Proiectul este structurat în 6 capitole după cum urmează:

În ***capitolul I – Dispoziții generale*** sunt reglementate aspecte ce țin de domeniul de aplicare al legii, principalele noțiuni utilizate și definițiile acestora, aspecte generale privind procesul de identificare a persoanelor juridice asupra cărora prevederile legii urmează să fie aplicate, precum și principiile generale conform cărora subiecții legii urmează să le aplice în procesul de asigurare a securității cibernetice.

Acest capitol de asemenea stabilește principalele criterii în baza cărora autoritatea competentă urmează să identifice persoanele juridice ca furnizori de servicii, criterii ce au la bază regula principală a dimensiunii organizației, dar și criterii specifice precum categoria de servicii prestate (ex. prestatorii de servicii de încredere, furnizorii de rețele și servicii de comunicații electronice accesibile publicului, etc), calitatea prestatorului de servicii (operator al obiectivelor infrastructurii critice), impact pe care l-ar putea avea perturbarea prestării serviciului, dependența serviciului de rețelele și sistemele informatice, importanța și interconexiunile cu alte servicii sau sectoare și subsectoare.

Capitolul II „Cadrul instituțional, cooperarea și coordonarea strategică la nivel național” cuprinde norme juridice ce reglementează problematice generale ale raporturilor juridice instituite în procesul de planificare și coordonare strategică în domeniul securității cibernetice la nivel național, inclusiv competența Guvernului de aprobare a Strategiei naționale de securitate cibernetică, misiunea Consiliului coordonator în domeniul securității informaționale, aspecte funcționale ale Autorității competente în domeniul reglementat de prevederile legii, modul de instituire/desemnare, atribuții specifice funcției de CSIRT național și de punct unic de contact la nivel național. De asemenea capitolul vizat stabilește norma legale primare de reglementare a cadrului național general de gestionare a crizelor în materie de securitate cibernetică, inclusiv responsabilitatea autorității de a aproba Planul național de răspuns la incidentele și crizele de securitate cibernetică, în baza cadrului metodologic aprobat de Guvern în ce privește elaborarea, actualizarea și implementarea prevederilor acestui plan. În același context, în acest capitol sunt propuse reglementări fundamentale ce vizează instituirea, organizarea și funcționarea Registrului de stat al incidentelor cibernetice și a sistemului informațional ce-l formează.

Capitolul III – Obligații privind asigurarea securității cibernetice – cuprinde reglementări privind măsurile obligatorii de securitate ce urmează a fi întreprinse de către persoanele juridice, identificate de autoritatea competentă ca furnizorii de servicii, pentru a asigura un nivel înalt de securitate a rețelelor și sistemelor informatice proprii, responsabilitățile acestora în legătură cu măsurile respective, aspecte procedurale generale și obligațiile concrete în procesul de gestionare a incidentelor cibernetice semnificative, responsabilitățile în relațiile cu persoanele juridice terțe care nu cad sub incidența prevederilor legii.

De asemenea, capitolul cuprinde reglementări generale privind asigurarea de către echipa de răspuns la incidente cibernetice a autoritatea competentă a procesului de gestionare a acțiunilor orientate spre prevenirea și soluționarea a incidentelor, dar și spre prevenirea și atenuarea impactului asupra continuității serviciului sau a securității rețelei și/sau a sistemului informatic cauzat de un incident cibernetic.

De rând cu acestea, acest capitol include și prevederi privind notificarea voluntară, ceea ce dreptul furnizorilor de servicii să notifice autoritatea competentă cu privire la incidente cibernetice, amenințări cibernetice și incidente evitate la limită, iar persoanele juridice de drept public sau de drept privat care nu sunt identificate de autoritatea competentă ca furnizori de servicii – să transmită acesteia notificări cu privire la incidente cibernetice semnificative, amenințările cibernetice și incidentele evitate la limită.

În contextul acestor reglementări, capitolul în speță abordează și problematica schimbului de informații voluntar, prin instituirea contextului juridico-normativ suficient pentru crearea unor comunități și platforme de schimb de informații, între furnizorii de servicii și dintre aceștia și alte persoane juridice care nu intră în domeniul de aplicare al prezentei legi. Astfel subiecții respectivi pot face schimb reciproc de informații relevante în materie de securitate cibernetică, în mod voluntar, inclusiv de informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice. Conform proiectului de act normativ autoritatea competentă trebuie să intermedieze acest schimb de informații prin crearea și gestionarea unor platforme, inclusiv tehnico-tehnologice, și comunități de încredere, iar pentru a asigura protecția informațiilor ce au un caracter potențial sensibil, autoritatea competentă urmează să-și aroge funcția de a facilita semnarea acordurilor de schimb de informații între participanții la astfel de platforme și comunități.

În ***Capitolul IV – Supraveghere și control de stat*** sunt cuprinse normele juridice ce reglementează aspectele privind exercitarea de către autoritatea competentă a funcțiilor de supraveghere și control de stat. Astfel aceste funcții urmează a fi realizate prin monitorizarea continuă a modului în care aceștia realizează obligațiile ce le revin conform prevederilor prezentei legi și a actelor normative de punere în aplicare a acesteia. Atunci când un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluționeze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluționarea incidentului cibernetic utilizând, dacă este necesar, asistență profesionistă terță.

În același context, pentru a contracara o amenințare gravă imediată asupra securității rețelelor și sistemelor informatice sau pentru a elimina o perturbare gravă în cazul unui incident cibernetic sunt stabilite expres condițiile în care autoritatea competentă poate restricționa utilizarea sau accesul la un sistem informatic. În ce privește controlul sunt stabilite reglementările primare minime necesare pentru asigurarea legalității intervenției autorității competente pe această dimensiune.

În ambele cazuri, ale supravegherii controlului de stat, pentru implementarea prevederilor legii conform articolelor corespunzătoare din capitolul respectiv al proiectului de lege, Guvernul urmează să adopte acte normative care să reglementeze mai detaliat modul de aplicare a măsurilor de supraveghere și modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin.

Capitolul V – Răspunderea – abordează generic, în scop de interconexiune cu legislația cadru din domeniul administrativ, contravențional, penal și de altă natură, problematica răspunderii, pe de o parte a autorității competente inclusiv a personalului acesteia, iar pe de altă parte a persoanelor juridic care cad sub incidența prevederilor legii în calitate de furnizori de servicii, inclusiv angajații acestora.

Capitolul VI – Dispoziții finale și tranzitorii – prevede termenul de intrare în vigoare al legii – 1 an din data publicării, precum și termenele concrete și sarcinile stabilite:

Guvernului: de a întreprinde măsurile necesare pentru instituirea/desemnarea autorității competente, reglementarea modului de organizare și funcționare a acesteia și dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege, de a prezenta propuneri

Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege și de aduce în concordanță actele proprii;

Autorității competente: de a identifica furnizorii de servicii, îi va notifica în modul stabilit și îi va include în Lista furnizorilor de servicii, întocmită în condițiile legii și de a aproba actele normative necesare punerii în aplicare a legii;

Autorităților și instituțiilor publice să acorde suportul necesar autorității competente în procesul de identificare a furnizorilor de servicii.

c) Expuneți opțiunile alternative analizate sau explicați motivul de ce acestea nu au fost luate în considerare

În contextul obiectivelor urmărite, mai ales de transpunere în cadrul legislativ național a Directivei NIS2, inclusiv a necesității instituirii sau desemnării unei autorități competente la nivel național și a unei echipe de răspuns la incidentele de securitate cibernetică la nivel național o opțiune alternativă opțiunii de reglementare se prezintă ca fiind inutilă. Or, pentru a acoperi domeniul de aplicare al NIS2 chiar și în măsură limitată presupune instituirea unor norme legale primare care ar reglementa obligațiunile entităților din sectorul privat în contextul gestionării riscurilor și incidentelor cibernetice, precum și a crizelor în domeniul securității cibernetice

Este necesar de evidențiat faptul că intervenție la nivel legislativ: o lege cadru sau modificări la legislația actuală sunt modalități ale uneia și aceleiași opțiuni.

4. Analiza impacturilor opţiunilor

a) Expuneți efectele negative şi pozitive ale stării actuale și evoluția acestora în viitor, care vor sta la baza calculării impacturilor opțiunii recomandate

Lipsa unei intervenții prompte și bine structurate din partea statului ar putea fi tradusă în următoarele efecte sau consecințe nefavorabile:

- Lipsa unui cadrului legislativ menit să reglementeze exact și transparent securitatea cibernetică la nivel național în continuare va crea temei de perturbare și afectare directă și indirectă a societății;
- Lipsa cadrului de cooperare la nivel național și de participare la nivel internațional în domeniul asigurării securității cibernetice va limita atât instituțiile statului, cât și furnizorii de servicii de a face față provocărilor prin prevenirea incidentelor și minimizare a riscurilor în baza experienței altor state;
- Lipsa autorității competente la nivel național și a entității de drept public și privat care deține competențe și responsabilități privind securitatea cibernetică, lipsa punctului unic de contact la nivel național și echipei naționale de intervenție în caz de incidente de securitate cibernetică va limita statul și entitățile în mecanisme transparente și eficiente de asigurare a securității cibernetice;
- Lipsa informației privind stabilirea exacte a entităților (publice și private) care sunt esențiale și importante în contextul unei eventuale perturbări a serviciului furnizat, care ar putea avea un impact asupra siguranței publice, a securității publice sau a sănătății publice sau ar putea genera riscuri sistemice, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier în continuare va duce la limitarea statului în exercitarea atribuțiilor în asigurarea securității cibernetice, iar a entităților în suport din partea statului;

- Lipsa unor cerințe de securitate pentru entitățile esențiale și importante, stabilite la nivel național va duce la diferențe esențiale între entități și drept rezultat la incapacitatea unei colaborări eficiente a acestora în prevenirea incidentelor de securitate cibernetică;
- Lipsa obligațiilor de gestionare și de raportare a riscurilor privind securitatea cibernetică pentru entitățile esențiale și importante, stabilite la nivel național, va duce potențiale perturbări a serviciilor esențiale și importante;
- Consecințe negative asupra rezilienței cibernetice a entităților survenite din cauza lipsei regimul de supraveghere în domeniul securității cibernetice;
- Resursele financiare și umane pe care entitățile (publice și private) le alocă pentru asigurarea securității cibernetice și nivelul de maturitate în abordarea riscurilor de securitate cibernetică variază foarte mult. Acest lucru agravează și mai mult diferențele dintre entități în ceea ce privește reziliența cibernetică;
- Entitățile (publice și private) nu dispun de mecanisme reglementate de schimb sistematic de informații. Acest lucru are consecințe negative, în special asupra eficacității măsurilor de securitate cibernetică și asupra nivelului de cunoaștere comună a situației la nivelul național;
- Diminuarea transferului de know-how în țară, fapt care ar contribui nemijlocit la stagnarea evoluției sectorului de securitate cibernetică;
- Aspecte de ordin social precum: gradul redus al ocupării forței de muncă, migrarea profesioniștilor în căutarea oportunităților de angajare mai avantajoase peste hotare, reconversia profesională;
- Majorarea costurilor Guvernului în atingerea obiectivelor propuse în documentele de planificare strategică.

b[1]) Pentru opțiunea recomandată, identificați impacturile completînd tabelul din anexa la prezentul formular. Descrieți pe larg impacturile sub formă de costuri sau beneficii, inclusiv părțile interesate care ar putea fi afectate pozitiv și negativ de acestea

Beneficii

Impact asupra securității și protecției rețelelor și sistemelor informatice. În cadrul acestei opțiuni, protecția consumatorilor, a sectorului public și a celui privat împotriva incidentelor, amenințărilor și riscurilor de securitate cibernetică ar fi îmbunătățită considerabil. Obligațiile impuse furnizorilor de servicii ar asigura că toate entitățile sunt dotate corespunzător, atât din perspectiva capacităților tehnice și organizaționale, cât și în ceea ce privește pregătirea. Un set minim comun de cerințe ar contribui la crearea unui climat de încredere reciprocă, care este o condiție prealabilă pentru orice cooperare eficientă, în mod special între sectorul public și cel privat. Funcționarea continuă și stabilă și fiabilă a serviciilor esențiale și importante este esențială pentru economia digitală și pentru întreaga societate.

O cooperare sigură și eficientă la nivel național ar permite o prevenire și o reacție coerentă și coordonată la incidentele, riscurile și amenințările semnificative la adresa rețelelor și sistemelor informatice utilizate în procesul prestării serviciilor. Introducerea unor cerințe de gestionare a riscurilor de securitate cibernetică pentru persoanele juridice de drept public și cele de drept privat ar crea un stimulent puternic pentru gestionarea și dimensionarea eficientă a riscurilor de securitate. Obligația de a raporta de către aceștia a incidentelor cibernetice cu impact semnificativ ar spori capacitatea de reacție la incidente și ar promova transparența.

Disponibilitatea datelor și informațiilor-cheie privind securitatea rețelelor și sistemele informatice ar permite, de asemenea, autorităților publice responsabile să efectueze analize specifice și să întocmească statistici și, prin urmare, să utilizeze informații fiabile privind securitatea rețelelor și sistemelor informatice pentru a stabili cele mai adecvate priorități în acest domeniu. Opțiunea de reglementare, prin creșterea nivelului de securitate, ar permite țării noastre să-și crească credibilitatea în ce privește nivelul

de protecție și securitate a rețelelor și sistemelor sale informatice și să beneficieze în consecință de informații pertinente de la partenerii săi internaționali.

Impactul economic. Ca urmare a creșterii nivelului de securitate, problemele de securitate ar fi mai rapid remediate și impactul lor ar fi diminuat. De asemenea, pierderile financiare asociate ar fi reduse. Aceste beneficii ar fi resimțite în mod egal în toate sectiarele relevante ale economiei naționale, deoarece vor fi unificate procedurile pentru toate entitățile care vor intra în domeniul de aplicare al legii, permițând astfel crearea unor condiții de concurență echitabile și sprijinind dezvoltarea economică. Acest lucru ar spori încrederea întreprinderilor și a consumatorilor în lumea digitală și în internet și ar crea astfel noi oportunități pentru întreprinderi și pentru economia digitală. Utilizatorii se vor simți mai în siguranță online, ceea ce va spori încrederea acestora în internet, în beneficiul economiei naționale. În special, promovarea unei abordări de gestionare a riscurilor și a unei culturi a securității ar fi benefică pentru atât pentru sectorul privat cât și pentru cel public. Efectuarea evaluării riscurilor de securitate cibernetică le-ar permite și le-ar stimula să aloce eficient resursele pentru a gestiona aceste riscuri și, prin urmare, ar crește valoarea organizației pentru public.

De asemenea, întrucât întreprinderilor din același sector li s-ar cere să pună în aplicare măsuri de securitate similare, întreprinderile ar vor concura pe picior de egalitate. Organizațiile ar fi mai bine echipate pentru a face față incidentelor și atacurilor, ceea ce ar avea ca rezultat o mai mare disponibilitate, fiabilitate și calitate a serviciilor lor. Acest lucru ar crește nivelul de încredere și de satisfacție al celor care utilizează aceste servicii, ar crește profiturile și ar favoriza dezvoltarea economică. Promovarea unei culturi îmbunătățite a gestionării riscurilor ar stimula, de asemenea, cererea de produse și soluții TIC sigure. Acest lucru ar crea noi oportunități și ar valorifica investițiile în cercetare prin îmbunătățirea perspectivelor de exploatare comercială a acestora.

Impactul social. Un nivel mai ridicat de securitate ar îmbunătăți încrederea on-line a cetățenilor, 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.

Impact asupra competitivității. În general, este de așteptat ca o disponibilitate, o fiabilitate și o calitate sporită a serviciilor oferite în sectoarele critice care se bazează în mare măsură pe rețele și sisteme informatice va fi în beneficiul competitivității economiei naționale în ansamblu. De exemplu, disponibilitatea platforme sigure pentru comerțul electronic și alte servicii bazate pe web ar putea aduce importante beneficii economice și ar permite unei game largi de întreprinderi să aducă noi produse și servicii pe piață.

În cele din urmă, se așteaptă un impact pozitiv și pentru furnizorii de produse și servicii de securitate din domeniul tehnologiei informației și comunicațiilor . În primul rând, se așteaptă o creștere a cererii. În plus, dezvoltarea de măsuri de securitate specifice pentru sectoarele din domeniul de aplicare, combinată cu o abordare uniformă la nivelul național, va permite dezvoltarea de produse inovatoare și realizarea de economii de scară.

Estimarea costurilor.

Implementarea acestei inițiative va implica pe de o parte costuri:

1. pentru bugetul de stat, determinate de necesitatea instituirii/desemnării autorității competente și creării unui CSIRT național sau atribuirii competenței unui astfel de CSIRT către CERT-GOV,

2. pentru furnizorii de servicii din sectorul privat privind necesitatea conformării cerințelor noi stabilite de noul cadru legal în domeniul securității cibernetice.

1. În ce privește costurile privind autoritatea competentă și CSIRT național modelul de cost estimat pentru înființarea acestora este în mare măsură determinat de obiectivele stabilite pentru această organizație, de poziția sa juridică și de grupul de interese.

Cu toate acestea, se poate argumenta că anumite resurse critice pot fi identificate în continuare pentru a asigura alinierea la cerințele care decurg din legislația UE (Directiva NIS2). Finanțarea Autorității competente și a CSIRT ar trebui să acopere investițiile inițiale pentru a pune în funcțiune echipa (CAPEX), precum și costurile operaționale recurente (OPEX) pentru personal, instalații și licențe de software, precum și costurile necesare pentru furnizarea și întreținerea serviciilor.

a) Astfel **realizarea funcției de CSIRT național, inclusiv gestionarea incidentelor: prevenție detecție și răspuns** (cerințele de conformare stabilite de art. 11 alin. (1) din Directiva NIS2) implică anumite elemente critice ale misiunii ce urmează a fi realizată, precum:

Expertiză și resurse suficiente echipa ar trebui să includă experți în securitatea rețelelor, analiza jurnalizării, criminalistică informatică și reverse engineering, precum și în arhitectură de securitate și securitate avansată a informațiilor. De asemenea, este important ca echipa să dispună de resurse proprii de dezvoltare, deoarece natura specifică a activității CSIRT înseamnă că toate instrumentele necesare nu pot fi externalizate, ci unele dintre ele trebuie dezvoltate chiar de către echipă. Succesul în răspunsul la incidente la nivel național necesită, de asemenea, cunoașterea funcționării statului și a serviciilor critice, a gestionării riscurilor și a crizelor și a continuității activității. De asemenea, trebuie asigurate hardware și software necesare, comunicații, o locație securizată și alte lucruri necesare pentru această activitate.

Informații privind amenințările. Culegerea și analiza continuă a informațiilor privind incidentele de securitate, atât la nivel național, cât și internațional, fac posibilă identificarea rapidă a amenințărilor și rezolvarea mai eficientă a incidentelor. Conceptul de incident trebuie definit cu precizie, împreună cu procesul de raportare și analiză a incidentelor. Pe lângă colectarea de informații din surse publice (OSINT), raportarea la nivel național și schimbul de informații, schimbul internațional de informații cu organizații surori din alte țări este foarte de dorit.

Astfel finanțarea minimă a acestor elemente critice este compusă din componentele:

Personal - Un CERT cu servicii complete, care funcționează numai în timpul orelor de birou și care își menține propriile sisteme, necesită un minim de 6-8 angajați cu normă întreagă (FTE), iar pentru o operațiune 7x24 (3 schimburi pe zi), minim 12 FTE. Personalul trebuie să se califice pentru a avea o expertiză tehnică solidă și competențele-cheie ale angajaților CERT/CSIRT (de exemplu, așa cum sunt descrise în orientările ENISA[59]) Este important să se asigure formarea constantă și contemporană a întregului personal. Formarea externă de înaltă calitate pentru personalul CSIRT este, de exemplu, organizată de TRANSITS , CERT/CC , SANS Institute , și FIRST. Resursele financiare minime ar trebui să fie cuprinse între 3 000 și 5 000 EUR pe expert pentru a acoperi costurile de formare anuale. **Acestea ar constitui un minim de 18 000 EUR și un maxim de 60 000 EUR pe an.**

În ce privește salarizarea personalului o estimarea inițială a costurilor de salarizare a personalului CCA depinde în mod direct de statutul juridic al acestui personal. Statutul juridic al personalului este

[59] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

determinat de forma juridică de organizare în care va funcționa autoritate competentă, precum și de locul pe care îl va ocup în structura actuală a administrației publice guvernamentale:

a) instituție publică (prevăzută la articolul 32 din Legea nr. 98/20141 privind administrația publică centrală de specialitate) sau

b) autoritate administrativă centrală sau autoritate administrativă, subordonată unui minister (articolele 14 și 17 din aceeași lege).

În cazul în care noua entitate va fi organizată **sub forma juridică a unei instituții publice**, ceea ce ar fi justificat din perspectiva unei salarizări mai corespunzătoare profilului, dar ar contraveni Legii nr. 98/2014 privind administrația publică centrală de specialitate din punctul de vedere al convergenței prerogativelor exercitate cu forma de organizare juridică la salarizarea personalului acesteia se vor aplica prevederile Hotărârii Guvernului nr. 743/20022 privind salarizarea angajaților din unitățile cu autonomie financiară. În acest caz, salariile angajaților vor varia în funcție de funcția deținută, pe baza salariului minim de 3.500 lei, stabilit prin Hotărârea Guvernului nr. 670/2022 privind stabilirea cuantumului salariului minim pe țară, după cum urmează:

Poziția	**Nivelul de salarizare /lei**	
	min	**max**
Director	Directorul urmează să primească un salariu egal cu trei salarii medii lunare pe autoritate pentru perioada de la începutul anului până la sfârșitul lunii de gestiune și este stabilit în contractul de gestiune încheiat cu directorul instituției publice.	
Director adjunct	35.700	47.600
Șef de subdiviziune	11.900	35.700
Specialist	11.900	26.775

În cazul în care noua entitate va fi organizată sub forma juridică a unei autorități administrative centrale sau a unei autorități administrative, subordonată unui minister, atunci prevederile Legii nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar vor fi aplicabile salariilor personalului acesteia. Tabelul de mai jos cuprinde informații privind salariile de bază aproximative ale angajaților noii entități, fără a lua în considerare variabile precum: sporul lunar pentru gradul profesional; sporul lunar pentru un titlu științific și/sau științific/didactic; sporul lunar pentru un titlu onorific; sporul de performanță; alte sporuri speciale:

poziția	**Nivelul de salarizare /lei**	
	Min.	**Max.**
Director General /Director al autorității administrative centrale (demnitate publică)	16.850	19.100
Director General adjunct/ Deputy Director adjunct al autorității administrative centrale (funcționar public)	15.500	17.550
Director al autorității administrative subordonate ministerului (funcționar public)	18.550	21000

Director adjunct al autorității administrative subordonate ministerului (funcționar public)	15500	19.350
Șef de subdiviziune (funcționar public)	9.700	15000
Poziții de execuție (funcționar public)	5700	9700

Sediu

Există, de asemenea, cerințe speciale de securitate pentru sediile CERT/CSIRT, de exemplu:

- încăperi securizate pentru amplasarea oricăror servere și depozite de date ale CSIRT;

- încăperi securizate și izolate fonic pentru discuțiile privind activitățile și investigațiile CSIRT;

- seif pentru depozitarea datelor și notelor non-electronice;

- Un distrugător și o instalație pentru distrugerea completă a suporturilor (de exemplu, EMP) care nu mai sunt necesare.

- Separarea fizică a personalului CSIRT de alte părți ale organizației, inclusiv controlul accesului.

Volumul investițiilor rămâne un subiect care urmează a fi clarificat având în vedere caracteristicile speciale ale locației unui CSIRT național..

Echipamente IT pentru utilizarea CSIRT/CERT. Lista propusă în continuare este una neexhaustivă:

- mecanisme de comunicare securizate, cum ar fi telefoane, faxuri și e-mailuri securizate;

- sisteme hard, inclusiv computerele de lucru (de exemplu, versiunea întărită Microsoft Enterprise).

- Rețea proprie, separată de rețeaua celorlalte subdiviziuni sau personal care nu e implicat nemijlocit în activitățile CSIRT;

- Facilitate de reinstalare rapidă a sistemelor care au fost în afara zonei securizate sau care au fost utilizate pentru analiza malware;

- Instrumente și infrastructură specifice CSIRT, cum ar fi sistemul de gestionare a cazurilor (sistem de ticketing etc.), baza de date de contacte a membrilor echipei, a mandanților și a altor POC etc.

- Configurarea și întreținerea instrumentelor de securitate

- Dezvoltarea de instrumente de securitate

- Instrumente de detectare a intruziunilor, instrumente de monitorizare a rețelei

- instrumente de interogare a domeniilor și a adreselor IP

- instrumente de evaluare a vulnerabilității

- Instrumente de expertiză criminalistică

- Instrumente de analiză a programelor malware

- Honeypots, etc.

Costurile mai specifice depind de dimensiunea reală a echipei și de funcțiile acesteia. **Costul inițial estimat este de aproximativ 500 000 EUR.**

b) Funcții realizate în contextul cadrului de gestionare a crizelor și f**uncțiile de organizare a coordonării naționale a CIIP, identificarea serviciilor esențiale/critice și a furnizorilor de servicii, stabilirea și menținerea listei entităților esențiale/critice**

Personalul și competențele necesare sunt dictate de necesitate de

- expertiză juridică pentru care e recomandabil să se dispună de cel puțin 3 experți juridici cu normă întreagă care pot participa la elaborarea de regulamente și legislație.

- Expertiză în domeniul protecția infrastructurii informaționale critice, al gestionării riscurilor și al gestionării crizelor – pentru care sunt necesari cel puțin 6 persoane angajate cu normă întreagă care să stabilească și să mențină o cooperare solidă cu părțile interesate, atât în sectorul public, cât și în cel privat.

De asemenea va fi necesară formare și participare la exerciții internaționale. Este important faptul că toți experții au nevoie de formare periodică pentru a-și menține cunoștințele relevante și a-și dezvolta competențele. Se recomandă cu insistență organizarea sau participarea la cel puțin 1 curs de formare la nivel internațional anual. În cadrul cooperării internaționale, ar trebui să se ia în considerare costurile de deplasare a 2-4 experți care permit participarea la un exercițiu anual (cel puțin). De exemplu, participarea la exerciții cu focuri reale organizate de CCDCOE al NATO (exercițiul tehnic Locked Shields) și/sau la exerciții de gestionare a crizelor orgnaizate sub auspiciile ENISA.

În context este necesar de evidențiat că Directiva NISD2 pune accentul pe identificarea entităților critice/esențiale care intră în domeniul de aplicare al acesteia și creează o listă de operatori (entități) care furnizează servicii esențiale (vitale) în statul în cauză. Lista ar trebui să conțină toate serviciile furnizate pe teritoriul unui anumit stat și ar trebui să fie completată prin includerea de noi servicii. Lista de servicii stabilită de fiecare stat membru ar servi ca o contribuție suplimentară la evaluarea practicii de reglementare a fiecărui stat membru în vederea asigurării nivelului general de coerență a procesului de identificare între statele membre.

c) Schimbul de informații

Cooperarea cu comunitatea națională de IT, infrastructura critică și serviciile esențiale.

Este important să înțelegem că funcționarea serviciilor IT de care are nevoie societatea depinde în mare măsură de companiile din sectorul privat. În mod obișnuit, profesioniștii din domeniul IT își dezvoltă propriile comunități spontane sau organizate, de la alianțe profesionale la forumuri online. Este important ca un CSIRT să colaboreze cu aceste comunități și să fie vizibil pentru acestea. Aceasta oferă acces rapid la informațiile necesare privind schimbările de securitate, accelerează schimbul de informații și chiar subliniază disponibilitatea unor expertize sau resurse IT specifice care pot fi utilizate pentru a răspunde la incidente în caz de urgență. Instrumente specifice de schimb de informații sunt necesare pentru a permite notificarea incidentelor și schimbul de informații sensibile (de exemplu, poșta electronică securizată și platformele desemnate pentru schimbul de informații privind amenințările cibernetice).

Comunicare și vizibilitate

Informarea publicului, precum și a instituțiilor partenere cu privire la amenințările la adresa securității trebuie să fie o activitate regulată și trebuie să existe un proces clar în acest sens. Deși

campaniile de informare și comunicarea cu mass-media pot fi realizate și prin intermediul partenerilor, este recomandabil să existe o funcție corespunzătoare în cadrul CSIRT-ului însuși. Un CSIRT ar trebui, de asemenea, să fie vizibil în social media și să interacționeze cât mai mult posibil cu grupul său de interes.

Formatele pentru schimbul de informații pot consta în:

1) Platforme tehnice pentru schimbul de date privind vulnerabilitatea tehnică și amenințările (de exemplu, MISP).

2) formate și evenimente formale și non-formale de creare de rețele pentru părțile interesate.

Pentru realizarea acestor funcții vor fi necesare pentru **relațiile publice- cel puțin 2 persoane** cu normă întreagă care ar trebui să se ocupe de relațiile publice și cu mass-media ale Autorității competente, precum și cel puțin **5 analiști** cu normă întreagă care pot analiza datele privind incidentele și amenințările și pot furniza rapoarte publice și clasificate privind peisajul amenințărilor, analize ale incidentelor etc.

d) Funcția de supraveghere și audit

Autoritatea competentă trebuie să instituie o funcție solidă de supraveghere și audit care să supravegheze și să testeze punerea în aplicare a reglementărilor naționale în materie de securitate cibernetică. Se recomandă, de asemenea, ca autoritatea respectivă să aibă propria echipă independentă de testare a securității (echipa RED). Pentru aceasta autoritatea trebuie să includă în statul său de personal experți în supraveghere - numărul acestora depinde de numărul de subiecți supravegheate. Prin urmare, determinarea resurselor umane necesare necesită o înțelegere a numărului de entități esențiale/importante care intră în domeniul de aplicare a noii legi. De asemenea autoritate va avea nevoie de experți în testare (RED Team)- 3-4 experți tehnici de înaltă calificare cu normă întreagă și cu capacitate de testare a penetrării, etc.

În concluzie pentru realizarea funcțiilor enunțate mai sus autoritatea competentă, în cazul în care va include în competența sa și realizarea funcției de CSIRT național va avea necesarul de **minim 25 de angajați**, fără a include aici conducătorii, personalul de suport (în cazul creării unei entități noi) și personalul dedicat realizării funcției de supraveghere (după cum s-a menționat mai sus numărul acestuia este direct dependent de numărul furnizorilor de servicii). Având în vedere prevederile cadrului normativ național în domeniul salarizării**,** și presupunând că personalul respectiv este divizat în patru subdiviziuni (numărul funcțiile fundamentale ce urmează a fi realizate de autoritatea competentă) **remunerarea anuală a muncii acestui personal ar constitui:**

- în cazul instituției publice: **între 3,6 mil. lei și 8,5 mil lei anual;**
- în cazul unei autorități administrative centrale sau autorități administrative în subordinea unui minister**: între 1,9 mil lei și 3,2 mil. lei anual.**

La aceste cheltuieli de personal urmează a fi adăugate cheltuieli investiționale unice inițiale de circa 10 mil. lei în echipamentul și instrumentariul tehnic al CSIRT.

De asemenea, o estimare a costurilor ce țin de asigurarea cu sediu ce corespunde cerințelor Directivei NIS2 urmează a fi efectuat atunci când Guvernul, în temeiul prevederilor legale propuse în proiect va exercita dreptul său discreționar de a decide înființarea unei noi entități sau atribuirea competențelor unei autorități existente.

În analiza de impact la Directiva NIS1, experții Comisiei Europene au stabilit că „*Pentru cele trei state membre care nu au înființat încă CERT-uri naționale/guvernamentale (Cipru, Irlanda și Polonia), costul estimat al punerii în funcțiune a infrastructurii și serviciilor aferente, pe baza interviurilor realizate cu CERT-uri care sunt deja operaționale, ar fi de* ***aproximativ 2,5 milioane EUR pentru fiecare CERT*****.”.**

În același context, Agenția Europeană pentru Securitate Cibernetică a publicat un ghid[60] privind modul de creare și asigurare a funcționalității unui CSIRT care oferă informații și privind costurile estimative la nivelul țărilor membre, necesare pentru instituirea unui CSIRT național.

b[2]) Pentru opțiunile alternative analizate, identificați impacturile completînd tabelul din anexa la prezentul formular. Descrieți pe larg impacturile sub formă de costuri sau beneficii, inclusiv părțile interesate care ar putea fi afectate pozitiv și negativ de acestea

Nu este cazul.

c) Pentru opțiunile analizate, expuneți cele mai relevante/iminente riscuri care pot duce la eșecul intervenției și/sau schimba substanțial valoarea beneficiilor și costurilor estimate și prezentați presupuneri privind gradul de conformare cu prevederile proiectului a celor vizați în acesta

Există riscul implementării lente a prevederilor legii din motivul domeniului nou de reglementare, drept urmare, unele problemele existente riscând să-și păstreze actualitatea pentru o anumită perioadă de timp.

Un alt risc este insuficiența resurselor umane calificate în corespundere cu nivelul de salarizare existent la moment. Respectiv, sunt necesare acțiuni de asigurare a unei remunerări adecvate.

Alt risc este pericolul dotării insuficiente a Autorității competente pentru exercitarea atribuțiilor ce-i revin. În vederea minimizării riscului respectiv, se consideră oportună abordarea organismelor specializate UE și programelor europene și regionale care pot asigura un suport în crearea, dotarea și instruirea Autorității competente naționale.

d) Dacă este cazul, pentru opțiunea recomandată expuneți costurile de conformare pentru întreprinderi, dacă există impact disproporționat care poate distorsiona concurența și ce impact are opțiunea asupra întreprinderilor mici și mijlocii. Se explică dacă sînt propuse măsuri de diminuare a acestor impacturi

Estimarea costurilor de implementare a legii pentru întreprinderile care vor cădea sub incidența obligațiilor stabilite de lege actualmente este o provocare în condițiile unei lipse acute a datelor statistice primare în domeniu securității cibernetice, precum și lipsei unor evaluări și analize financiare bazate pe astfel de date la nivel național. Totuși anumite orientări pe această dimensiune sunt acordate de Comisia Europeană în procesul de evaluare a costurilor de conformare pentru mediul privat în procesul de pregătire a propunerii de Directivă NIS1: *„Pornind de la costurile totale de conformare pentru sectorul privat, care variază între 360 și 720 de milioane de euro, costul de conformare pentru fiecare întreprindere mică și mijlocie s-ar situa între 2 500 și 5 000 de euro. La efectuarea calculului, s-a presupus că întreprinderile mici și mijlocii reprezintă 20% din cifra de afaceri a întreprinderilor private vizate de regulament și reprezintă 68% din toate întreprinderile afectate, adică puțin peste 28 000 de întreprinderi. Acesta este costul mediu estimat pentru fiecare IMM pentru atingerea nivelului actual de "cel mai bun din clasă" în ceea ce privește protecția NIS. Pe măsură ce tehnologiile evoluează, riscurile, pe de o parte, și măsurile de protecție, pe de altă parte, vor continua să evolueze și ele. Astfel, vor fi necesare investiții continue pentru a ține pasul cu stadiul actual al tehnologiei, dar este foarte dificil, în acest stadiu, să se prevadă care vor fi costurile pe care le implică menținerea pasului cu evoluțiile tehnologice. Cu toate acestea, aceste investiții vor garanta că atât întreprinderile mari și mici, cât și economia europeană vor fi bine poziționate pentru a profita de avantajele pieței globale a securității cibernetice, care, potrivit estimărilor, se va număra printre segmentele cu cea mai rapidă creștere din sectorul tehnologiei*

[60] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

informației (IT) în următorii 3-5 ani; în 2011, piața securității cibernetice valora 63,7 miliarde de dolari și se preconizează că va crește între 80 și 120,1 miliarde de dolari până în 2017."

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

„Pentru a evalua costurile de raportare a incidentelor grave din NIS, a fost extrapolată o estimare a notificărilor care ar trebui efectuate pe parcursul unui an, pe baza datelor existente privind punerea în aplicare a articolului 13a din directiva-cadru privind comunicațiile electronice. Pe această bază, numărul de notificări de incidente NIS preconizate s-ar ridica la aproximativ 1 700 pe an. Presupunând că un angajat ar trebui să aloce 0,5 zile lucrătoare pentru notificare și că notificarea ca atare ar avea costuri neglijabile (de exemplu, ar fi efectuată prin intermediul unui e-mail), costul preconizat pentru fiecare notificare de încălcare ar fi de 125 EUR, ceea ce ar duce la un cost total pentru notificarea încălcărilor pe bază anuală de 212 500 EUR la nivelul UE. În ceea ce privește posibilele investigații care pot fi inițiate de către autoritățile competente din NIS cu privire la respectarea obligațiilor de gestionare a riscurilor și de notificare a incidentelor NIS, nu este posibil în acest stadiu să se estimeze dacă și câte investigații ar putea fi inițiate. Cu toate acestea, se poate presupune în mod rezonabil că între 10 și 20% din notificările de incidente NIS ar putea fi urmate de o investigație, ceea ce corespunde unei valori absolute de 170-340 de investigații preconizate pe an. Ținând cont de costul salarial standard, costul maxim pentru entitatea afectată ar fi de maximum 25 000 EUR pe investigație…"

În plus, Agenția Europeană pentru Securitate Cibernetică a publicat Raportul privind investițiile NIS 2021[61], care acoperă toate cele 27 de state membre ale UE și oferă informații suplimentare cu privire la alocarea bugetelor NIS ale operatorilor de servicii esențiale și a furnizorilor de servicii digitale, impactul economic al incidentelor de securitate cibernetică și organizarea securității cibernetice în cadrul acestor operatori

Concluzie

e) Argumentați selectarea unei opțiunii, în baza atingerii obiectivelor, beneficiilor și costurilor, precum și a asigurării celui mai mic impact negativ asupra celor afectați

Analiza beneficiilor și costurilor opțiunilor, în mod special al celei recomandate, în contextul bunelor practici reflectate în studiile și rapoartele de evaluare ale situației în materie de securitate cibernetică în Republica Moldova putem concluziona că opțiunea recomandată în prezenta analiză de elaborare și adoptare a unei legi cadru privind securitate cibernetică este opțiunea preferabilă, recomandabilă și cea mai plauzibilă în contextul actual național și internațional al Republicii Moldova.

În același context relevăm stringența soluționării problematicii instituționale și organizaționale prin instituirea/ desemnarea unei autorități competente și a unui CSIRT național cu capacități suficiente și necesare pentru a preveni, detecta și răspunde adecvat amenințărilor și incidentelor de securitate cibernetică.

Opțiunea recomandată, prin determinarea clară a domeniului de aplicare al legii, va asigura transparența în aplicarea cerințelor de către furnizorii de servicii, la care se adaugă un cadru transparent de supraveghere și de asigurare a respectării legii.

De asemenea prin intervenția propusă vor fi stabilite precondițiile necesare pentru stabilirea clară a responsabilităților și a răspunderii, precum și a mecanismelor orientate spre o promovare a unei mai

[61] https://www.enisa.europa.eu/publications/nis-investments-2021

mari încrederi atât la nivel de autorități, cât și la nivel de întreprinderi, stimulând schimbul de informații și asigurând o asistența reciprocă bazată pe încredere și diligență.

Este cert că opțiunea recomandată presupune costuri de implementare atât pentru sectorul public cât și pentru cel privat, dar în rezultatul implementării măsurilor și cerințelor propuse în proiectul de lege se va asigura o creștere consecventă a nivelului de reziliență cibernetică a entităților-cheie din Republica Moldova, vor fi generate, bineînțeles pe termen mediu și lung economii de costuri atât pentru sectorul privat, cât și pentru societate.

Opțiunea va genera anumite sarcini administrative suplimentare și costuri de asigurare a conformității pentru autoritățile publice, dar în contextul atingerii unui nivel sporit de securitate cibernetică, ar duce, în cele din urmă, la economii de costuri prin prisma minimizării pierderilor economiei naționale din cauza amenințărilor la adresa securității cibernetice.

Pe termen mediu și lung, atingerea unei creșteri a capacităților în materie de securitate cibernetică la nivel național ar aduce beneficii substanțiale printr-o cooperare la nivel operațional, stimulare și asistență reciprocă și o mai bună interacțiune cu mediul privat.

5. Implementarea şi monitorizarea

a) Descrieți cum va fi organizată implementarea opțiunii recomandate, ce cadru juridic necesită a fi modificat și/sau elaborat și aprobat, ce schimbări instituționale sînt necesare

3. Cadrul juridic ce necesită a fi modificat și/sau elaborat și aprobat

În conformitate cu prevederile art. 20 alin (2) din proiectul actului normativ, Guvernul urmează, în termen de cel mult 6 luni din data publicării Legii privind securitatea cibernetică să asigure elaborarea și să prezinte Parlamentului propuneri de modificare a legilor în vigoare care sunt conexe domeniului reglementat de actul normativ în speță. Astfel, deși la momentul actual este destul de ambițios de a identifica prevederile specifice ale unor legi-cadru ce reglementează alte domenii și care cu certitudine necesită a fi modificate în contextul aducerii în concordanță cu prevederile legii în speță, totuși ar putea fi anticipată necesitatea, cel puțin a examinării, în contextul realizării acestui obiectiv, a următoarelor legi care cuprind reglementări privind securitatea și protecția :

- Legea nr. 1069/2000 cu privire la informatică;
- Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat;
- Legea nr.71/2007 cu privire la registre;
- Legea nr. 241/2007 comunicațiilor electronice;
- Legea nr.133/2011 privind protecția datelor cu caracter personal;
- Legea nr. 124/2022 privind identificarea electronica și serviciile de încredere;

În același context, unei examinări aprofundate urmează a fi supuse legile cadru care reglementează sectoarelor, subsectoarele și tipurile de entități ce prestează servicii în acestea, enumerate în anexele 1 și 2 la Directiva NIS2, în contextul în care Guvernul urmează să aprobe lista acestor sectoare și subsectoare de rând cu tipurile persoanelor juridice. Examinarea acestei categorii de acte normative naționale urmează a fi efectuată în primul rând din perspectiva armonizării acestora cu actele sectoriale relevante ale Uniunii Europene, menționate de altfel în anexele respective ale Directivei NIS2.

În continuare pentru a asigura implementarea prevederilor legale noi, urmează a fi supuse dacă nu unei revizuiri, cel puțin unei examinări aprofundate în scopul confirmării conformității cu prevederile noii legi a următoarelor acte normative Guvernamentale:

- Hotărârea Guvernului nr. 201/2017[62] privind aprobarea cerințelor minime obligatorii de securitate cibernetică;
- Hotărârea Guvernului nr. 482/2020[63] privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental;
- Hotărârea Guvernului nr. 388/2022[64] cu privire la aprobarea Concepției Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică".

În același context, Guvernul urmează să aprobe un set de acte normative de punere în aplicare a noului cadru normativ în domeniul securității cibernetice, prevăzute de proiectul de lege:

o) lista sectoarelor, subsectoarelor și, respectiv, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și/sau subsectoare (art. 2 alin. (5);

p) cadrul metodologic privind identificarea persoanelor juridice de drept publice sau privat ca fiind furnizori de servicii (art. 2 alin. (5);

q) Strategia națională de securitate cibernetică (art.6 alin. (3), având la bază pe de o parte rezultatele și concluziile procesului de analiză a modului de implementare a Strategiei naționale de securitate informațională, aprobată prin Hotărârea Parlamentului nr. 257/2018, și pe de altă parte prevederile articolului 7 al Directivei (UE) 2022/... a Parlamentului European și a Consiliului 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*);

r) modul de organizare și funcționare a entității care va exercita funcțiile autorității competente (art. 7 alin. (1);

s) modul de coordonare de către autoritatea competentă a procesului de divulgare a vulnerabilităților (art. 7 alin. (4) lit. i));

t) cadrul metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidente cibernetice și crize de securitate cibernetică, interacțiunea dintre autoritățile și instituțiile publice cu atribuții în procesul de elaborare și actualizare, precum și interacțiunea acestora cu sectorul privat (art. 8 alin. (4);

u) modul de organizare și funcționare a Registrului de stat al incidentelor cibernetice și a sistemului informațional corespunzător art. 9 alin. (1);

v) asigurarea, prin intermediul organismului național de standardizare și în cooperare cu autoritatea competentă, aprobarea Standardului Moldovenesc în domeniul securității informațiilor, securității cibernetice și protecția confidențialității în baza standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice art. 10 alin. (4);

w) cerințele specifice privind măsurile de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii (art. 10 alin. (4);

x) procedura de notificare a incidentelor cibernetice, inclusiv interacțiunea dintre furnizorul de servicii și autoritatea competentă, modul de stabilire a impactului unui incident cibernetic și formatul informațiilor evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic (art. 11 alin. (8).

y) regulamentul privind condițiile și cerințele în care sunt semnate de către autoritățile și instituțiile publice acordurile de schimb de informații în materie de securitate cibernetică (art. 15 alin. (3);

z) modul de aplicare a măsurilor de supraveghere de către autoritatea competentă (art. 16 alin. (5);

[62] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro

[63] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro

[64] https://www.legis.md/cautare/getResults?doc_id=132011&lang=ro

aa) modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii privind securitatea cibernetică (art. 17 alin. (5).

4. Schimbările instituționale preconizate prin aprobarea proiectului de act normativ

În temeiul art. 7 alin. (1) din proiectul de act normativ Guvernul urmează să desemneze autoritatea competentă la nivel național în domeniul securității cibernetice. De asemenea, potrivit prevederilor art. 20 alin. (2) Guvernul urmează să asigure dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege.

Potrivit proiectului de act normativ Guvernului i se conferă o marjă discreționară în procesul de desemnare a acestei autorități competente fie prin instituirea unei autorități/instituții publice noi fie prin identificarea și atribuirea competenței prevăzute de proiectul de act normativ unei entități publice existente.

În oricare dintre cazurile menționate Guvernul urmează, după aprobarea sau, după caz, revizuirea modului de organizare a entității desemnate ca fiind autoritatea competentă în sensul prevederilor proiectului de lege, să inițieze procesul de ajustare a structurii, efectivului-limită și organigramei entității respective și să asigure aprobarea statelor de personal noi ș a schemei de încadrare corespunzătoare.

b) Indicați clar indicatorii de performanță în baza cărora se va efectua monitorizarea

Monitorizarea modului de implementare a opțiunii recomandate de reglementare printr-o lege cadru a domeniului securității cibernetice, urmează a se efectua în conformitate cu următorii indicatori de performanță:

1) ***În interiorul perioadei tranzitorii:***
   - instituirea și asigurarea funcționalității depline a echipei de răspuns la incidentele de securitate cibernetică la nivel național și, implicit a autorității competente în domeniul securității cibernetice;
   - gradul de corespundere a CSIRT național criteriilor stabilite de art. 11 din Directiva NIS2
   - ponderea numărului actelor normative de implementare a legii aprobate, prevăzute în textul legii;
   - finalizarea procesului de identificare a furnizorilor de servicii de către autoritatea competentă, în conformitate cu procedurile stabilite de lege și de actele normative de punere în aplicare a acesteia, în termenul de 3 luni din data finalizării procesului de constituire și asigurării funcționalității depline a acesteia.
2) ***După finalizarea perioadei tranzitorii:***
   - indicatorii de monitorizare și cei de evaluare ce vor fi stabiliți de Strategia națională de securitate cibernetică și Planul de acțiuni de implementare a acesteia aprobate de Guvern în temeiul prevederilor legii;
   - numărul incidentelor de securitate cibernetică prevenite și soluționate de CSIRT în raport cu perioadele precedente de până la instituire conform prevederilor legii;
   - ponderea furnizorilor de servicii care corespund cerințelor stabilite de măsurile de securitate prevăzute de lege, în numărul total de furnizori de servicii identificați de către autoritatea competentă, estimare ce urmează a fi efectuată de autoritatea competentă în procesul de supraveghere și control al corespunderii acestor furnizori cu cerințele stabilite de lege.

c) Identificați peste cît timp vor fi resimțite impacturile estimate și este necesară evaluarea performanței actului normativ propus. Explicați cum va fi monitorizată şi evaluată opţiunea

Într-o **primă etapă** evaluarea performanței implementării prevederilor proiectului de lege va fi determinată de perioada tranzitorie de circa 18 luni (intrarea în vigoare - 12 luni de la data publicării + 6 luni de la data intrării în vigoare a legii pentru aprobarea de către Guvern a Strategiei naționale de securitate cibernetică) în interiorul căreia urmează a fi aprobat întregul cadrul normativ de punere în aplicare a prevederilor legii, de aducere în concordanță cu prevederile legii a cadrului normativ legal și cel al Guvernului. Astfel, un indicator de performanță inițial ar fi aprobarea de către Guvern, în termenele stabilite de proiectul de act normativ al întregului spectru de acte normative necesare punerii în aplicare a prevederilor noii legi.

De asemenea, în perioada tranzitorie de 6 luni după publicarea legii, Guvernul urmează să instituie (desemneze) autoritatea competentă, dotând-o cu resursele umane, financiare și tehnice corespunzătoare. Nivelul de performanță în acest context urmează a fi evaluat în conformitate cu criteriile stabilite la art. 11 alin. (1) din Directiva NIS2 pentru echipa de răspuns la incidentele de securitate cibernetică instituită la nivel național (CSIRT), și anume:

1) disponibilitate ridicată a canalelor lor de comunicare evitând punctele unice de defecțiune;
2) dispunerea de mai multe mijloace pentru a fi contactate și pentru a contacta alte entități în orice moment;
3) specificarea clară a canalelor de comunicare și difuzarea acestora bazei de utilizatori și a partenerilor de cooperare;
4) localuri și sistemele informatice de suport situate în amplasamente securizate;
5) sistem și mecanisme adecvate de gestionare și procesare a cererilor, în special în vederea facilitării eficace și eficiente a transferurilor;
6) asigurarea confidențialității și credibilității operațiunilor;
7) personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor echipei CSIRT, inclusiv instruit și cu formare continuă permanentă, asigurată în mod corespunzător sarcinilor pe care le realizează, și capabil să-și dezvolte singur capacitățile tehnice;
8) sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor lor.

Într-o etapă ulterioară, care începe cu aprobarea de către Guvern a Strategiei naționale de securitate cibernetică și a planului de acțiuni pentru implementarea acesteia, indicatorii de performanță în baza cărora se va evalua modul și gradul de implementare a inițiativei în speță, inclusiv în vederea evaluării creșterii rezilienței cibernetice și a nivelului de asigurare a securității rețelelor și sistemelor informatice la nivel național, vor constitui indicatorii de monitorizare și evaluare stabiliți în documentul respectiv de politici. Astfel, în conformitate cu indicatorii de monitorizare a activităților și a indicatorilor de evaluare de realizare a obiectivelor stabilite în Strategia și în planul respectiv de acțiuni, urmează a fi măsurat nivelul de atingere a obiectivelor urmărite prin aprobarea proiectului de act normativ în speță.

6. Consultarea

a) Identificați principalele părți (grupuri) interesate în intervenţia propusă

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

1. ***Guvernul și autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice*** (competență exercitată în prezent de Ministerul Economiei, în coordonarea Viceprim-ministrului pentru digitalizare) – din perspectiva, pe de o parte, a necesității instituirii unui mecanism instituțional și organizațional viabil de implementare a politicii de stat în domeniul securității cibernetice, în vederea asigurării rezilienței cibernetice a cercului de subiecți care cad sub incidența actului normativ, iar, pe de altă parte – necesitatea armonizării cadrului normativ național ;

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

b) Explicați succint cum (prin ce metode) s-a asigurat consultarea adecvată a părţilor

După finalizarea elaborării proiectului, analiza de impact, proiectul de act normativ propriu-zis și tabelul de concordanță al proiectului urmează a fi supuse unor consultări preliminare cu viceprim-ministrul pentru digitalizare, Instituția publică Serviciul Tehnologia Informației și Securitate Cibernetică precum și cu subdiviziunea structurală internă a Ministerului Economiei responsabilă de realizarea politicii de stat în domeniul securității cibernetice.

După consultarea opiniilor preliminare și ajustarea corespunzătoare a proiectului de act normativ și documentelor de suport, Analiza de impact, conform rigorilor stabilite de Hotărârea Guvernului nr.23/2019 „Cu privire la aprobarea Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative”, urmează a fi supusă examinării de către:

a) Cancelaria de Stat, având în vedere că proiectul prevede reorganizări şi reforme structurale/instituționale ale sistemului autorităților administrației publice centrale de specialitate;
b) Ministerul Finanțelor, având în vedere faptul că prevederile proiectului de act normativ conține reglementări ce vor avea impact asupra bugetului public național;
c) Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător, având în vedere faptul că proiectul de act normativ conține norme de reglementare a activității de întreprinzător.

După examinarea pachetului de documente de către instituțiile menționate a literele a)-c), și ajustarea eventuală a acestora, proiectul de act normativ urmează a fi prezentat Cancelariei de stat pentru înregistrare în vederea examinării în ședința Secretarilor generali ai ministerelor.

Ulterior, potrivit prevederilor art. 32 din Legea nr. 100/2017 cu privire la actele normative și în conformitate cu procedurile stabilite de Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, proiectul de act normativ și analiza de impact urmează a fi transmise pentru examinare în cadrul Ședinței secretarilor generali de stat, cu scopul înregistrării oficiale a proiectului de către Cancelaria de Stat și, în cazul susținerii, lansării acestuia în avizări și consultări publice oficiale. Proiectul și analiza de impact urmează a fi lansate în consultări publice, publicate pe portalul particip.gov.md, inclusiv consultate suplimentar în cadrul meselor rotunde cu persoanele ce vor fi vizate de proiectul propus, în scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional.

c) Expuneți succint poziţia fiecărei entităţi consultate față de documentul de analiză a impactului și/sau intervenţia propusă (se expune poziția a cel puțin unui exponent din fiecare grup de interese identificat)

Poziția fiecărei entități consulate urmează a fi analizată după consultarea publică a documentului de analiză a impactului și a proiectului de act normativ propus.

Anexă

Tabel pentru identificarea impacturilor

Categorii de impact	**Punctaj atribuit**		
	Opțiunea propusă	*Opțiunea alterativă 1*	*Opțiunea alterativă 2*
Economic			
costurile desfășurării afacerilor	-2		
povara administrativă	-1		
fluxurile comerciale și investiționale	0		
competitivitatea afacerilor	0		
activitatea diferitor categorii de întreprinderi mici și mijlocii			
concurența pe piață	0		
activitatea de inovare și cercetare	+1		
veniturile și cheltuielile publice	-1		
cadrul instituțional al autorităților publice	+2		
alegerea, calitatea și prețurile pentru consumatori	0		
bunăstarea gospodăriilor casnice și a cetățenilor	0		
situația social-economică în anumite regiuni	0		
situația macroeconomică	0		
alte aspecte economice	0		
Social			
gradul de ocupare a forței de muncă	0		
nivelul de salarizare	0		
condițiile și organizarea muncii	0		
sănătatea și securitatea muncii	0		
formarea profesională	0		
inegalitatea și distribuția veniturilor	0		

nivelul veniturilor populației	0		
nivelul sărăciei	0		
accesul la bunuri și servicii de bază, în special pentru persoanele social-vulnerabile	0		
diversitatea culturală și lingvistică	0		
partidele politice și organizațiile civice	0		
sănătatea publică, inclusiv mortalitatea și morbiditatea	0		
modul sănătos de viață al populației	0		
nivelul criminalității și securității publice	+3		
accesul și calitatea serviciilor de protecție socială	+1		
accesul și calitatea serviciilor educaționale	+1		
accesul și calitatea serviciilor medicale	+1		
accesul și calitatea serviciilor publice administrative	+1		
nivelul și calitatea educației populației	+1		
conservarea patrimoniului cultural	0		
accesul populației la resurse culturale și participarea în manifestații culturale	0		
accesul și participarea populației în activități sportive	0		
discriminarea	0		
alte aspecte sociale	0		
De mediu			
clima, inclusiv emisiile gazelor cu efect de seră și celor care afectează stratul de ozon	0		
calitatea aerului			
calitatea și cantitatea apei și resurselor acvatice, inclusiv a apei potabile și de alt gen	0		
biodiversitatea	0		
flora	0		
fauna	0		
peisajele naturale	0		
starea și resursele solului	0		

producerea și reciclarea deșeurilor	0		
utilizarea eficientă a resurselor regenerabile și neregenerabile	0		
consumul și producția durabilă	0		
intensitatea energetică	0		
eficiența și performanța energetică	0		
bunăstarea animalelor	0		
riscuri majore pentru mediu (incendii, explozii, accidente etc.)	0		
utilizarea terenurilor	0		
alte aspecte de mediu	0		
Tabelul se completează cu note de la -3 la +3, în drept cu fiecare categorie de impact, pentru fiecare opțiune analizată, unde variația între -3 și -1 reprezintă impacturi negative (costuri), iar variația între 1 și 3 – impacturi pozitive (beneficii) pentru categoriile de impact analizate. Nota 0 reprezintă lipsa impacturilor. Valoarea acordată corespunde cu intensitatea impactului (1 – minor, 2 – mediu, 3 – major) față de situația din opțiunea „a nu face nimic", în comparație cu situația din alte opțiuni și alte categorii de impact. Impacturile identificate prin acest tabel se descriu pe larg, cu argumentarea punctajului acordat, inclusiv prin date cuantificate, în compartimentul 4 din Formular, lit. b[1]) și, după caz, b[2]), privind analiza impacturilor opțiunilor.			
Anexe			
Proiectul preliminar de act normativ			

TABEL DE CONCORDANȚĂ

a proiectului de Lege privind securitatea cibernetică cu Directiva (UE) 2022/2335 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)*

1	**Titlul actului Uniunii Europene, inclusiv cele mai recente amendamente incluse: Directiva (UE) 2022/2335 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)***
2	**Titlul proiectului de act normativ național: Legea privind securitatea cibernetică**
3	**Gradul general de compatibilitate: Parțial compatibil**

Actul Uniunii Europene	**Proiectul de act normativ național**	**Gradul de compatibilitate**	**Diferențele**	**Observațiile**	**Autoritatea/ persoana responsabilă**
4	**5**	**6**	**7**	**8**	9
Capitolul I. Dispoziții generale **Articolul 1. Obiectul** (1) Prezenta directivă stabilește măsuri ***care vizează obținerea*** unui nivel comun ridicat de securitate cibernetică în Uniune***, cu scopul de a îmbunătăți funcționarea pieței interne***. (2) În acest scop, prezenta directivă stabilește: (a) obligațiile statelor membre de a adopta strategii naționale de securitate cibernetică și de a desemna sau de a înființa autorități competente, autorități de gestionare a crizelor cibernetice, puncte unice de contact în materie de securitate cibernetică (denumite în continuare „puncte unice de contact”) și echipe de intervenție în caz de incidente de securitate informatică (denumite în continuare „echipe CSIRT”); (b) măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare pentru entitățile de tipul celor menționate în ***anexa*** I sau II, precum și pentru entitățile identificate drept entități critice în temeiul Directivei (UE) .../...[35]; (c) ***normele și*** obligațiile privind schimbul de informații în materie de securitate cibernetică***;*** (d) ***obligațiile în materie de supraveghere și de asigurare a respectării legii pentru statele membre.***	**Articolul 1. Obiectul de reglementare al legii** Prezenta lege reglementează cadrul juridic, organizațional și de cooperare în domeniul securității cibernetice, stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică, determină cadrul național general de gestionare a crizelor în domeniul securității cibernetice, instituie cerințe, măsuri și mecanisme pentru asigurarea securității rețelelor și sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și stabilește modul de gestionare a incidentelor cibernetice.	**compatibil**	**-**		Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
Articolul 2. Domeniul de aplicare (1) Prezenta directivă se aplică entităților publice sau private de tipul celor menționate în *anexa* I sau II, *care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE sau care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la alineatul (1) din respectivul articol și care prestează servicii sau își desfășoară activitățile în cadrul Uniunii*. *Articolul 3 alineatul (4) din anexa la recomandarea respectivă nu se aplică în sensul prezentei directive.* (2) Indiferent de dimensiunea lor, prezenta directivă se aplică, de asemenea, entităților de tipul celor menționate în anexa I sau II, în cazul în care: (a) serviciile sunt furnizate de: (i) *furnizorii de* rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului; (ii) prestatorii de servicii de încredere; (iii) registrele de nume de domenii de prim nivel și de furnizorii de servicii de sistem de nume de domenii; (b) entitatea este singurul furnizor *dintr-un stat membru al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice*; (c) *perturbarea* serviciului furnizat de entitate ar putea avea un impact *semnificativ* asupra siguranței publice, a securității publice sau a sănătății publice; (d) *perturbarea* serviciului furnizat de entitate ar putea genera un risc sistemic *semnificativ*, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier; (e) entitatea este critică din cauza importanței sale specifice la nivel național sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente din statul membru;	**Articolul 3. Domeniul de aplicare** (1)Prezenta lege se aplică persoanelor juridice care se califică drept întreprinderi mijlocii sau care depășesc plafoanele pentru întreprinderile mijlocii, potrivit clasificării prevăzute de legislația cu privire la întreprinderile mici și mijlocii, care furnizează servicii în unul sau mai multe dintre sectoarele sau subsectoarele stabilite de către Guvern, instituită conform articolului 7, și care sunt identificate de către autoritatea competentă în conformitate cu prevederile prezentei legi și a actelor normative de punere a acesteia în aplicare. (2)Indiferent de dimensiunea lor, prezenta lege se aplică și persoanelor juridice, de tipul stabilit de Guvern, dacă acestea îndeplinesc cel puțin una dintre următoarele condiții: a) sunt furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului în sensul legislației privind comunicațiile electronice; b) sunt prestatori de servicii de încredere în sensul legislației privind identificarea electronică și serviciile de încredere; c) este Registratorul național al domeniului de nivel superior .md; d) furnizează servicii de înregistrare a numelor de domenii; e) sunt singurul furnizor în Republica Moldova a unui serviciu care este esențial pentru susținerea unor activități societale și economice critice; f) 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 sau ar putea genera un risc sistemic semnificativ, în special pentru sectoarele	**Parțial compatibil**		Adițional prevederile respective urmează a fi transpuse prin aprobarea cadrului normativ de implementare a legii și cel de modificare a altor legi pentru a le aduce în concordanță cu prevederile proiectului de lege	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(f) *entitatea este o entitate a administrației publice:* (i) *la nivel central, astfel cum este definită de un stat membru în conformitate cu dreptul intern;* (ii) *la nivel regional, astfel cum este definită de un stat membru în conformitate cu dreptul intern, care, în urma unei evaluări bazate pe riscuri, furnizează servicii a căror întrerupere ar putea avea un impact semnificativ asupra activităților societale sau economice critice.* (3) Prezenta directivă se aplică entităților identificate ca fiind entități critice în temeiul Directivei (UE).../... [(36)], indiferent de dimensiunea lor. (4) Prezenta directivă se aplică *entităților care furnizează servicii de înregistrare a numelor de domenii, indiferent de dimensiunea lor.* (5) *Statele membre pot prevedea ca prezenta directivă să se aplice:* (a) *entităților administrației publice de la nivel local;* (b) *instituțiilor de învățământ, în special în cazul în care acestea desfășoară activități critice de cercetare.* (6) Prezenta directivă nu aduce atingere *responsabilității* statelor membre *de a proteja securitatea națională și competenței acestora de a proteja alte funcții esențiale ale statului, inclusiv asigurarea integrității teritoriale a statului și menținerea ordinii publice.* (7) *Prezenta directivă nu se aplică entităților administrației publice care își desfășoară activitățile în domeniile securității naționale, siguranței publice, apărării sau aplicării legii, inclusiv prevenirii, investigării, depistării și urmăririi penale a infracțiunilor.* (8) *Statele membre pot exonera anumite entități care desfășoară activități în domeniile securității naționale, siguranței publice, apărării sau aplicării legii, inclusiv în*	în care o astfel de perturbare ar putea avea un impact transfrontalier; g) este critică din cauza importanței sale specifice la nivel național sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente; h) furnizează un serviciu dependent de o rețea și/sau de un sistem informatic și de un obiectiv al infrastructurii critice și este identificată în conformitate cu cadrul normativ național relevant ca fiind operator al unei astfel de infrastructuri. (3)Prevederile prezentei legi se aplică și persoanelor juridice de drept public. (4)Prezenta lege se aplică rețelelor și sistemelor informatice care sunt destinate prelucrării informațiilor atribuite la secretul de stat în măsura în care prevederile acesteia nu contravin prevederilor legislației care reglementează prelucrarea unor astfel de informații. (5)Prezenta lege se aplică rețelelor și sistemelor informatice necesare pentru cooperarea militară internațională și pentru pregătirea pentru apărarea națională în domeniul de competență al Ministerului Apărării în măsura în care prevederile acesteia nu contravin legislației privind apărarea națională. (6)În cazul în care tratatele internaționale la care Republica Moldova este parte stabilesc măsuri de securitate ale rețelelor și sistemelor informatice, prevederile respective se aplică în coroborare cu cerințele prevăzute de prevederile prezentei legi. (7)În cazul în care legile sectoriale specifice care reglementează activitatea unor furnizori de servicii stabilesc implementarea unor măsuri de gestionare a riscurilor sau obligații de notificare a incidentelor semnificative, ale căror efecte sunt cel puțin echivalente cu efectele				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
domeniul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, sau care furnizează servicii exclusiv entităților administrației publice menționate la alineatul (7) de la prezentul articol, de obligațiile prevăzute la articolul 21 sau la articolul 23 în ceea ce privește activitățile sau serviciile respective. În astfel de cazuri, măsurile de supraveghere și de asigurare a respectării legii menționate în capitolul VII nu se aplică în legătură cu aceste activități sau servicii specifice. În cazul în care entitățile desfășoară activități sau prestează servicii exclusiv de tipul celor menționate în prezentul alineat, statele membre pot decide, de asemenea, să exonereze respectivele entități de obligațiile prevăzute la articolele 3 și 27. (9) *Alineatele (7) și (8) nu se aplică în cazul în care o entitate acționează ca prestator de servicii de încredere.*	obligațiilor stabilite de prezenta lege, prevederile legilor respective au caracter special în raport cu prevederile prezentei legi. (8)În cazul în care obligațiile, prevăzute la alineatul (7), stabilite de legile sectoriale specifice, sunt aplicabile unui cerc mai restrâns de persoane juridice decât cel prevăzut de prezenta lege și de actele normative de pune în aplicare a acesteia, prevederile prezentei legi se aplică persoanelor juridice care nu cad sub incidența obligațiilor impuse de legile sectoriale specifice. (9)Prevederile alineatelor (7) și (8) se aplică de către autoritatea competentă pentru fiecare caz în parte în procesul de identificare a furnizorilor de servicii. (10) Prevederile Codului administrativ se aplică procedurilor administrative prevăzute în prezenta lege, în măsura în care nu contravin acestora.				
(10) *Prezenta directivă nu se aplică entităților pe care statele membre le-au exclus din domeniul de aplicare al Regulamentului (UE).../...* [(37)] *(DORA) în conformitate cu articolul 2 alineatul (4) din regulamentul respectiv.* (11) *Obligațiile prevăzute în prezenta directivă nu implică furnizarea de informații a căror divulgare ar contraveni intereselor esențiale ale statelor membre în materie de securitate națională, siguranță publică sau apărare.* (12) Prezenta directivă se aplică fără a aduce atingere *Regulamentului (UE) 2016/679, Directivei 2002/58/CE,* Directivelor 2011/93/UE[(38)] și 2013/40/UE[(39)] ale Parlamentului European și ale Consiliului *și* Directivei .../...[(40)].		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
(13) Fără a aduce atingere articolului 346 din TFUE, informațiile confidențiale în conformitate cu normele Uniunii sau cu cele naționale, precum cele privind secretul		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea**		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
comercial, fac obiectul schimbului de informații cu Comisia și cu alte autorități relevante *în conformitate cu prezenta directivă*, numai dacă acest lucru este necesar pentru aplicarea prezentei directive. Informațiile care fac obiectul schimbului se limitează la informații relevante pentru scopul urmărit și proporționale cu acesta. Schimbul de informații păstrează confidențialitatea respectivelor informații și protejează securitatea și interesele comerciale ale entităților în cauză. (14) *Entitățile, autoritățile competente, punctele unice de contact și echipele CSIRT prelucrează date cu caracter personal în măsura necesară pentru scopurile prezentei directive și în conformitate cu Regulamentul (UE) 2016/679, în special această prelucrare se bazează pe articolul 6 din aceasta.* *Prelucrarea datelor cu caracter personal în temeiul prezentei directive 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 dreptul Uniunii privind protecția datelor și cu dreptul Uniunii privind protejarea confidențialității, în special cu Directiva 2002/58/CE.*			**Republicii Moldova la UE**		
Articolul 3. Entități esențiale și entități importante (1) *În sensul prezentei directive, următoarele entități sunt considerate a fi entități esențiale:* (a) *entitățile de tipul celor menționate în anexa I care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la articolul 2 alineatul (1) din anexa la Recomandarea 2003/361/CE;* (b) *prestatorii de servicii de încredere calificați și registrele de nume de domenii de prim nivel, precum și prestatorii de servicii DNS, indiferent de dimensiunea lor;*	**Articolul 3. Domeniul de aplicare** **(**1) Prezenta lege se aplică persoanelor juridice care se califică drept întreprinderi mijlocii sau care depășesc plafoanele pentru întreprinderile mijlocii, potrivit clasificării prevăzute de legislația cu privire la întreprinderile mici și mijlocii, care furnizează servicii în unul sau mai multe dintre sectoarele sau subsectoarele stabilite de către Guvern, instituită conform articolului 7, și care sunt identificate de către autoritatea competentă în conformitate cu prevederile prezentei legi și a actelor	**Parțial compatibil**		**Adițional prevederile respective urmează a fi transpuse prin aprobarea cadrului normativ de implementare a legii și cel de modificare a altor legi pentru a le aduce în concordanță cu prevederile proiectului de lege. În mod special aici ne referim la cadrul metodologic ce urmează a fi aprobat de Guvern în temeiul art. 4 alin. (3) din proiectul de lege, în ce privește**	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(c) *furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE;* (d) *entitățile administrației publice menționate la articolul 2 alineatul (2) litera (f) punctul (i);* (e) *orice alte entități de tipul celor menționate în anexa I sau II care sunt identificate de un stat membru drept entități esențiale în temeiul articolului 2 alineatul (2) literele (b)-(e);* (f) *entitățile identificate drept entități critice în temeiul Directivei (UE).../...*[41]*, menționate la articolul 2 alineatul (3) din prezenta directivă;* (g) *în cazul în care statul membru prevede acest lucru, entitățile pe care statul membru respectiv le-a identificat înainte de... [data intrării în vigoare a prezentei directive] ca operatori de servicii esențiale în conformitate cu Directiva (UE) 2016/1148 sau cu dreptul intern.* (2) *În sensul prezentei directive, entitățile de tipul celor menționate în anexa I sau II care nu se califică drept entități esențiale în temeiul alineatului (1) de la prezentul articol sunt considerate a fi entități importante. Sunt incluse aici entitățile identificate de statele membre ca fiind entități importante în temeiul articolului 2 alineatul (2) literele (b)-(e).*	normative de punere a acesteia în aplicare. (2) Indiferent de dimensiunea lor, prezenta lege se aplică și persoanelor juridice, de tipul stabilit de Guvern, dacă acestea îndeplinesc cel puțin una dintre următoarele condiții: a) sunt furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului în sensul legislației privind comunicațiile electronice; b) sunt prestatori de servicii de încredere în sensul legislației privind identificarea electronică și serviciile de încredere; c) este Registratorul național al domeniului de nivel superior .md; d) furnizează servicii de înregistrare a numelor de domenii; e) sunt singurul furnizor în Republica Moldova a unui serviciu care este esențial pentru susținerea unor activități societale și economice critice; f) 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 sau ar putea genera un risc sistemic semnificativ, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier; g) este critică din cauza importanței sale specifice la nivel național sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente; h) furnizează un serviciu dependent de o rețea și/sau de un sistem informatic și de un obiectiv al infrastructurii critice și este identificată în conformitate cu cadrul normativ național relevant ca			**identificarea furnizorilor de servicii.**	

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	fiind operator al unei astfel de infrastructuri. (3) Prevederile prezentei legi se aplică și persoanelor juridice de drept public. (4) Prezenta lege se aplică rețelelor și sistemelor informatice care sunt destinate prelucrării informațiilor atribuite la secretul de stat în măsura în care prevederile acesteia nu contravin prevederilor legislației care reglementează prelucrarea unor astfel de informații. (5) Prezenta lege se aplică rețelelor și sistemelor informatice necesare pentru cooperarea militară internațională și pentru pregătirea pentru apărarea națională în domeniul de competență al Ministerului Apărării în măsura în care prevederile acesteia nu contravin legislației privind apărarea națională. (6) În cazul în care tratatele internaționale la care Republica Moldova este parte stabilesc măsuri de securitate ale rețelelor și sistemelor informatice, prevederile respective se aplică în coroborare cu cerințele prevăzute de prevederile prezentei legi. (7) În cazul în care legile sectoriale specifice care reglementează activitatea unor furnizori de servicii stabilesc implementarea unor măsuri de gestionare a riscurilor sau obligații de notificare a incidentelor semnificative, ale căror efecte sunt cel puțin echivalente cu efectele obligațiilor stabilite de prezenta lege, prevederile legilor respective au caracter special în raport cu prevederile prezentei legi. (8) În cazul în care obligațiile, prevăzute la alineatul (7), stabilite de legile sectoriale specifice, sunt aplicabile unui cerc mai restrâns de persoane juridice decât cel prevăzut de prezenta lege și de actele normative de pune în				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	aplicare a acesteia, prevederile prezentei legi se aplică persoanelor juridice care nu cad sub incidența obligațiilor impuse de legile sectoriale specifice. (9) Prevederile alineatelor (7) și (8) se aplică de către autoritatea competentă pentru fiecare caz în parte în procesul de identificare a furnizorilor de servicii. (10) Prevederile Codului administrativ se aplică procedurilor administrative prevăzute în prezenta lege, în măsura în care nu contravin acestora.				
(3) *Până la ... [27 de luni de la data intrării în vigoare a prezentei directive], statele membre întocmesc o listă a entităților esențiale și a entităților importante, precum și a entităților care furnizează servicii de înregistrare a numelor de domenii. Statele membre revizuiesc lista în mod regulat, cel puțin o dată la doi ani, și o actualizează atunci când este cazul.*	**Articolul 4. Identificarea furnizorilor de servicii** (1) Autoritatea competentă întocmește și ține o listă a furnizorilor de servicii, care cuprinde cel puțin tipul, categoria furnizorului de servicii și sectorul și subsectorul în care prestează serviciul respectiv și asigură ori de câte ori este necesar, însă nu mai rar decât o dată la doi ani, actualizarea acesteia.	**Compatibil**		Adițional pentru implementarea acestor norme legale Guvernul urmează să adopte cadrul metodologic privind identificarea furnizorilor de servicii și lista sectoarelor, subsectoarelor, a categoriilor și tipurilor de persoane juridice d drept public sau privat care cad sub incidența prevederilor legii.	Viceprim-ministru pentru digitalizare Ministerul Economiei
(4) *În scopul întocmirii listei menționate la alineatul (3), statele membre solicită entităților menționate la respectivul alineat să prezinte autorităților competente cel puțin următoarele informații:* (a) *denumirea entității;* (b) *adresa și datele de contact actualizate, inclusiv adresele de e-mail, gama de IP-uri și numerele de telefon;* (c) *dacă este cazul, sectorul și subsectorul relevante menționate în anexa I sau II; precum și* (d) *după caz, o listă a statelor membre în care furnizează servicii care intră în domeniul de aplicare al prezentei directive.* *Entitățile menționate la alineatul (3) notifică fără întârziere orice modificări ale detaliilor transmise în temeiul primului paragraf de la prezentul alineat și, în orice caz,*	**Articolul 4 din proiectul de lege** (2) În scopul întocmirii listei menționate la alineatul (1), persoanele juridice, la solicitarea autorității competente, sunt obligați să prezinte următoarele date: denumirea persoanei juridice, adresa și datele de contact actualizate, inclusiv adresele de e-mail, gama de IP-uri și numerele de telefon, sectorul și subsectorul relevant în care își desfășoară activitatea.	**Compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
în termen de două săptămâni de la data modificării.					
Comisia, cu sprijinul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), oferă, fără întârzieri nejustificate, orientări și modele privind obligațiile prevăzute în prezentul alineat. *Statele membre pot institui mecanisme naționale prin care entitățile să se înregistreze.* (5) *Până la ... [27 de luni de la data intrării în vigoare a prezentei directive] și, ulterior, o dată la doi ani, autoritățile competente notifică:* (a) *Comisiei și Grupului de cooperare numărul entităților esențiale și al entităților importante enumerate în temeiul alineatului (3) pentru fiecare sector și subsector menționat în anexa I sau II; și* (b) *Comisiei informațiile relevante privind numărul de entități esențiale și de entități importante identificate în temeiul articolului 2 alineatul (2) literele (b)-(e), sectorul și subsectorul menționate în anexa I sau II din care fac parte, tipul de servicii pe care le furnizează și dispoziția, dintre cele prevăzute la articolul 2 alineatul (2) literele (b)-(e), în temeiul căreia au fost identificate.* (6) *Până la... [27 de luni de la data intrării în vigoare a prezentei directive] și la cererea Comisiei, statele membre pot notifica Comisiei denumirile entităților esențiale și ale entităților importante menționate la alineatul (5) litera (b).*		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
Articolul 4. Acte juridice sectoriale ale Uniunii (1) *În cazul în care actele juridice sectoriale ale Uniunii impun entităților esențiale sau entităților importante să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să notifice incidentele semnificative, iar cerințele respective au un efect cel puțin echivalent cu efectul obligațiilor prevăzute în prezenta directivă, dispozițiile relevante ale prezentei directive, inclusiv dispozițiile privind*	**Articolul 3 din proiectul de lege** (7) În cazul în care legile sectoriale specifice care reglementează activitatea unor furnizori de servicii stabilesc implementarea unor măsuri de gestionare a riscurilor sau obligații de notificare a incidentelor semnificative, ale căror efecte sunt cel puțin echivalente cu efectele obligațiilor stabilite de prezenta lege, prevederile legilor respective au caracter special în raport cu prevederile prezentei legi.	**Compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
supravegherea și asigurarea respectării legii prevăzute în capitolul VII, nu se aplică acestor entități. În cazul în care actele juridice sectoriale ale Uniunii nu acoperă toate entitățile dintr-un anumit sector care intră în domeniul de aplicare al prezentei directive, dispozițiile relevante ale prezentei directive se aplică în continuare entităților care nu fac obiectul respectivelor acte juridice sectoriale ale Uniunii. (2) *Cerințele menționate la alineatul (1) din prezentul articol sunt considerate echivalente în privința efectului cu obligațiile prevăzute în prezenta directivă, în cazul în care:* (a) *măsurile de gestionare a riscurilor în materie de securitate cibernetică sunt cel puțin echivalente în privința efectului cu cele prevăzute la articolul 21 alineatele (1) și (2); sau* (b) *actul juridic sectorial al Uniunii prevede accesul imediat, după caz automat și direct, la notificările incidentelor pentru echipele CSIRT, autoritățile competente sau punctele unice de contact în temeiul prezentei directive și dacă cerințele de notificare a incidentelor semnificative au un efect cel puțin echivalent cu cele prevăzute la articolul 23 alineatele (1)-(6) din prezenta directivă.*	(8) În cazul în care obligațiile, prevăzute la alineatul (7), stabilite de legile sectoriale specifice, sunt aplicabile unui cerc mai restrâns de persoane juridice decât cel prevăzut de prezenta lege și de actele normative de pune în aplicare a acesteia, prevederile prezentei legi se aplică persoanelor juridice care nu cad sub incidența obligațiilor impuse de legile sectoriale specifice. (9) Prevederile alineatelor (7) și (8) se aplică de către autoritatea competentă pentru fiecare caz în parte în procesul de identificare a furnizorilor de servicii.				
(3) *Comisia, până la... [șase luni de la data intrării în vigoare a prezentei directive], oferă orientări care clarifică aplicarea alineatelor (1) și (2). Comisia revizuiește orientările respective în mod periodic. La elaborarea acestor orientări, Comisia ia în considerare observațiile Grupului de cooperare și ale ENISA.*		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
Articolul 5. Armonizarea minimă *Prezenta directivă nu împiedică* statele membre să *adopte sau să mențină* dispoziții care asigură un nivel mai ridicat de securitate cibernetică*, cu condiția ca aceste dispoziții să*		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii.					
Articolul 6. Definiții În sensul prezentei directive, se aplică următoarele definiții: 1. **„rețea și sistem informatic”** înseamnă: (a) o rețea de comunicații electronice, astfel cum este definită la articolul 2 punctul 1 din Directiva (UE) 2018/1972; (b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale; sau (c) datele digitale stocate, prelucrate, recuperate sau transmise de elemente reglementate în temeiul literelor (a) și (b) în vederea funcționării, utilizării, protejării și întreținerii lor;	**Articolul 2. Principalele noțiuni și definițiile lor** ***10) rețea și sistem informatic*:** a) rețea de comunicații electronice în sensul prevederilor Legii comunicațiilor electronice nr. 241/2007 sau b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale sau c) date digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la lit. a) și b) în vederea funcționării, utilizării, protejării și întreținerii lor.	**Compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
2. **„securitatea rețelelor și a sistemelor informatice”** înseamnă capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, *oricărui eveniment* care *poate* compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;	***13) securitatea rețelelor și a sistemelor informatice*** – capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora	Compatibil			Viceprim-ministru pentru digitalizare Ministerul Economiei
3. **„securitate cibernetică”** înseamnă securitate cibernetică astfel cum este definită la articolul 2 alineatul (1) din Regulamentul (UE) 2019/881;	***12) securitate cibernetică*** - activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice;	Compatibil			Viceprim-ministru pentru digitalizare Ministerul Economiei
4. **„strategie națională de securitate cibernetică”** înseamnă un cadru coerent al unui stat membru care prevede obiective și priorități strategice *în domeniul securității cibernetice și guvernanța necesară pentru realizarea acestora* în statul membru respectiv;	**Articolul 6.** ***Planificarea și coordonarea strategică în domeniul securității cibernetice la nivel național din proiectul de lege*** (3) Strategia națională de securitate cibernetică este un document de politici	**Compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	care definește obiectivele strategice și măsurile de politică și de reglementare care au ca scop atingerea și menținerea unui nivel ridicat de securitate cibernetică. Strategia națională de securitate cibernetică se aprobă de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.				
5. ***„incident evitat la limită”*** *înseamnă un eveniment care ar fi putut compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora, dar care a fost împiedicat cu succes să se materializeze sau care nu s-a materializat;*	***Articolul 2 din proiectul de lege:*** ***6) incident cibernetic evitat la limită*** – un eveniment care ar fi putut compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora, dar care a fost împiedicat cu succes să se materializeze sau care nu s-a materializat;	**Compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
6. **„incident”** înseamnă un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora;	***5) incident cibernetic*** **-** orice eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor conexe oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora;	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
7. ***„incident*** **de securitate cibernetică *de mare amploare”*** *înseamnă 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;*		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
8. **„gestionarea incidentului”** înseamnă toate acțiunile și procedurile care vizează *prevenirea,* detectarea, analizarea și limitarea unui incident, sau vizează răspunsul la acesta *și redresarea în urma incidentului*;	**4) gestionarea incidentului cibernetic** – toate acțiunile și procedurile care vizează *prevenirea,* detectarea, analizarea, limitarea și izolarea unui incident cibernetic, sau vizează	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	răspunsul la acesta *și redresarea în urma acestui incident;*				
9. ***„risc”*** *înseamnă potențialul de pierderi sau de perturbări cauzate de un incident și trebuie exprimat ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului;*	***11) risc –*** potențialul de pierderi sau de perturbări cauzate de un incident și trebuie exprimat ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului;	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
10. ***„amenințare cibernetică”*** înseamnă o amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;	***1) amenințare cibernetică*** – orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora;	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
11. ***„amenințare cibernetică semnificativă”*** *înseamnă o amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor sale tehnice, că are potențialul de a afecta grav rețeaua și sistemele informatice ale unei entități sau utilizatorii serviciilor furnizate de entitate, cauzând prejudicii materiale sau morale considerabile;*	**2) amenințare cibernetică semnificativă -** amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor sale tehnice, că are potențialul de a afecta grav rețeaua și sistemele informatice ale unei persoane juridice care prestează servicii sau utilizatorii serviciilor furnizate de aceasta, cauzând prejudicii materiale sau morale considerabile;	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
12. ***„produs TIC”*** *înseamnă un produs astfel cum este definit la articolul 2 punctul 12 din Regulamentul (UE) 2019/881;*	***9) produs TIC*** **-** un element sau un grup de elemente al unei rețele sau al unui sistem informatic;	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
13. ***„serviciu TIC”*** *înseamnă un serviciu TIC astfel cum este definit la articolul 2 punctul 13 din Regulamentul (UE) 2019/881;*	***14) serviciu TIC*** **-** un serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice;	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
14. ***„proces TIC”*** *înseamnă un proces TIC astfel cum este definit la articolul 2 punctul 14 din Regulamentul (UE) 2019/881;*	***9) proces TIC*** **–** un set de activități desfășurate pentru a concepe, a dezvolta, a furniza sau a întreține un produs TIC sau un serviciu TIC	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
15. **„vulnerabilitate”** înseamnă un punct slab, o susceptibilitate sau o deficiență a *unor produse TIC sau a unor servicii TIC* care poate fi exploatată de o amenințare cibernetică;	***18) vulnerabilitate*** **-** un punct slab, o susceptibilitate sau o deficiență a unor produse TIC sau a unor servicii TIC care poate fi exploatată de o amenințare cibernetică;	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
16. **„standard”** înseamnă un standard astfel cum este definit la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[(42)];	***17) standard*** – un standard în sensul Legii nr. 20/2016 cu privire la standardizarea națională	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
17. **„specificație tehnică”** înseamnă o specificație tehnică astfel cum este definită la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012;	**16) specificație tehnică –** o specificație tehnică în sensul Legii nr. nr. 20/2016 cu privire la standardizarea națională	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei
18. **„internet exchange point”** înseamnă o facilitate a rețelei 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 a traficului de internet dintre orice pereche de sisteme autonome participante și nici nu modifică sau interacționează într-un alt mod cu acest trafic;		**incompatibil**		Această noțiune ar putea fi transpusă în procesul de elaborare a cadrului normativ metodologic, în temeiul art. 4 alin. (3) din proiect de lege, dacă va i necesară în scopurile reglementării procesului de identificare a furnizorilor de servicii.	Viceprim-ministru pentru digitalizare Ministerul Economiei
19. **„sistem de nume de domenii DNS”** sau „DNS” înseamnă 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*;	**Art.3 alineatul (5) din Legea comunicațiilor electronice nr. 241/2004** (5) Registratorul național al domeniului de nivel superior .md este desemnat de către Guvern și exercită următoarele atribuții: a) ține Registrul numelor din domeniul de nivel superior .md, asigură actualizarea acestuia și accesul on-line; b) atribuie, înregistrează, reînregistrează, retrage numele din domeniul de nivel	**Parțial compatibil**			Ministerul Infrastructurii și Dezvoltării Regionale (MIDR) Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	superior .md, modifică datele de înregistrare necesare funcționalității acestora; c) deține controlul asupra punctelor de indexare a domeniului de nivel superior .md în rețeaua globală internet; d) desemnează entitățile cu funcție de dealer și supraveghează activitatea acestora; e) stabilește tariful standard și grila de tarife pentru entitățile cu funcție de dealer pentru înregistrarea numelor în cadrul domeniului de nivel superior.md. **Hotărârea ANRCETI nr. 42/2020** privind aprobarea Regulamentului cu privire la gestionarea domeniului de nivel superior .md				Informației (ANRCETI) Viceprim-ministru pentru digitalizare
20. **„furnizor de servicii DNS”** înseamnă o entitate 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;*	**Art.3 alineatul (5) din Legea comunicațiilor electronice nr. 241/2004** (5) Registratorul național al domeniului de nivel superior .md este desemnat de către Guvern și exercită următoarele atribuții: a) ține Registrul numelor din domeniul de nivel superior .md, asigură actualizarea acestuia și accesul on-line; b) atribuie, înregistrează, reînregistrează, retrage numele din domeniul de nivel superior .md, modifică datele de înregistrare necesare funcționalității acestora; c) deține controlul asupra punctelor de indexare a domeniului de nivel superior .md în rețeaua globală internet; d) desemnează entitățile cu funcție de dealer și supraveghează activitatea acestora; e) stabilește tariful standard și grila de tarife pentru entitățile cu funcție de dealer pentru înregistrarea numelor în cadrul domeniului de nivel superior.md.	**Parțial compatibil**			MIDR ANRCETI Viceprm-ministru pentru digitalizare

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	Hotărârea ANRCETI nr. 42/2020 privind aprobarea Regulamentului cu privire la gestionarea domeniului de nivel superior .md				
21. **„registru de nume de domenii de prim nivel”** sau **„registru de nume TLD”** (*top–level domain* – TLD) înseamnă o entitate 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 entitatea însăși sau este externalizată, dar excluzând situațiile în care numele TLD sunt utilizate de un registru numai pentru uzul propriu*;	**Art.3 alineatul (5) din Legea comunicațiilor electronice nr. 241/2004** (5) Registratorul național al domeniului de nivel superior .md este desemnat de către Guvern și exercită următoarele atribuții: a) ține Registrul numelor din domeniul de nivel superior .md, asigură actualizarea acestuia și accesul on-line; b) atribuie, înregistrează, reînregistrează, retrage numele din domeniul de nivel superior .md, modifică datele de înregistrare necesare funcționalității acestora; c) deține controlul asupra punctelor de indexare a domeniului de nivel superior .md în rețeaua globală internet; d) desemnează entitățile cu funcţie de dealer și supraveghează activitatea acestora; e) stabilește tariful standard și grila de tarife pentru entitățile cu funcție de dealer pentru înregistrarea numelor în cadrul domeniului de nivel superior.md. **Hotărârea ANRCETI nr. 42/2020** privind aprobarea Regulamentului cu privire la gestionarea domeniului de nivel superior .md	**compatibil**			MIDR ANRCETI; Viceprim-ministru pentru digitalizare
22. ***„entitate care furnizează servicii de înregistrare a numelor de domenii”*** *înseamnă un 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;*	**Punctul 4 din Regulamentul cu privire la gestionarea domeniului de nivel superior .md, aprobat prin Hotărârea ANRCETI nr. 42/2020** **Registrator național al domeniului de nivel superior .md –** entitate cu atribuții de organizare, administrare și gestionare a domeniului de nivel superior .md.	**compatibil**			Ministerul (ANRCETI); Viceprim-ministru pentru digitalizare

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	Dealer **-** persoană fizică sau juridică eligibilă în condițiile prezentului Regulament de a înregistra și administra nume de subdomenii din domeniul de nivel superior .md, în baza unui contract de parteneriat încheiat cu Registratorul național;				
23. **„serviciu digital”** înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului[(43)];		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
24. ***„serviciu de încredere”*** *înseamnă un serviciu de încredere astfel cum este definit la articolul 3 punctul 16 din Regulamentul (UE) nr. 910/2014;* ***articolul 3 punctul 16 din Regulamentul (UE) nr. 910/2014*** *„serviciu de încredere”* înseamnă un serviciu electronic prestat în mod obișnuit în schimbul unei remunerații, care constă în: (a) crearea, verificarea și validarea semnăturilor electronice, a sigiliilor electronice sau a mărcilor temporale electronice, a serviciilor de distribuție electronică înregistrată și a certificatelor aferente serviciilor respective; sau (b) crearea, verificarea și validarea certificatelor pentru autentificarea unui site internet; sau (c) păstrarea semnăturilor electronice, a sigiliilor sau a certificatelor aferente serviciilor respective;	**Art. 2 din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere:** ***serviciu de încredere*** – serviciu electronic, prestat, de regulă, în schimbul unei remunerații, care constă în una sau mai multe din următoarele activități: a) crearea, verificarea și validarea semnăturilor electronice, a sigiliilor electronice sau a mărcilor temporale electronice, a serviciilor de distribuție electronică înregistrată și a certificatelor aferente serviciilor respective; b) crearea, verificarea și validarea certificatelor pentru autentificarea unei pagini web; c) păstrarea semnăturilor electronice, a sigiliilor electronice sau a certificatelor aferente serviciilor respective;	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei Serviciul de Informații și Securitate
25. ***„prestator de servicii de încredere”*** *înseamnă un prestator de servicii de încredere astfel cum este definit la articolul 3 punctul 19 din Regulamentul (UE) nr. 910/2014;* ***articolul 3 punctul 19 din Regulamentul (UE) nr. 910/2014*** *„prestator de servicii de încredere”* înseamnă o persoană fizică sau juridică care prestează unul sau mai multe servicii de	**Art. 2 din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere:** ***prestator de servicii de încredere*** – întreprinzător individual sau persoană juridică care prestează unul sau mai multe servicii de încredere ca prestator de servicii de încredere calificat sau prestator de servicii de încredere necalificat;	**compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei Serviciul de Informații și Securitate

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
încredere ca prestator de servicii de încredere calificat sau necalificat;					
26. ***„serviciu de încredere calificat”*** *înseamnă un serviciu de încredere calificat astfel cum este definit la articolul 3 punctul 17 din Regulamentul (UE) nr. 910/2014;* ***articolul 3 punctul 17 din Regulamentul (UE) nr. 910/2014:*** *„serviciu de încredere calificat”* înseamnă un serviciu de încredere care îndeplinește cerințele aplicabile prevăzute de prezentul regulament;	**Art. 2 din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere:** ***serviciu de încredere calificat*** – serviciu de încredere care întrunește cerințele aplicabile, prevăzute de prezenta lege;	**Compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei Serviciul de Informații și Securitate
27. ***„prestator de servicii de încredere calificat”*** *înseamnă un prestator de servicii de încredere calificat astfel cum este definit la articolul 3 punctul 20 din Regulamentul (UE) nr. 910/2014;* ***articolul 3 punctul 20 din Regulamentul (UE) nr. 910/2014:*** *„prestator de servicii de încredere calificat”* înseamnă un prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate și căruia i se acordă statutul de calificat de către organismul de supraveghere;	**Art. 2 din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere:** ***prestator de servicii de încredere calificat*** – prestator de servicii de încredere care prestează unul sau mai multe servicii de încredere calificate și care deține statut de prestator de servicii de încredere calificat, acordat de către organul de supraveghere și control;	**Compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei Serviciul de Informații și Securitate
28. **„piață online”** înseamnă o piață online astfel cum este definită la articolul 2 litera (n) din Directiva 2005/29/CE a Parlamentului European și a Consiliului[(44)];		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
29. **„motor de căutare online”** înseamnă un motor de căutare online astfel cum este definit la articolul 2 punctul 5 din Regulamentul (UE) 2019/1150 al Parlamentului European și al Consiliului[(45)];		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
30. **„serviciu de cloud computing”** înseamnă un 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 atunci când aceste resurse sunt* distribuite *în mai multe locații*;		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
31. **„serviciu de centre de date”** înseamnă un 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 infrastructurile de distribuție a energiei electrice și de control al mediului;		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
32. **„rețea de furnizare de conținut”** înseamnă o rețea de servere distribuite geografic cu scopul de a asigura o disponibilitate ridicată, accesibilitate sau furnizare rapidă de conținut digital și servicii către utilizatorii de internet în numele furnizorilor de conținut și de servicii;		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
33. **„platformă de servicii de socializare în rețea”** înseamnă o platformă care le permite utilizatorilor finali să se conecteze, să partajeze, să descopere și să comunice între ei prin intermediul mai multor dispozitive, în special prin chat, postări, materiale video și recomandări;		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
34. **„reprezentant”** înseamnă o persoană fizică sau juridică stabilită în Uniune 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 Uniune, căreia o autoritate națională competentă sau o echipă CSIRT i se poate adresa în locul entității în cauză în ceea ce privește obligațiile entității respective în temeiul prezentei directive;		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
35. **„entitate a administrației publice”** înseamnă o entitate *recunoscută ca atare într-un* stat membru *în conformitate cu dreptul intern, cu excepția sistemului judiciar, a parlamentelor și a băncilor centrale,* care îndeplinește următoarele criterii: (a) a fost înființată în scopul de a răspunde unor necesități de interes general și nu are un caracter industrial sau comercial; (b) are personalitate juridică *sau este abilitată prin lege să acționeze în numele unei alte entități cu personalitate juridică*; (c) este finanțată, în cea mai mare parte, de stat, de autoritățile regionale sau de alte organisme de drept public, este supusă controlului de gestiune din partea autorităților sau a organismelor respective sau are un consiliu de administrație, de conducere sau de supraveghere ai cărui membri sunt desemnați în proporție de peste 50 % de stat, de autoritățile regionale sau de alte organisme de drept public; (d) are competența de a adresa persoanelor fizice sau juridice decizii administrative sau de reglementare care le afectează drepturile în ceea ce privește circulația transfrontalieră a persoanelor, mărfurilor, serviciilor sau capitalurilor;	noțiunea este definită în Codul administrativ **Articolul 7. Autoritățile publice** Autoritate publică se consideră orice structură organizatorică sau organ instituită/instituit prin lege sau printr-un alt act normativ, care acționează în regim de putere publică în scopul realizării unui interes public. Art. 307 din Codul civil **Articolul 307.** Instituția publică (1) Instituția publică este persoană juridică de drept public care se constituie în baza unui act emis de autoritatea publică și care este finanțată, integral sau parțial, de la bugetul acesteia din urmă. (2) Fondatorul răspunde pentru obligațiile instituției publice în măsura în care patrimoniul acesteia nu este suficient pentru stingerea lor. (3) Instituția publică este în drept să desfășoare activitatea neinterzisă de lege, care ține de realizarea scopurilor prevăzute de lege sau statut. (4) Activitatea care, conform legii, este supusă licențierii poate fi practicată de instituția publică doar după obținerea licenței, dacă legea nu prevede altfel. (5) Pentru desfășurarea activității de întreprinzător care nu rezultă nemijlocit din scopul prevăzut în statut, instituția publică poate constitui, singură sau împreună cu alte persoane juridice de drept public, societăți cu răspundere limitată sau societăți pe acțiuni. Instituția publică poate constitui societăți cu răspundere limitată sau societăți pe acțiuni împreună cu persoane juridice de drept privat în condițiile legislației privind parteneriatul public-privat. **Art. 32 din Legea nr. 98/2012 privind administrația publică centrală de specialitate:**	**Compatibil**			Viceprim-ministru pentru digitalizare

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	Articolul 32. Instituțiile publice în care ministerul sau altă autoritate administrativă centrală are calitatea de fondator (1) Pentru realizarea unor funcții de administrare, sociale, culturale, de învățământ și a altor funcții de interes public, de care este responsabil ministerul sau altă autoritate administrativă centrală, cu excepția celor de reglementare normativ-juridică, supraveghere și control de stat, precum și a altor funcții care implică exercitarea prerogativelor de putere publică, în sfera de competență a acestora pot fi constituite instituții publice.				
36. ***„rețea publică de comunicații electronice”*** *înseamnă o rețea publică de comunicații electronice astfel cum este definită la articolul 2 punctul 8 din Directiva (UE) 2018/1972;* ***articolul 2 punctul 8 din Directiva (UE) 2018/1972:*** ***„rețea publică de comunicații electronice”*** înseamnă o rețea de comunicații electronice utilizată în întregime sau în principal pentru furnizarea unor servicii de comunicații electronice destinate publicului, care permite transferul de informații între punctele terminale ale rețelei;	**Articolul 2 din Legea nr. 241 comunicațiilor electronice:** rețea de comunicaţii electronice – sisteme de transmisie şi, după caz, echipamente de comutare sau rutare, precum şi alte resurse care permit transmiterea semnalelor prin suport fizic, electromagnetic sau prin orice alte mijloace, incluzînd reţele de comunicaţii prin satelit, reţele fixe (cu comutare de circuite sau comutare de pachete, inclusiv Internet) şi reţele mobile terestre, reţele de transport al energiei electrice, în cazul în care acestea sînt utilizate şi pentru transmiterea semnalelor, reţele utilizate pentru difuzarea programelor audiovizuale, reţele de televiziune prin cablu, indiferent de tipul informaţiei transmise; reţea publică de comunicaţii electronice – reţea de comunicaţii electronice utilizată în întregime sau în principal pentru furnizarea de servicii de comunicaţii electronice accesibile publicului, care asigură transferul de informaţii între punctele terminale ale reţelei;	**Compatibil**			Viceprim-ministru pentru digitalizare MIDR ANRCETI

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
37. ***„serviciu de comunicații electronice”*** *înseamnă un serviciu de comunicații electronice astfel cum este definit la articolul 2 punctul 4 din Directiva (UE) 2018/1972;* ***articolul 2 punctul 4 din Directiva (UE) 2018/1972:*** ***„serviciu de comunicații electronice”*** înseamnă un serviciu furnizat de regulă contra cost prin intermediul rețelelor de comunicații electronice și care include, cu excepția serviciilor care constau în furnizarea de conținuturi prin intermediul rețelelor și serviciilor de comunicații electronice sau în exercitarea unui control editorial asupra conținuturilor respective, următoarele tipuri de servicii: (a) „serviciul de acces la internet”, astfel cum este definit la articolul 2 al doilea paragraf punctul 2 din Regulamentul (UE) 2015/2120; (b) „serviciul de comunicații interpersonale”; și (c) servicii care constau, în totalitate sau în principal, în transmiterea de semnale, cum ar fi serviciile de transmisie utilizate pentru furnizarea de servicii între dispozitive (machine-to-machine) și pentru radiodifuziune;	**Articolul 2 din Legea nr. 241/2007 comunicațiilor electronice** ***serviciu de comunicaţii electronice*** **–** serviciu furnizat, de regulă, contra plată, care constă în întregime sau în principal în transportul semnalelor prin reţelele de comunicaţii electronice, inclusiv serviciile de telecomunicaţii şi serviciile de transmisie prin reţelele utilizate pentru difuzarea de programe audiovizuale, dar fără a include serviciile prin care se furnizează conţinutul informaţiei transmise prin intermediul reţelelor sau serviciilor de comunicaţii electronice sau prin care se exercită controlul editorial asupra acestui conţinut; de asemenea, nu se includ serviciile societăţii informaţionale (în particular, serviciile de comerţ electronic) care nu constau, în întregime sau în principal, în transportul semnalelor prin intermediul reţelelor de comunicaţii electronice;	**compatibil**			MIDR ANRCETI Viceprim-ministru pentru digitalizare
38. **„entitate”** înseamnă o persoană fizică sau juridică constituită și recunoscută ca atare în temeiul dreptului intern al locului său de stabilire care poate, acționând în nume propriu, să exercite drepturi și să fie supusă unor obligații;	**Codul civil:** **Articolul 23. Noțiunea de persoană fizică** Persoană fizică este omul, privit individual, ca titular de drepturi şi de obligaţii civile. **Articolul 171. Noțiunea de persoană juridică** (1) Persoana juridică este subiectul de drept constituit în condițiile legii, având o organizare de sine stătătoare și un patrimoniu propriu şi distinct, afectat realizării unui anumit scop conform cu	**Compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	legea, ordinea publică şi bunele moravuri. (2) Persoană juridică poate să dobândească şi să exercite în nume propriu drepturi patrimoniale şi personale nepatrimoniale, să-şi asume obligaţii, poate fi reclamant şi pîrît în instanța de judecată. (3) Persoana juridică poate fi organizată în mod corporativ sau în baza calităţii de membru, poate fi dependentă sau independentă de un anumit număr de membri, poate avea scop lucrativ sau nelucrativ. (4) În funcţie de participare la constituirea patrimoniului persoanei juridice, fondatorii (membrii) au sau nu au drepturi de creanţă faţă de ea. Persoane juridice în a căror privinţă fondatorii (membrii) au drepturi de creanţă sunt societăţile comerciale şi cooperativele. Persoane juridice în a căror privinţă fondatorii (membrii) nu au drepturi de creanţă sînt organizaţiile necomerciale.				
39. ***„furnizor de servicii gestionate”*** *înseamnă o entitate care furnizează servicii legate de instalarea, gestionarea, funcționarea sau întreținerea produselor, rețelelor, infrastructurii, aplicațiilor TIC sau a oricăror alte rețele și sisteme informatice, prin intermediul asistenței sau al administrării active efectuate fie la sediul clienților, fie la distanță;*		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
40. ***„furnizor de servicii de securitate gestionate”*** *înseamnă un furnizor de servicii gestionate care efectuează sau furnizează asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică;*		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
41. ***„organizație de cercetare”*** *înseamnă o entitate care are ca obiectiv principal să desfășoare activități de cercetare aplicată sau de dezvoltare experimentală în vederea*	**Articolul 15 din Codul cu privire la știință și inovare** *Organizație din domeniile cercetării și inovării* – persoană juridică care	Parțial compatibil prevederile actului Uniunii Europene			Viceprim-ministru pentru digitalizare

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
exploatării rezultatelor cercetării respective în scopuri comerciale, dar care nu include instituțiile de învățământ.	desfășoară una dintre următoarele activități: cercetări fundamentale și/sau aplicative, dezvoltarea experimentală, implementarea rezultatelor științifice și inovațiilor, transferul tehnologic, pregătirea și perfecționarea cadrelor științifice.	netranspuse nu sunt fundamentale			Ministerul Economiei
Capitolul II. Cadre coordonate în materie de securitate cibernetică **Articolul 7. Strategia națională de securitate cibernetică** (1) Fiecare stat membru adoptă o strategie națională de securitate cibernetică care prevede obiectivele strategice, *resursele necesare pentru atingerea obiectivelor respective* și măsurile de politică și de reglementare adecvate, în vederea atingerii și menținerii unui nivel ridicat de securitate cibernetică. Strategia națională de securitate cibernetică include următoarele elemente: (a) *obiectivele și prioritățile* strategiei de securitate cibernetică *a statului membru, care acoperă în special sectoarele menționate în anexele I și II*; (b) un cadru de guvernanță pentru realizarea obiectivelor și priorităților menționate la litera (a) de la prezentul alineat, inclusiv politicile menționate la alineatul (2); (c) *un cadru de guvernanță care clarifică rolurile și responsabilitățile părților interesate relevante la nivel național, care sprijină cooperarea și coordonarea la nivel național între autoritățile competente, punctele unice de contact și echipele CSIRT în temeiul prezentei directive, precum și coordonarea și cooperarea dintre aceste organisme și autoritățile competente în temeiul actelor juridice sectoriale ale Uniunii;* (d) *un mecanism care* să identifice activele și *o evaluare a riscurilor* din statul membru respectiv; (e) o identificare a măsurilor de asigurare a pregătirii pentru incidente, a capacității de răspuns la acestea și a redresării în urma	**Articolul 6. Planificarea și coordonarea strategică în domeniul securității cibernetice la nivel național** (1) Coordonarea strategică la nivel național în domeniul securității cibernetice se realizează de Guvern prin intermediul autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. (2) Pentru asigurarea funcției de coordonare strategică, Guvernul instituie și stabilește modul de organizare și funcționare a Consiliului coordonator în domeniul securității cibernetice, organ colegial fără personalitate juridică, a cărui funcție de bază este promovarea și coordonarea, la nivel strategic și operațional, a politicilor în domeniul securității cibernetice. (3) Strategia națională de securitate cibernetică este un document de politici care definește obiectivele strategice și măsurile de politică și de reglementare care au ca scop atingerea și menținerea unui nivel ridicat de securitate cibernetică. Strategia națională de securitate cibernetică se aprobă de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.	**Compatibil**		Adițional pentru implementarea prevederilor proiectului Guvernul urmează să aprobe documentul respectiv de politici și să asigure evaluarea periodică a acestuia în conformitate cu cadrul normativ național relevant	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
acestora, inclusiv cooperarea dintre sectorul public și cel privat; (f) o listă a diferitelor autorități și părți interesate care participă la punerea în aplicare a strategiei naționale de securitate cibernetică; (g) un cadru de politică menit să asigure o mai bună coordonare între autoritățile competente în temeiul prezentei directive și al Directivei (UE) .../...[(46)] în scopul schimbului de informații privind *riscurile*, amenințările cibernetice și incidentele, *precum și privind riscurile, amenințările și incidentele fără caracter cibernetic* și al exercitării sarcinilor de supraveghere*, după caz*; (h) *un plan, inclusiv măsurile necesare pentru a spori nivelul general de sensibilizare a cetățenilor cu privire la securitatea cibernetică.* (2) În cadrul strategiei naționale de securitate cibernetică, statele membre adoptă politici: (a) care abordează securitatea cibernetică în lanțul de aprovizionare pentru produsele TIC și serviciile TIC utilizate de *entități* pentru furnizarea serviciilor lor; (b) privind includerea și specificarea cerințelor legate de securitatea cibernetică pentru produsele TIC și serviciile TIC în cadrul achizițiilor publice, *inclusiv în legătură cu certificarea de securitate cibernetică, criptarea și utilizarea produselor de securitate cibernetică cu sursă deschisă;* (c) *de gestionare a vulnerabilităților, inclusiv promovarea și facilitarea* divulgării coordonate a vulnerabilităților în temeiul articolului 12 *alineatul (1);* (d) legate de menținerea disponibilității, integrității *și confidențialității* generale a nucleului public al internetului deschis, *inclusiv securitatea cibernetică a cablurilor de comunicații submarine, după caz*; (e) *de promovare a dezvoltării și integrării tehnologiilor avansate relevante care vizează implementarea unor măsuri de ultimă*					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
generație de gestionare a riscurilor în materie de securitate cibernetică; (f) *de promovare și dezvoltare a educației și a formării privind* securitatea cibernetică, competențele, sensibilizarea și inițiativele de cercetare și dezvoltare în materie de securitate cibernetică*, precum și orientări privind bunele practici și controale în materie de igienă cibernetică, destinate cetățenilor, părților interesate și entităților*; (g) de sprijinire a instituțiilor academice și de cercetare în vederea dezvoltării, *consolidării și promovării implementării* unor instrumente de securitate cibernetică și a unei infrastructuri de rețele securizate; (h) care să includă proceduri relevante și instrumente adecvate de schimb de informații care să sprijine schimbul voluntar de informații în materie de securitate cibernetică între entități, în conformitate cu dreptul Uniunii; (i) de *consolidare a rezilienței cibernetice și a nivelului de referință în materie de igienă cibernetică* pentru întreprinderile mici și mijlocii, în special pentru cele excluse din domeniul de aplicare al prezentei directive, *prin furnizarea de orientări și asistență ușor accesibile pentru nevoile lor specifice*; (j) *de promovare a unei protecții cibernetice active.* (3) Statele membre notifică Comisiei strategiile lor naționale de securitate cibernetică în termen de trei luni de la adoptarea acestora. Statele membre pot exclude din astfel de notificări *informații care se referă la* securitatea lor națională. (4) Statele membre își evaluează *periodic, dar* cel puțin o dată la *cinci* ani, strategiile naționale de securitate cibernetică pe baza indicatorilor-cheie de performanță și, dacă este necesar, le actualizează. ENISA sprijină statele membre, la *cererea acestora,* la elaborarea *sau actualizarea* unei strategii naționale de					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
securitate cibernetică și a unor indicatori-cheie de performanță pentru evaluarea strategiei respective, *în vederea alinierii acesteia la cerințele și obligațiile prevăzute în prezenta directivă*.					
Articolul 8. Autoritățile naționale competente și punctele unice de contact (1) Fiecare stat membru desemnează sau instituie una sau mai multe autorități competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere menționate în capitolul VII (autorități competente). (2) Autoritățile competente menționate la alineatul (1) monitorizează punerea în aplicare a prezentei directive la nivel național. (3) Fiecare stat membru desemnează sau instituie un punct unic de contact. În cazul în care un stat membru desemnează sau instituie o singură autoritate competentă conform alineatului (1), autoritatea competentă respectivă servește, de asemenea, drept punct unic de contact pentru statul membru respectiv. (4) Fiecare punct unic de contact exercită o funcție de legătură menită să asigure cooperarea transfrontalieră a autorităților din statul membru de care aparține cu autoritățile relevante din alte state membre, *și, acolo unde este cazul, cu Comisia și cu ENISA,* dar și să asigure cooperarea transsectorială cu alte autorități competente din statul membru de care aparține. (5) Statele membre se asigură că autoritățile lor competente și punctele unice de contact dispun de resurse adecvate pentru a-și îndeplini în mod eficace și eficient atribuțiile și a realiza astfel obiectivele prezentei directive.	**Articolul 7. Autoritatea competentă** (1) Guvernul desemnează autoritatea competentă la nivel național în domeniul securității cibernetice și stabilește modul de organizare și funcționare a acesteia. (2) Autoritatea competentă desemnată de Guvern exercită funcțiile de punct național unic de contact și echipă de răspuns la incidentele cibernetice la nivel național. (3) Autoritatea competentă exercită următoarele atribuții principale: a) identifică furnizorii de servicii pe teritoriul Republicii Moldova; b) elaborează și promovează practici comune pentru gestionarea incidentelor cibernetice și a riscurilor și pentru sistemele de clasificare a incidentelor cibernetice, a riscurilor și a informațiilor; c) asigură interacțiunea strategică la nivel internațional și schimbul de experiență cu alte state, organizații internaționale sau entități create de acestea privind aspecte legate de securitatea rețelelor și a sistemelor informatice, studiază exemple de bune practici privind riscurile și incidente cibernetice; d) asigură interacțiunea cu autoritățile și instituțiile publice naționale; e) exercită supravegherea și controlul respectării de către furnizorii de servicii a obligațiilor ce le revin conform prezentei legi; f) emite acte cu caracter obligatoriu, recomandări și orientări	Parțial Compatibil		Guvernul urmează să desemneze autoritatea competentă și să asigure constituirea și organizarea CSIRT	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	metodologice pentru furnizorii de servicii în vederea conformării și remedierii deficiențelor constatate și stabilește termenul până la care aceștia trebuie să se conformeze; g) examinează sesizări cu privire la neîndeplinirea obligațiilor de către furnizorii de servicii; h) exercită, atribuțiile organului constatator pentru cauze contravenționale în domeniul securității rețelelor și sistemelor informatice în conformitate cu prevederile Codului contravențional; i) alte atribuții care decurg din prevederile prezentei legi. (4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale: a) monitorizează și analizează amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național, precum și acordă asistență furnizorilor de servicii, la solicitarea acestora, în procesul de monitorizare de către aceștia a rețelei lor și a sistemelor lor informatice; b) emite avertizări timpurii, alerte, anunțuri și diseminează informații persoanelor relevante privind amenințările cibernetice, vulnerabilitățile, riscurile și incidentele cibernetice; c) recepționează notificări privind incidentele cibernetice care afectează rețelele și sistemele informatice ale furnizorilor de servicii; d) asigură răspunsul la incidente cibernetice, în conformitate cu procedurile stabilite de prezenta lege și actele normative de punere în aplicare a acesteia, inclusiv acordă asistență în acest sens furnizorilor de servicii;				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	e) colectează și analizează date criminalistice și furnizează analize dinamice de risc și de incident și conștientizare a situației în materie de securitate cibernetică; f) cooperează, la nivel național și internațional, cu echipele de răspuns la incidentele cibernetice în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații; g) efectuează, la cererea unui furnizor de servicii, scanări proactive a rețelelor și a sistemelor informatice ale solicitantului pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, în conformitate cu actul normativ aprobat de Guvern în temeiul articolului 17 alineatul (5); h) implementează în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate; i) asigură coordonarea procesului de divulgare a vulnerabilităților în conformitate cu cadrul normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. (5) În exercitarea funcției de punct unic de contact la nivel național, autoritatea competentă exercită următoarele atribuții principale: a) asigură o legătură a autorităților și instituțiilor publice naționale cu autoritățile similare din alte state și/sau cu organizații internaționale sau entități constituite de către acestea; b) transmite, la cererea autorităților și instituțiilor publice sau a echipelor de răspuns la incidente cibernetice către punctele unice de contact din alte state notificări și				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	solicitări privind incidentele cibernetice ce afectează prestarea de servicii de către furnizorii respectivi; c) transmite autorităților și instituțiilor publice naționale, conform competenței acestora, notificări și cereri primite din alte state sau de la organizații internaționale ori de la entitățile constituite de către acestea.				
(6) Fiecare stat membru notifică fără întârzieri nejustificate Comisiei identitatea autorității competente menționate la alineatul (1) și a punctului unic de contact menționat la alineatul (3), sarcinile respectivelor autorități și orice modificare ulterioară a acestora. Fiecare stat membru face publică identitatea autorității sale competente. Comisia face publică lista punctelor unice de contact.		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
Articolul 9. Cadrele naționale de gestionare a crizelor cibernetice (1) 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"). Statele membre se asigură că respectivele autorități dispun de resurse adecvate pentru a îndeplini, în mod eficace și eficient, sarcinile care le-au fost încredințate. *Statele membre asigură corelarea cu cadrele existente pentru gestionarea națională generală a crizelor.* (2) *În cazul în care un stat membru desemnează sau instituie mai mult de o autoritate de gestionare a crizelor cibernetice în temeiul alineatului (1), acesta indică în mod clar care dintre autoritățile respective servește drept coordonator pentru gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor.* (3) Fiecare stat membru identifică capacitățile, mijloacele și procedurile care pot	**Articolul 8. Cadrul național de gestionare a crizelor în domeniul securității cibernetice** **(1)** Autoritatea competentă este responsabilă de administrarea incidentelor și a crizelor în domeniul securității cibernetice la nivel național. **(2)** În acest scop autoritatea competentă aprobă planul național de răspuns la incidente și crize de securitate cibernetică în care sunt stabilite obiectivele și modalitățile de administrare a incidentelor cibernetice și a crizelor de securitate cibernetică de mare amploare la nivel național. **(3)** Planul național de răspuns la incidente și crize de securitate cibernetică trebuie să includă cel puțin însă fără să se limiteze la acestea: a) obiectivele măsurilor și ale activităților naționale de pregătire; b) sarcinile și responsabilitățile autorităților naționale competente; c) procedurile de gestionare a crizelor și canalele de schimb de informații;	**Compatibil**		Suplimentar, Guvernul urmează să aprobe cadrul metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidente cibernetice și crize de securitate cibernetică, interacțiunea dintre autoritățile și instituțiile publice cu atribuții în procesul de elaborare și actualizare, precum și interacțiunea acestora cu sectorul privat.	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
fi utilizate în caz de criză în sensul prezentei directive. (4) Fiecare stat membru adoptă un plan național de răspuns la incidente de securitate cibernetică de mare amploare și crize, în care sunt stabilite obiectivele și modalitățile de gestionare a incidentelor de securitate cibernetică de mare amploare și a crizelor. Planul respectiv stabilește, în special: (a) obiectivele măsurilor și ale activităților naționale de pregătire; (b) sarcinile și responsabilitățile autorităților de gestionare a crizelor cibernetice; (c) procedurile de gestionare a crizelor *cibernetice, inclusiv integrarea acestora în cadrul național general de gestionare a crizelor* și canalele de schimb de informații; (d) măsurile naționale de pregătire, inclusiv exerciții și activități de formare; (e) părțile interesate relevante din sectorul public și privat și infrastructura implicată; (f) procedurile naționale și acordurile dintre autoritățile și organismele naționale relevante menite să asigure participarea efectivă a statului membru la gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare și a crizelor la nivelul Uniunii și sprijinul acordat de acesta.	d) măsurile de pregătire, inclusiv exerciții și activități de formare; e) părțile interesate relevante din sectorul public și privat și infrastructura implicată; f) procedurile și mecanismele de interacțiune dintre autoritățile și instituțiile publice responsabile la nivel național, precum și de interacțiune coordonată a acestora în administrarea incidentelor și a crizelor de securitate cibernetică de mare amploare la nivel european și internațional. **(4)** Guvernul aprobă cadrul metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidente cibernetice și crize de securitate cibernetică, interacțiunea dintre autoritățile și instituțiile publice cu atribuții în procesul de elaborare și actualizare, precum și interacțiunea acestora cu sectorul privat.				
(Articolul 9. Cadrele naționale de gestionare a crizelor cibernetice) (5) În termen de trei luni de la desemnarea sau instituirea autorității de gestionare a crizelor cibernetice menționate la alineatul (1), fiecare stat membru *notifică* Comisiei identitatea autorității sale și orice modificări ulterioare ale acesteia. *Statele membre* prezintă *Comisiei și Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) informații relevante referitoare la cerințele de la alineatul (4) cu privire la* planurile lor naționale de răspuns la incidente de securitate cibernetică de mare amploare și crize, în termen de trei luni de		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
la adoptarea planurilor respective. Statele membre pot exclude informații în cazul și în măsura în care o asemenea excludere este necesară pentru securitatea lor națională.					
Articolul 10. Echipele de intervenție în caz de incidente de securitate informatică (echipe CSIRT) (1) Fiecare stat membru desemnează sau instituie una sau mai multe echipe CSIRT. Echipele CSIRT pot fi desemnate sau instituite din cadrul unei autorități competente. Echipele CSIRT respectă cerințele prevăzute la articolul 11 alineatul (1), acoperă cel puțin sectoarele, subsectoarele și tipurile de entități menționate în anexele I și II și sunt responsabile de gestionarea incidentelor în conformitate cu o procedură bine definită. (2) Statele membre se asigură că fiecare echipă CSIRT dispune de resurse adecvate pentru a-și îndeplini efectiv sarcinile stabilite la articolul 11 alineatul (3). (3) Statele membre se asigură că fiecare echipă CSIRT dispune de o infrastructură de comunicare și de informații adecvată, sigură și rezilientă prin care face schimb de informații cu entitățile esențiale și entitățile importante și cu alte părți interesate relevante. În acest scop, statele membre se asigură că fiecare echipă CSIRT contribuie la implementarea unor instrumente securizate de schimb de informații. (4) Echipele CSIRT cooperează și, după caz, fac schimb de informații relevante în conformitate cu articolul 29 cu comunități sectoriale sau transsectoriale formate din entități esențiale și entități importante.	**Articolul 7. Autoritatea competentă din proiectul de lege:** (1) Guvernul desemnează autoritatea competentă la nivel național în domeniul securității cibernetice și stabilește modul de organizare și funcționare a acesteia. (2) Autoritatea competentă desemnată de Guvern exercită funcțiile de punct național unic de contact și echipă de răspuns la incidentele cibernetice la nivel național. …….. (4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale: a) monitorizează și analizează amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național, precum și acordă asistență furnizorilor de servicii, la solicitarea acestora, în procesul de monitorizare de către aceștia a rețelei lor și a sistemelor lor informatice; b) emite avertizări timpurii, alerte, anunțuri și diseminează informații persoanelor relevante privind amenințările cibernetice, vulnerabilitățile, riscurile și incidentele cibernetice; c) recepționează notificări privind incidentele cibernetice care afectează rețelele și sistemele informatice ale furnizorilor de servicii; d) asigură răspunsul la incidente cibernetice, în conformitate cu procedurile stabilite de prezenta lege și actele normative de punere în aplicare a acesteia, inclusiv acordă asistență în acest sens furnizorilor de servicii;	**Compatibil**		Cerințele stabilite de art. 11 al Directivei urmează a fi implementate în procesul constituirii, reglementării modului de organizare și funcționare a autorității competente/ CSIRT respective și dotării acesteia cu resursele umane și financiare și cu mijloacele tehnice necesare asigurării îndeplinirii acestor cerințe.	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	e) colectează și analizează date criminalistice și furnizează analize dinamice de risc și de incident și conștientizare a situației în materie de securitate cibernetică; f) cooperează, la nivel național și internațional, cu echipele de răspuns la incidentele cibernetice în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații; g) efectuează, la cererea unui furnizor de servicii, scanări proactive a rețelelor și a sistemelor informatice ale solicitantului pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, în conformitate cu actul normativ aprobat de Guvern în temeiul articolului 17 alineatul (5); h) implementează în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate; i) asigură coordonarea procesului de divulgare a vulnerabilităților în conformitate cu cadrul normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.				
(5) Echipele CSIRT participă la evaluările inter pares organizate în conformitate cu articolul 19. (6) Statele membre asigură cooperarea efectivă, eficientă și sigură a propriilor echipe CSIRT în cadrul rețelei CSIRT. (7) *Echipele CSIRT pot stabili relații de cooperare cu echipele naționale de intervenție în caz de incidente de securitate informatică din țări terțe. În cadrul acestor relații de cooperare, statele membre facilitează un schimb de informații eficace, eficient și securizat cu respectivele echipe naționale de*		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
intervenție în caz de incidente de securitate informatică din țări terțe, utilizând protocoalele relevante de schimb de informații, inclusiv „Traffic Light Protocol”. Echipele CSIRT pot face schimb de informații relevante cu echipele naționale de intervenție în caz de incidente de securitate informatică din țări terțe, inclusiv de date cu caracter personal în conformitate cu dreptul Uniunii privind protecția datelor. (8) *Echipele CSIRT pot coopera cu echipele naționale de intervenție în caz de incidente de securitate informatică sau cu organisme echivalente din țări terțe, în special pentru a le oferi asistență în materie de securitate cibernetică.* (9) Fiecare stat membru notifică fără întârzieri nejustificate Comisiei identitatea echipei CSIRT menționate la alineatul (1) de la prezentul articol *și a* echipei CSIRT desemnată drept coordonator în conformitate cu articolul 12 alineatul (1), sarcinile acestora în legătură cu entitățile *esențiale și entitățile importante*, precum și orice modificări ulterioare. (10) Statele membre pot solicita asistența ENISA pentru instituirea echipelor lor CSIRT.					
Articolul 11. Cerințele pe care trebuie să le respecte, *capacitățile tehnice* și sarcinile care le revin echipelor CSIRT (1) Echipele CSIRT trebuie să respecte următoarele cerințe: (a) echipele CSIRT asigură o disponibilitate ridicată a *canalelor lor de comunicare* evitând punctele unice de defecțiune și dispun de mai multe mijloace pentru a fi contactate și pentru a contacta alte entități în orice moment; acestea specifică în mod clar canalele de comunicare și le aduc la cunoștința bazei de utilizatori și a partenerilor de cooperare; (b) localurile echipelor CSIRT și sistemele informatice de suport sunt situate în amplasamente securizate;	**Articolul 7. Autoritatea competentă din proiectul de lege:** **(1)** Guvernul desemnează autoritatea competentă la nivel național în domeniul securității cibernetice și stabilește modul de organizare și funcționare a acesteia. (2) Autoritatea competentă desemnată de Guvern exercită funcțiile de punct național unic de contact și echipă de răspuns la incidentele cibernetice la nivel național. **Articolul 21. Intrarea în vigoare a legii și măsuri de implementare** (1) Guvernul:	Compatibil parțial		Cerințele stabilite de art. 11 al Directivei urmează a fi implementate în procesul constituirii, reglementării modului de organizare și funcționare a autorității competente respective și dotării acesteia cu resursele umane și financiare și cu mijloacele tehnic necesare asigurării îndeplinirii acestor cerințe	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(c) echipele CSIRT dispun de un sistem adecvat de gestionare și rutare a cererilor, în special în vederea facilitării eficace și eficiente a transferurilor; (d) *echipele CSIRT asigură confidențialitatea și credibilitatea operațiunilor lor;* (e) echipele CSIRT dispun de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor lor *și se asigură că personalul lor este format în mod corespunzător*; (f) echipele CSIRT sunt echipate cu sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor lor. Echipele CSIRT pot participa la rețele internaționale de cooperare. (2) *Statele membre se asigură că echipele lor CSIRT dispun colectiv de capacitățile tehnice necesare pentru a-și îndeplini sarcinile menționate la alineatul (3). Statele membre se asigură că se alocă resurse suficiente echipelor lor CSIRT pentru a garanta un nivel adecvat de personal pentru ca acestea să își poată dezvolta capacitățile tehnice.*	a) în termen de 6 luni din data publicării prezentei legi, va întreprinde măsurile necesare pentru instituirea/desemnarea autorității competente, reglementarea modului de organizare și funcționare a acesteia și dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite prin prezenta lege; ….. (3) Pentru realizarea eficientă a sarcinii stabilite la alineatul (2) litera a), Guvernul trebuie să asigure autoritatea competentă, astfel încât echipa de răspuns la incidente cibernetice la nivel național să corespundă următoarelor cerințe: a) să asigure o disponibilitate ridicată a canalelor lor de comunicare evitând punctele unice de defecțiune; b) să dispună de mai multe mijloace pentru a fi contactată și pentru a contacta alte entități în orice moment; c) să specifice în mod clar canalele de comunicare și să le aducă la cunoștința bazei de utilizatori și a partenerilor de cooperare; d) să dispună de sediu/sedii și sistemele informatice de suport, situate în amplasamente securizate; e) să dispună de un sistem adecvat de gestionare și direcționare a solicitărilor, în special pentru a facilita preluarea, prelucrarea și transmiterea acestora întru-un mod efectiv și eficient; f) să asigure confidențialitatea și credibilitatea operațiunilor lor; g) să dispună de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor sale și se asigură că personalul său este format în mod corespunzător; h) să dispună de sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor sale.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(3) Echipelor CSIRT le revin următoarele sarcini: (a) monitorizarea *și analizarea* amenințărilor cibernetice, a vulnerabilităților și a incidentelor la nivel național *și, la cerere, acordarea 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*; (b) asigurarea unor mecanisme de avertizare timpurii, alerte, anunțuri și diseminare de informații către entitățile esențiale și entitățile importante, precum și către *autoritățile competente și* alte părți interesate relevante cu privire la amenințările cibernetice, vulnerabilități și incidente*, în timp aproape real, dacă este posibil*; (c) răspunsul la incidente *și acordarea de asistență entităților esențiale și entitățile importante implicate, atunci când este cazul*; (d) *colectarea și analizarea datelor criminalistice și* furnizarea de analize dinamice de risc și de incident și conștientizarea situației în materie de securitate cibernetică; (e) furnizarea, la cererea unei entități esențiale sau a unei entități importante, a unei scanări proactive a rețelelor și a sistemelor informatice a*le entității implicate pentru a detecta vulnerabilitățile cu un impact potențial semnificativ*; ……. (g) *după caz, acționarea în calitate de coordonator în scopul procesului de divulgare coordonată a vulnerabilităților menționat la articolul 12 alineatul (1);* (h) *contribuirea la implementarea unor instrumente securizate de schimb de informații, în temeiul articolului 10 alineatul (3).* *Echipele CSIRT pot efectua scanări proactive și neintruzive ale rețelelor și sistemelor informatice accesibile publicului ale*	**Articolul 7 din proiectul de lege** (4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale: a) monitorizează și analizează amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național, precum și acordă asistență furnizorilor de servicii, la solicitarea acestora, în procesul de monitorizare de către aceștia a rețelei lor și a sistemelor lor informatice; b) emite avertizări timpurii, alerte, anunțuri și diseminează informații persoanelor relevante privind amenințările cibernetice, vulnerabilitățile, riscurile și incidentele cibernetice; c) recepționează notificări privind incidentele cibernetice care afectează rețelele și sistemele informatice ale furnizorilor de servicii; d) asigură răspunsul la incidente cibernetice, în conformitate cu procedurile stabilite de prezenta lege și actele normative de punere în aplicare a acesteia, inclusiv acordă asistență în acest sens furnizorilor de servicii; e) colectează și analizează date criminalistice și furnizează analize dinamice de risc și de incident și conștientizare a situației în materie de securitate cibernetică; f) cooperează, la nivel național și internațional, cu echipele de răspuns la incidentele cibernetice în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații; g) efectuează, la cererea unui furnizor de servicii, scanări proactive a	Compatibil		Adițional competența CSIRT național urmează a fi detaliată în actul de constituire a autorității competente/CSIRT care va reglementa modul de organizare și funcționare a autorității competente respective și dotării acesteia cu resursele umane și financiare și cu mijloacele tehnice necesare asigurării îndeplinirii acestor sarcini	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
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. *Atunci când îndeplinesc sarcinile menționate la primul paragraf, echipele CSIRT pot acorda prioritate anumitor sarcini pe baza unei abordări bazate pe riscuri.* (4) Echipele CSIRT stabilesc relații de cooperare cu părțile interesate relevante din sectorul privat, în vederea îndeplinirii obiectivelor prezentei directive. (5) Pentru a facilita cooperarea menționată la alineatul (4), echipele CSIRT promovează adoptarea și utilizarea unor practici, sisteme de clasificare și taxonomii comune sau standardizate în legătură cu: (a) procedurile de gestionare a incidentelor; (b) gestionarea crizelor; și (c) divulgarea coordonată a vulnerabilităților în temeiul articolului 12 alineatul (1).	rețelelor și a sistemelor informatice ale solicitantului pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, în conformitate cu actul normativ aprobat de Guvern în temeiul articolului 17 alineatul (5); h) implementează în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate; i) asigură coordonarea procesului de divulgare a vulnerabilităților în conformitate cu cadrul normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.				
Articolul 11. Cerințele pe care trebuie să le respecte, *capacitățile tehnice* și sarcinile care le revin echipelor CSIRT **(**3) Echipelor CSIRT le revin următoarele sarcini: (f) participarea la rețeaua CSIRT și furnizarea de asistență reciprocă *în funcție de capacitățile și competențele lor* altor membri ai rețelei, la cererea acestora;		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
Articolul 12. Divulgarea coordonată a vulnerabilităților și *baza de date europeană* a vulnerabilităților (1) Fiecare stat membru desemnează una dintre echipele sale CSIRT drept coordonator în scopul divulgării coordonate a vulnerabilităților. Echipa CSIRT desemnată drept coordonator acționează ca intermediar de	**Articolul 7 alineatul (4) din proiectul de lege** (4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale: …..	Parțial compatibil		Suplimentar prevederile respective ale Directivei urmează a fi transpuse prin aprobarea cadrului normativ de punere în aplicare a prevederilor noii legi, în mod special actul normativ al Guvernului la care se face	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
încredere, facilitând, dacă este necesar, interacțiunea dintre persoana fizică sau juridică care raportează o vulnerabilitate și producătorul sau furnizorul de produse TIC sau servicii TIC *potențial vulnerabile, la cererea oricărei părți. Sarcinile echipei CSIRT desemnate drept coordonator includ:* (a) *identificarea și contactarea entităților implicate;* (b) *asistarea persoanelor fizice sau juridice care raportează o vulnerabilitate;* (c) *negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități.* *Statele membre se asigură că persoanele fizice sau juridice pot raporta, în mod anonim atunci când solicită acest lucru, o vulnerabilitate echipei CSIRT desemnate drept coordonator. Echipa CSIRT desemnată drept coordonator se asigură că au loc acțiuni subsecvente susținute în ceea ce privește vulnerabilitatea raportată și asigură anonimatul persoanei fizice sau juridice care raportează vulnerabilitatea.* 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.	i) asigură coordonarea procesului de divulgare a vulnerabilităților în conformitate cu cadrul normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.			referință în art. 6 alin. (4) lit. i).	
(2) ENISA creează și menține*, după consultarea Grupului de cooperare, o bază de date europeană a* vulnerabilităților. În acest scop, ENISA instituie și menține sisteme, politici și proceduri de informare adecvate *și adoptă măsurile tehnice și organizatorice necesare pentru a garanta securitatea și integritatea bazei de date europene a vulnerabilităților*, în special pentru a permite entităților, indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, și furnizorilor acestora de rețele și sisteme informatice să divulge și să înregistreze*, pe*		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
bază voluntară, vulnerabilitățile *public cunoscute* din produsele TIC sau serviciile TIC. *Se oferă* acces tuturor părților interesate la informațiile privind vulnerabilitățile conținute în *baza de date europeană* a vulnerabilităților. *Baza de date* include: (a) informații care descriu vulnerabilitatea; (b) produsele TIC sau serviciile TIC afectate și gravitatea vulnerabilității în ceea ce privește circumstanțele în care aceasta poate fi exploatată; (c) disponibilitatea unor corecții conexe și, dacă astfel de corecții nu sunt disponibile, orientări *oferite de autoritățile* competente sau de echipele CSIRT adresate utilizatorilor de produse *TIC* și servicii *TIC* vulnerabile cu privire la modul în care pot fi atenuate riscurile care rezultă din vulnerabilitățile divulgate.					
Articolul 13. Cooperarea la nivel național (1) Atunci când sunt separate, autoritățile competente, punctul unic de contact și echipele CSIRT ale aceluiași stat membru cooperează între ele pentru îndeplinirea obligațiilor ce le revin în temeiul prezentei directive. (2) Statele membre se asigură că echipele lor CSIRT *sau, atunci când este cazul, autoritățile lor competente* primesc notificări privind incidentele *semnificative în temeiul articolului 23*, și incidentele, amenințările cibernetice și incidentele evitate la limită în temeiul articolului *30*. (3) Statele membre se asigură că echipele sale CSIRT sau, atunci când este cazul, autoritățile sale competente informează punctele lor unice de contact cu privire la notificările privind incidentele, amenințările cibernetice și incidentele evitate la limită comunicate în temeiul prezentei directive. (4) *Pentru a garanta că* sarcinile și obligațiile *autorităților competente , ale punctelor unice de contact și ale echipelor CSIRT sunt îndeplinite în mod eficient,* statele membre asigură*, în măsura posibilului,* o	**Articolul 7. Autoritatea competentă** (1) Guvernul desemnează autoritatea competentă la nivel național în domeniul securității cibernetice și stabilește modul de organizare și funcționare a acesteia. (2) Autoritatea competentă desemnată de Guvern exercită funcțiile de punct național unic de contact și echipă de răspuns la incidentele cibernetice la nivel național. **Articolul 11. Obligațiile furnizorilor de servicii de a notifica incidentele cibernetice** (1) Furnizorul de servicii informează imediat autoritatea competentă, dar nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre un incident cibernetic: a) care are un impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului; b) al cărui impact semnificativ asupra securității rețelei sau sistemului	Parțial compatibil Prevederile Directivei transpuse fac referință la alte acte ale Uniunii Europene ce nu sunt transpuse de proiectul de lege și nu a fost transpus de legislația națională în vigoare;		În proiectul de act normativ se propune concentrarea funcțiilor de autoritate competentă, punct unic de contact la nivel național și CSIRT național într-o singură entitate.	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
cooperare adecvată între *aceste organisme* și autoritățile de aplicare a legii, autoritățile pentru protecția datelor, *autoritățile naționale în temeiul Regulamentelor (CE) nr. 300/2008 și (UE) 2018/1139, organismele de supraveghere în temeiul Regulamentului (UE) nr. 910/2014,* autoritățile competente în temeiul Regulamentului (UE) .../...[47], *autoritățile naționale de reglementare în temeiul Directivei (UE) 2018/1972,* autoritățile *competente* în temeiul Directivei (UE) .../...[48], *precum și autoritățile competente în temeiul altor acte juridice sectoriale ale Uniunii,* din statul membru respectiv. (5) Statele membre se asigură că autoritățile lor competente *în temeiul prezentei directive și autoritățile lor* competente în temeiul Directivei (UE) .../...[49] *cooperează și fac schimb periodic de informații pentru identificarea entităților critice,* cu privire la riscurile, amenințările cibernetice și incidentele, *precum și la riscurile, amenințările și incidentele de altă natură decât cibernetică* care afectează entitățile esențiale identificate ca fiind critice în temeiul Directivei (UE) .../...+, precum și cu privire la măsurile luate *ca răspuns la astfel de riscuri, amenințări și incidente. Statele membre se asigură, de asemenea, că* autoritățile *lor* competente *în temeiul prezentei directive și autoritățile lor competente în temeiul Regulamentului (UE) nr. 910/2014, al Regulamentului (UE) .../...[50] și al Directivei (UE) 2018/1972 fac schimb de informații relevante în mod periodic, inclusiv în ceea ce privește incidentele și amenințările cibernetice relevante.* (6) *Statele membre simplifică raportarea prin mijloace tehnice pentru notificările menționate la articolele 23 și 30.*	informatic ori asupra continuității serviciului nu este evident, dar poate fi presupus în mod rezonabil. (2) Furnizorul de servicii, prezintă autorității competente, imediat, dar nu mai târziu de 72 de ore din momentul în care a luat cunoștință despre incidentul cibernetic, o actualizare a informațiilor prezentate în conformitate cu alineatul (1) și o evaluare inițială a incidentului cibernetic cu impact semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili. (3) În cazul în care rețeaua sau sistemul informatic al furnizorului de servicii este administrat și/sau găzduit de un terț, furnizorul de servicii trebuie să se asigure că terțul îl informează în termenii stabiliți la alineatele (1) și (2) despre un incident cibernetic, specificat în alineatul (1) sau că terțul informează concomitent în aceiași termeni autoritatea competentă despre faptul producerii unui astfel de incident cibernetic. (4) Un incident cibernetic are un impact semnificativ dacă este îndeplinită cel puțin una dintre următoarele condiții: a) impactul incidentului cibernetic este sever conform gradului de consecințe determinat în raportul de evaluare a riscurilor rețelei și sistemului informatic întocmit în conformitate cu prevederile articolul 11 alineatului (2) literele a) - c) și a cerințelor prevăzute de actele menționate la articolul 11 alineatul (4); b) din cauza incidentului cibernetic prestarea serviciului este întreruptă pentru o perioadă mai mare decât perioada maximă de timp permisă pentru întrerupere, prevăzută în acordul corespunzător privind nivelul agreat al serviciilor, stabilit în cadrul relațiilor contractuale ale furnizorului de servicii, sau cerințele privind continuitatea				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	serviciului stabilite în documentația prevăzută la articolul 11 alineatul (2) litere a) - c); c) continuitatea serviciului unui terț este perturbată de incidentul cibernetic; d) furnizorului de servicii, furnizorului altui serviciu sau utilizatorilor serviciilor le-au fost cauzate sau le-ar putea fi cauzate prejudicii materiale sau non-materiale considerabile din cauza incidentului cibernetic. (5) Furnizorul de servicii este obligat să notifice într-o perioadă rezonabilă de timp, însă nu mai mult de 3 zile: a) persoanele potențial afectate de incidentul cibernetic cu impact semnificativ sau publicul, dacă persoanele afectate nu pot fi notificate individual; b) destinatarii serviciilor lor care ar putea fi afectați de o amenințare cibernetică semnificativă și orice măsuri sau măsuri corective pe care destinatarii respectivi le pot lua ca răspuns la amenințarea respectivă. Dacă este cazul, furnizorii de servicii informează, de asemenea, destinatarii în cauză despre amenințarea semnificativă propriu-zisă. (6) În cazul în care furnizorul de servicii nu realizează obligațiunile de notificare prevăzute de alineatul (5) în termenul respectiv, autoritatea competentă își poate aroga obligația de notificare a persoanelor posibil afectate sau publicul, informând despre aceasta furnizorul de servicii. (7) În cazul soluționării unui incident cibernetic cu impact semnificativ, furnizorul de servicii este obligat, în termen de 30 zile, să transmită autorității competente un raport care să includă cel puțin informații despre cauzele producerii incidentului cibernetic, timpul de soluționare a acestuia,				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	măsurile aplicate și impactul incidentului cibernetic. (8) Procedura de notificare a incidentelor cibernetice, inclusiv interacțiunea dintre furnizorul de servicii și autoritatea competentă, modul de stabilire a impactului unui incident cibernetic și formatul informațiilor evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic sunt stabilite de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. (9) Furnizorul de servicii este obligat imediat, însă nu mai târziu de 24 de ore, să notifice autoritatea competentă despre impactul semnificativ al unui incident cibernetic, care a afectat un terț, asupra continuității serviciului său dacă prestarea acestui serviciu depinde de serviciile prestate de acest terț.				
CAPITOLUL III. Cooperare *la nivelul Uniunii și la nivel internațional* **Articolul 14. Grupul de cooperare** (1) Pentru a sprijini și a facilita cooperarea strategică și schimbul de informații între statele membre, *precum și pentru a consolida încrederea*, se instituie un Grup de cooperare. (2) Grupul de cooperare își îndeplinește sarcinile pe baza programelor bienale de lucru menționate la alineatul (7). (3) Grupul de cooperare este format din reprezentanți ai statelor membre, ai Comisiei și ai ENISA. Serviciul European de Acțiune Externă participă la activitățile Grupului de cooperare în calitate de observator. Autoritățile europene de supraveghere (AES) *și autoritățile competente în temeiul Regulamentului* (UE).../...[(51)] pot participa la activitățile Grupului de cooperare *în conformitate cu articolul 47 alineatul (1) din regulamentul respectiv*.		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
După caz, Grupul de cooperare poate invita să participe la lucrările sale *Parlamentul European și* reprezentanți ai părților interesate relevante. Comisia asigură secretariatul. (4) Grupului de cooperare îi revin următoarele sarcini: (a) furnizarea de orientări autorităților competente în legătură cu transpunerea și punerea în aplicare a prezentei directive; (b) *furnizarea de orientări autorităților competente în legătură cu elaborarea și punerea în aplicare a politicilor privind divulgarea coordonată a vulnerabilităților, astfel cum se menționează la articolul 7 alineatul (2) litera (c);* (c) schimbul de bune practici și de informații în legătură cu punerea în aplicare a prezentei directive, inclusiv în ceea ce privește amenințările cibernetice, incidentele, vulnerabilitățile, incidentele evitate la limită, inițiativele de sensibilizare, cursurile de formare, exercițiile și competențele, consolidarea capacităților, standardele și specificațiile tehnice*, precum și identificarea entităților esențiale și a entităților importante în temeiul articolului 2 alineatul (2) literele (b)-(e)*; (d) schimbul de opinii și cooperarea cu Comisia cu privire la inițiativele emergente de politică în materie de securitate cibernetică, *precum și coerența generală a cerințelor de securitate cibernetică specifice fiecărui sector*; (e) schimbul de opinii și cooperarea cu Comisia cu privire la proiectele de acte delegate sau de punere în aplicare adoptate în temeiul prezentei directive; (f) schimbul de bune practici și de informații cu instituțiile, organele, oficiile și agențiile relevante ale Uniunii; (g) *schimbul de opinii cu privire la punerea în aplicare a actelor juridice sectoriale ale Uniunii care conțin dispoziții privind securitatea cibernetică;*					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(h) *atunci când este cazul,* discutarea rapoartelor privind evaluarea inter pares menționate la articolul 19 alineatul (9) *și stabilirea de concluzii și recomandări*; (i) *efectuarea unor evaluări coordonate ale riscurilor de securitate la nivelul lanțurilor de aprovizionare critice, în conformitate cu articolul 22 alineatul (1);* (j) discutarea *cazurilor de asistență reciprocă, inclusiv a experiențelor și* rezultatelor acțiunilor comune de supraveghere transfrontaliere, astfel cum se menționează la articolul 37; (k) *la cererea unuia sau a mai multor state membre în cauză, discutarea cererilor specifice de asistență reciprocă astfel cum se menționează la articolul 37;* (l) furnizarea de orientări strategice rețelei CSIRT *și EU-CyCLONe* cu privire la aspecte emergente specifice; (m) *schimbul de opinii cu privire la politica privind acțiunile ulterioare incidentelor de securitate cibernetică de mare amploare și crizelor, pe baza lecțiilor învățate din rețeaua CSIRT și EU-CyCLONe;* (n) contribuția la capacitățile în materie de securitate cibernetică în întreaga Uniune prin facilitarea schimbului de funcționari naționali prin intermediul unui program de consolidare a capacităților care implică personal din cadrul autorităților competente sau al echipelor CSIRT; (o) organizarea de reuniuni comune periodice cu părțile interesate relevante din sectorul privat din întreaga Uniune pentru a discuta activitățile pe care le desfășoară Grupul de cooperare și pentru a colecta informații cu privire la provocările emergente în materie de politici; (p) discutarea activității desfășurate în legătură cu exercițiile de securitate cibernetică, inclusiv a activității desfășurate de ENISA; (q) *stabilirea metodologiei și a aspectelor organizatorice ale evaluărilor inter pares menționate la articolul 19 alineatul (1),*					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
precum și definirea metodologiei de autoevaluare pentru statele membre în conformitate cu articolul 19 alineatul (5), cu sprijinul Comisiei și al ENISA, și, în cooperare cu Comisia și cu ENISA, elaborarea codurilor de conduită care să stea la baza metodelor de lucru ale experților în materie de securitate cibernetică desemnați în conformitate cu articolul 19 alineatul (6); (r) *pregătirea de rapoarte în scopul revizuirii menționate la articolul 40 privind experiența obținută la nivel strategic și din evaluările inter pares;* (s) *discutarea și efectuarea periodică a unei evaluări a situației amenințărilor sau incidentelor cibernetice, cum ar fi ransomware.* *Grupul de cooperare prezintă rapoartele menționate la primul paragraf litera (r) Comisiei, Parlamentului European și Consiliului.* (5) Statele membre asigură cooperarea eficace, eficientă și sigură a reprezentanților lor în Grupul de cooperare. (6) Grupul de cooperare poate solicita rețelei CSIRT un raport tehnic pe anumite teme. (7) Până la 1 februarie 2024 și, ulterior, o dată la doi ani, Grupul de cooperare stabilește un program de lucru cu privire la acțiunile care urmează să fie întreprinse pentru punerea în aplicare a obiectivelor și a sarcinilor sale. (8) Comisia poate adopta acte de punere în aplicare prin care se stabilesc acordurile procedurale necesare pentru funcționarea Grupului de cooperare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2). *Comisia face schimb de opinii și cooperează cu Grupul de cooperare în ceea ce privește proiectele de acte de punere în aplicare menționate la primul paragraf de la*					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
prezentul alineat, în conformitate cu alineatul (4) litera (e). (9) Grupul de cooperare se reunește periodic, și în toate cazurile cel puțin o dată pe an, cu Grupul privind reziliența entităților critice instituit în temeiul Directivei (UE) .../...[52] pentru a promova *și facilita* cooperarea strategică și schimbul de informații.					
Articolul 15. Rețeaua CSIRT (1) Pentru a contribui la dezvoltarea încrederii și pentru a promova cooperarea operațională rapidă și eficace între statele membre, se stabilește o rețea a echipelor naționale CSIRT. (2) Rețeaua echipelor CSIRT este formată din reprezentanți ai echipelor CSIRT *desemnate sau instituite în temeiul articolului 10* și din Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE). Comisia participă la rețeaua CSIRT în calitate de observator. ENISA asigură secretariatul și acordă asistență în mod activ pentru cooperarea între echipele CSIRT. (3) Rețelei CSIRT îi revin următoarele sarcini: (a) schimbul de informații privind capacitățile echipelor CSIRT; (b) *facilitarea partajării, transferului și schimbului de tehnologie și măsuri, politici, instrumente, procese, bune practici și cadre relevante între echipele CSIRT;* (c) schimbul de informații relevante privind incidentele, incidentele evitate la limită, amenințările cibernetice, riscurile și vulnerabilitățile; (d) *schimbul de informații în ceea ce privește publicațiile și recomandările în materie de securitate cibernetică;* (e) *asigurarea interoperabilității în ceea ce privește specificațiile și protocoalele referitoare la schimbul de informații;* (f) la cererea unui *membru* al rețelei CSIRT care ar putea fi afectat de un incident, schimbul de informații și discutarea		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
informațiilor cu privire la incidentul respectiv și la amenințările cibernetice, riscurile și vulnerabilitățile conexe; (g) la cererea unui *membru* al rețelei CSIRT, discutarea și, după caz, punerea în aplicare a unui răspuns coordonat la un incident care a fost identificat în jurisdicția statului membru respectiv; (h) furnizarea de asistență statelor membre în abordarea incidentelor transfrontaliere în temeiul prezentei directive; (i) cooperarea, *schimbul de bune practici și* furnizarea de asistență echipelor CSIRT desemnate drept coordonatori în temeiul articolului 12 alineatul (1) în ceea ce privește gestionarea divulgării coordonate a vulnerabilităților care ar putea avea un impact semnificativ asupra entităților din mai multe state membre; (j) discutarea și identificarea de noi forme de cooperare operațională, inclusiv în legătură cu: (i) categoriile de amenințări cibernetice și incidente; (ii) alertele timpurii; (iii) asistența reciprocă; (iv) principiile și modalitățile de coordonare, ca răspuns la riscuri și incidente transfrontaliere; (v) contribuția la planul național de răspuns la incidente de securitate cibernetică de mare amploare și crize menționat la articolul 9 alineatul (4), *la solicitarea unui stat membru*; (k) informarea Grupului de cooperare cu privire la activitățile sale și cu privire la noi forme de cooperare operațională discutate în temeiul literei (j) și, după caz, solicitarea de orientări în acest sens; (l) bilanțul exercițiilor de securitate cibernetică, inclusiv al celor organizate de ENISA; (m) la cererea unei anumite echipe CSIRT, discutarea capacităților și a nivelului de pregătire al echipei CSIRT respective;					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(n) cooperarea și schimbul de informații cu centrele de operațiuni de securitate la nivel regional și la nivelul Uniunii pentru a îmbunătăți conștientizarea comună a situației cu privire la incidentele și amenințările cibernetice din întreaga Uniune; (o) *atunci când este cazul,* discutarea rapoartelor privind evaluarea *inter pares* menționate la articolul 19 alineatul (9); (p) oferirea de orientări pentru a facilita convergența practicilor operaționale în ceea ce privește aplicarea dispozițiilor prezentului articol referitoare la cooperarea operațională. (4) În termen de ... [24 luni de la data intrării în vigoare a prezentei directive] și, ulterior, o dată la doi ani, rețeaua CSIRT evaluează, în scopul revizuirii menționate la articolul 40, progresele înregistrate în ceea ce privește cooperarea operațională și adoptă un raport. Raportul formulează, în special, concluzii și recomandări pe baza rezultatelor evaluărilor *inter pares* menționate la articolul 19, care sunt efectuate în legătură cu echipele naționale CSIRT. Raportul respectiv se transmite Grupului de cooperare. (5) Rețeaua CSIRT își adoptă regulamentul de procedură. (6) *Rețeaua CSIRT și EU-CyCLONe convin asupra modalităților procedurale și cooperează pe baza acestora.*					
Articolul 16. Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU - CyCLONe) (1) EU-CyCLONe este instituită pentru a sprijini gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor și pentru a asigura schimbul periodic de informații *relevante* între statele membre și instituțiile, organele, oficiile și agențiile Uniunii. (2) EU-CyCLONe este compusă din reprezentanți ai autorităților de gestionare a crizelor *cibernetice* din statele membre,		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
precum și, în cazurile în care un incident de securitate cibernetică de mare amploare potențial sau în curs de desfășurare are sau este probabil să aibă un impact semnificativ asupra serviciilor și activităților care intră în domeniul de aplicare al prezentei directive, reprezentanți ai Comisiei. *În celelalte cazuri, Comisia participă la activitățile EU-CyCLONe în calitate de observator.* ENISA asigură secretariatul *EU-CyCLONe* și sprijină schimbul securizat de informații *și, de asemenea, furnizează instrumentele necesare pentru sprijinirea cooperării dintre statele membre, asigurând schimbul securizat de informații*. *După caz, EU-CyCLONe poate invita să participe la lucrările sale, în calitate de observatori, reprezentanți ai părților interesate relevante.* (3) EU-CyCLONe are următoarele sarcini: (a) consolidarea nivelului de pregătire pentru gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor; (b) dezvoltarea unei conștientizări comune a situației *în cazul incidentelor de securitate cibernetică de mare amploare și al crizelor*; (c) *evaluarea consecințelor și a impactului incidentelor de securitate cibernetică de mare amploare și crizelor relevante și propunerea unor posibile măsuri de atenuare;* (d) coordonarea gestionării incidentelor de securitate cibernetică de mare amploare și a crizelor și sprijinirea procesului decizional la nivel politic în legătură cu astfel de incidente și crize; (e) discutarea, la solicitarea unui stat membru în cauză, a planurilor naționale de răspuns la incidente de securitate cibernetică de mare amploare și crize menționate la articolul 9 alineatul (*4*). (4) EU-CyCLONe își adoptă regulamentul de procedură.					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(5) EU-CyCLONe prezintă periodic rapoarte Grupului de cooperare cu privire la *gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor, precum* și la tendințe, concentrându-se în special pe impactul acestora asupra entităților esențiale și a entităților importante. (6) EU-CyCLONe cooperează cu rețeaua CSIRT pe baza modalităților procedurale convenite *prevăzute la articolul 15 alineatul (6)*. (7) *Până la ... [18 luni de la data intrării în vigoare a prezentei directive] și, ulterior, la fiecare 18 luni, EU-CyCLONe prezintă un raport Parlamentului European și Consiliului în care își evaluează activitatea.*					
Articolul 17. Cooperarea internațională *După caz, Uniunea poate să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaționale cu țări terțe sau organizații internaționale, care să permită și să organizeze participarea acestora la anumite activități ale Grupului de cooperare, ale rețelei CSIRT, precum și ale EU-CyCLONe. Aceste acorduri respectă dreptul Uniunii în materie de protecție a datelor.*		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
Articolul 18. Raportul privind situația în materie de securitate cibernetică în Uniune (1) ENISA adoptă, în cooperare cu Comisia *și Grupul de cooperare*, un raport bienal privind situația în materie de securitate cibernetică în Uniune *și înaintează și prezintă respectivul raport Parlamentului European*. Raportul *este, printre altele, pus la dispoziție într-un format citibil automat și* include *următoarele*: (a) *o evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, ținând seama de situația amenințărilor cibernetice;* (b) *o evaluare a dezvoltării* capacităților în materie de securitate cibernetică *în sectorul public și cel privat* în întreaga Uniune;		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(c) *o evaluare a nivelului general de sensibilizare cu privire la securitatea cibernetică și igiena cibernetică în rândul cetățenilor și entităților, inclusiv al întreprinderilor mici și mijlocii;* (d) *o evaluare globală a* rezultatelor evaluărilor *inter pares* menționate la articolul 19; (e) o evaluare globală a nivelului de maturitate a capacităților *și a resurselor* în materie de securitate cibernetică *în întreaga Uniune, inclusiv a celor de la nivel sectorial, precum și a gradului de aliniere a strategiilor naționale de securitate cibernetică ale statelor membre.* (2) Raportul include recomandări de politică specifice pentru *a aborda deficiențele și* a îmbunătăți nivelul de securitate cibernetică în întreaga Uniune și un rezumat al constatărilor pentru perioada respectivă incluse în rapoartele UE privind situația tehnică în materie de securitate cibernetică cu privire la incidente și amenințări cibernetice, pregătite de ENISA în conformitate cu articolul 7 alineatul (6) din Regulamentul (UE) 2019/881. (3) *ENISA, în cooperare cu Comisia, Grupul de cooperare și rețeaua CSIRT, elaborează metodologia, inclusiv variabilele relevante, cum ar fi indicatori cantitativi și calitativi, pentru evaluarea globală menționată la alineatul (1) litera (e).*					
Articolul 19. Evaluări *inter pares* (1) *Grupul de cooperare stabilește, până la...* [*24 de* luni de la data intrării în vigoare a prezentei directive*], cu sprijinul Comisiei și al* ENISA *și, după caz, al rețelei CSIRT*, metodologia *și aspectele organizatorice ale evaluărilor inter pares pentru 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 ale statelor membre *necesare pentru punerea în aplicare a*		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
prezentei directive. Participarea la evaluările inter pares se face pe bază voluntară. Evaluările *inter pares* sunt efectuate de experți în materie de securitate cibernetică. Experții în materie de securitate cibernetică *sunt desemnați de cel puțin două* state membre, *diferite de statul membru* care face obiectul evaluării. Evaluările *inter pares* acoperă cel puțin *unul din* următoarele elemente: (a) *nivelul* punerii în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare menționate la articolele 21 și 23; (b) nivelul capacităților, inclusiv resursele financiare, tehnice și umane disponibile, precum și eficacitatea exercitării sarcinilor autorităților competente; (c) capacitățile operaționale *ale* echipelor CSIRT; (d) *nivelul de punere în aplicare a* asistenței reciproce menționate la articolul 37; (e) *nivelul de punere în aplicare a* acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la articolul 29; (f) *aspecte specifice de natură transfrontalieră sau transsectorială.* (2) Metodologia menționată la alineatul (1) include criterii obiective, nediscriminatorii, echitabile și transparente pe baza cărora statele membre desemnează experți *în domeniul securității cibernetice* eligibili pentru efectuarea evaluărilor *inter pares*. ENISA și Comisia *participă* în calitate de observatori la evaluările *inter pares*. (3) *Statele* membre *pot identifica aspecte specifice, astfel cum sunt menționate la alineatul (1) litera (f), pentru o evaluare inter pares*. (4) *Înainte de a începe o evaluare inter pares, astfel cum este menționată la alineatul (1), statele membre informează statele membre participante cu privire la domeniul de aplicare*					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
al acesteia, inclusiv aspectele specifice identificate în temeiul alineatului (3). (5) *Înainte de începerea evaluării inter pares, statele membre pot efectua o autoevaluare a aspectelor analizate și furniza autoevaluarea respectivă experților în materie de securitate cibernetică desemnați. Grupul de cooperare, cu sprijinul Comisiei și al ENISA, stabilește metodologia pentru autoevaluarea statelor membre.* (6) Evaluările *inter pares* implică vizite *fizice* sau virtuale și schimburi de informații ex situ. În conformitate cu principiul bunei cooperări, *statul membru supus* evaluării *inter pares* le furnizează experților în materie de securitate cibernetică desemnați informațiile necesare pentru [...]evaluare*, fără a aduce atingere dreptului Uniunii sau intern privind protecția informațiilor confidențiale sau clasificate și protejării funcțiilor esențiale ale statului, cum ar fi securitatea națională. Grupul de cooperare, în colaborare cu Comisia și ENISA, elaborează coduri de conduită adecvate care stau la baza metodelor de lucru ale experților în materie de securitate cibernetică desemnați.* Orice informație obținută prin intermediul evaluării *inter pares* este utilizată exclusiv în acest scop. Experții în materie de securitate cibernetică care participă la evaluarea *inter pares* nu divulgă terților nicio informație sensibilă sau confidențială obținută în cursul evaluării *inter pares* respective. (7) Odată *ce au făcut obiectul unei evaluări inter pares*, *aceleași aspecte* evaluate într-un stat membru nu fac obiectul unei noi evaluări *inter pares* în statul membru respectiv timp de doi ani de la încheierea evaluării *inter pares*, cu excepția cazului în care *statul membru* decide altfel *sau se convine astfel la propunerea Grupului de cooperare*. (8) Statele membre se asigură că orice risc de conflict de interese în ceea ce privește experții în materie de securitate cibernetică desemnați este dezvăluit celorlalte state					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
membre, *Grupului de cooperare*, Comisiei și ENISA*, înainte de începerea evaluării inter pares*. *Statul membru supus evaluării inter pares se poate opune desemnării anumitor experți în materie de securitate cibernetică din motive justificate corespunzător, comunicate statului membru care i-a desemnat.* (9) Experții în materie de securitate cibernetică care participă la evaluări *inter pares* elaborează rapoarte cu privire la constatările și concluziile evaluărilor *inter pares*. *Statele membre care fac obiectul unei evaluări inter pares pot prezenta observații cu privire la proiectele de rapoarte care le privesc, iar aceste observații se anexează la rapoarte. Rapoartele includ recomandări care să faciliteze îmbunătățirea aspectelor acoperite de evaluarea inter pares.* Rapoartele *sunt transmise* Grupului de cooperare și rețelei CSIRT *atunci când este cazul*. *Un stat membru care face obiectul unei evaluări inter pares poate decide să pună la dispoziția publicului raportul său sau o versiune ocultată a acestuia.*					
CAPITOLUL IV. Măsuri de gestionare a riscurilor în materie de securitate cibernetică și obligații de raportare **Articolul 20. Guvernanța** (1) Statele membre se asigură că organele de conducere ale entităților esențiale și ale entităților importante aprobă măsurile de gestionare a riscurilor în materie de securitate cibernetică luate de entitățile respective pentru a se conforma articolului 21, supraveghează punerea în aplicare a acestuia și *pot fi trase la răspundere* pentru încălcarea de către entități a respectivului articol. *Aplicarea prezentului alineat nu aduce atingere dreptului intern în ceea ce privește normele referitoare la răspundere aplicabile instituțiilor publice, precum și răspunderea funcționarilor publici și a funcționarilor aleși sau numiți.*	**Articolul 11. Măsurile de securitate ale rețelelor și sistemelor informatice ale furnizorilor de servicii** (1) Furnizorul de servicii este obligat să aplice continuu măsuri de securitate în scopul: a) prevenirii incidentelor cibernetice; b) soluționării incidentelor cibernetice; c) prevenirii și atenuării impactului asupra continuității serviciului sau a securității rețelei și/sau a sistemului informatic cauzat de un incident cibernetic; d) prevenirii și atenuării unui posibil impact asupra continuității unui serviciu ori rețea sau sistem informatic dependente de cele ale furnizorului de servicii.	Compatibil			Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(2) Statele membre se asigură că membrii organelor de conducere *din cadrul entităților esențiale și al entităților importante au obligația de a urma o* formare pentru a dobândi suficiente cunoștințe și competențe pentru a putea identifica riscurile și a evalua practicile de gestionare a riscurilor în materie de securitate cibernetică și impactul acestora asupra serviciilor pe care le *furnizează* entitatea, *și încurajează entitățile esențiale și entitățile importante să ofere o formare similară tuturor angajaților* în mod regulat. **Articolul 21. Măsuri de gestionare a riscurilor în materie de securitate cibernetică** (1) Statele membre se asigură că entitățile esențiale și entitățile importante iau măsuri tehnice, *operaționale* și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care entitățile respective le utilizează *pentru operațiunile lor sau pentru* a furniza servicii *și pentru a preveni sau reduce la minimum impactul incidentelor asupra beneficiarilor serviciilor lor și asupra altor servicii*. Ținând seama de cele mai avansate standarde în domeniu *și, atunci când este cazul, de standardele europene și internaționale relevante, precum și de costul punerii în aplicare*, măsurile menționate la primul paragraf asigură un nivel de securitate a rețelelor și a sistemelor informatice corespunzător riscurilor prezentate. *Atunci când se evaluează proporționalitatea acestor măsuri, se ține seama în mod corespunzător de gradul de expunere a entității la riscuri, de dimensiunea entității și de probabilitatea producerii incidentelor, precum și de gravitatea acestora, inclusiv de impactul lor societal și economic.* (2) Măsurile menționate la alineatul (1) *se bazează pe o abordare multirisc care vizează*	(2) În procesul aplicării măsurilor de securitate, furnizorul de servicii este obligat: a) să evalueze vulnerabilitățile și riscurile rețelei și sistemului informatic, să determine severitatea impactului unui eventual incident cibernetic survenit urmare a materializării riscurilor, precum și să descrie măsurile pentru soluționarea unui incident cibernetic. b) să ia măsuri tehnice și organizatorice corespunzătoare și proporționale în materie de securitate cibernetică, în conformitate cu standardul descris la alineatul (4) litera (a), pentru a gestiona riscurile legate de securitatea rețelelor și a sistemelor informatice pe care le utilizează în activitatea sa, inclusiv să aplice: - politici referitoare la analiza riscurilor și securitatea rețelelor și sistemelor informatice; - gestionarea incidentelor (prevenire, detectare și răspuns la incidente) - politici și proceduri privind utilizarea criptografiei și a criptării, - politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor de securitate cibernetică, - măsuri privind continuitatea activității, inclusiv gestionarea copiilor de rezervă și recuperarea în caz de dezastru, precum și gestionarea crizelor, - măsuri de securitate aplicate în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice, inclusiv gestionarea vulnerabilităților și divulgarea acestora, - măsuri de securitate a resurselor umane, politici de control al accesului și gestionarea activelor, - măsuri privind securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile dintre				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
protejarea rețelelor și a sistemelor informatice, precum și a mediului fizic al acestor sisteme împotriva incidentelor, și includ cel puțin următoarele: (a) politici referitoare la analiza riscurilor și securitatea sistemelor informatice; (b) gestionarea incidentelor; (c) continuitatea activității, de exemplu gestionarea copiilor de rezervă și recuperarea în caz de dezastru, precum și gestionarea crizelor; (d) securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile dintre fiecare entitate și prestatorii sau furnizorii săi *direcți* de servicii; (e) securitatea în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice, inclusiv gestionarea vulnerabilităților și divulgarea acestora; (f) politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor în materie de securitate cibernetică; (g) *practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice;* (h) *politici și proceduri privind* utilizarea criptografiei și*, după caz,* a criptării; (i) *securitatea resurselor umane, politicile de control al accesului și gestionarea activelor;* (j) *utilizarea de soluții de autentificare multifactor sau de autentificare continuă, de comunicații securizate voce, video și text și de sisteme securizate de comunicații de urgență în cadrul entității, după caz.* (3) Statele membre se asigură că, atunci când analizează care măsuri menționate la alineatul (2) litera (d) de la prezentul articol sunt adecvate, entitățile iau în considerare 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. *Statele membre se*	fiecare entitate și prestatorii sau furnizorii săi direcți de servicii, - practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice, - după caz, utilizarea de soluții de autentificare multifactor sau de autentificare continuă, de comunicații securizate voce, video și text și de sisteme securizate de comunicații de urgență în cadrul furnizorului de servicii,; c) să mențină în stare de actualitate documentația privind măsurile de securitate; d) să asigure monitorizarea în scopul detectării acțiunilor sau produselor TIC care compromit securitatea rețelei sau sistemului informatic; e) să întreprindă măsuri orientate spre reducerea impactului și a răspândirii unui incident cibernetic, inclusiv, dacă este necesar, restricționarea utilizării sau accesului la rețeaua sau sistemul informatic. (3) În cazul în care furnizorul de servicii autorizează un terț să administreze rețeaua și/sau sistemul informatic ori utilizează serviciile unui terț pentru găzduirea sistemului informatic, acesta este responsabil pentru aplicarea măsurilor de securitate a rețelei și/sau sistemului informatic de către terț. (4) În vederea asigurării îndeplinirii obligațiilor prevăzute în prezentul articol și a securității rețelelor și sistemelor informatice ale furnizorilor de servicii, Guvernul: a) prin intermediul organismului național de standardizare și în cooperare cu autoritatea competentă, asigură aprobarea Standardului Moldovenesc în domeniul securității informațiilor, securității cibernetice și protecția				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
asigură, de asemenea, că, atunci când analizează care măsuri menționate la litera respectivă sunt adecvate, entitățile au obligația de a ține seama de rezultatele evaluărilor coordonate ale riscurilor la nivelul lanțurilor de aprovizionare critice efectuate în conformitate cu articolul 22 alineatul (1). (4) Statele membre se asigură că o entitate care constată că nu respectă măsurile prevăzute la alineatul (2) ia, fără întârzieri nejustificate, toate măsurile corective necesare*, adecvate și proporționale*.	confidențialității în baza standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice; b) la propunerea autorității competente, aprobă cerințele specifice privind măsurile de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.				
(5) *Până la ... [21 de luni de la data intrării în vigoare a prezentei directive], Comisia adoptă acte de punere în aplicare de stabilire a cerințelor tehnice și metodologice ale măsurilor menționate la alineatul (2) în ceea ce privește furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere.* Comisia poate adopta acte de punere în aplicare *de stabilire a cerințelor* tehnice și metodologice*, precum și a cerințelor sectoriale, după caz,* ale *măsurilor* menționate la alineatul (2) *în ceea ce privește entitățile esențiale și entitățile importante, altele decât cele menționate la primul paragraf de la prezentul alineat*. Atunci când pregătește actele *de punere în aplicare menționate la primul și al doilea paragraf de la prezentul alineat*, Comisia urmează, în cea mai mare măsură posibilă, standardele europene și internaționale, precum și specificațiile tehnice relevante. *Comisia face schimb de opinii și cooperează cu Grupul de cooperare și ENISA privind proiectele de acte*		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
de punere în aplicare, în conformitate cu articolul 14 alineatul (4) litera (e). *Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).*					
Articolul 22. Evaluări coordonate la nivelul Uniunii ale riscurilor de securitate legate de lanțurile de aprovizionare critice (1) Grupul de cooperare, în cooperare cu Comisia și ENISA, poate efectua evaluări coordonate ale riscurilor în materie de securitate ale anumitor servicii TIC, sisteme TIC sau lanțuri de aprovizionare cu produse TIC critice, ținând seama de factorii de risc de natură tehnică și, după caz, care nu sunt de natură tehnică. (2) Comisia, după consultarea Grupului de cooperare și a ENISA *și, atunci când este necesar, a părților interesate relevante*, identifică serviciile TIC, sistemele TIC sau produsele TIC critice specifice care pot face obiectul evaluării coordonate a riscurilor de securitate menționate la alineatul (1).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
Articolul 23. Obligații de raportare (1) Fiecare stat membru se asigură că entitățile esențiale și entitățile importante notifică, fără întârzieri nejustificate, *echipei CSIRT sau, după caz, autorității sale* competente, în conformitate cu alineatul (4), orice incident care are un impact semnificativ asupra prestării serviciilor lor, astfel cum se menționează la alineatul (3) (incident semnificativ). Dacă este cazul, entitățile în cauză notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor incidentele semnificative care ar putea afecta în mod negativ prestarea serviciilor respective. Fiecare stat membru se asigură că entitățile respective raportează, *inter alia*, orice informație care îi permite *echipei CSIRT* sau, după caz, *autorității* competente să constate orice impact transfrontalier al	**Articolul 12. Obligațiile furnizorilor de servicii de a notifica incidentele cibernetice** (1) Furnizorul de servicii informează imediat autoritatea competentă, dar nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre un incident cibernetic: a) care are un impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului; b) al cărui impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului nu este evident, dar poate fi presupus în mod rezonabil. (2) Furnizorul de servicii, prezintă autorității competente, imediat, dar nu	Compatibil			Viceprim-ministru pentru digitalizare

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
incidentului. *Simpla notificare nu expune entitatea notificatoare unei răspunderi sporite.* *În cazul în care entitățile în cauză notifică autorității competente un incident semnificativ în temeiul primului paragraf, statul membru se asigură că autoritatea competentă „înaintează notificarea echipei CSIRT la primirea acesteia.* *În cazul unui incident semnificativ transfrontalier sau transsectorial, statele membre se asigură că punctele lor unice de contact primesc în timp util informațiile relevante notificate în conformitate cu alineatul (4).* (2) *Dacă este cazul,* statele membre se asigură că entitățile esențiale și entitățile importante *comunică*, fără întârzieri nejustificate, destinatarilor serviciilor lor care ar putea fi afectați de o amenințare cibernetică semnificativă orice măsuri sau măsuri corective pe care destinatarii respectivi le pot lua ca răspuns la amenințarea respectivă. *Dacă este cazul, entitățile informează, de asemenea, destinatarii în cauză despre amenințarea semnificativă propriu-zisă.* (3) Un incident este considerat semnificativ dacă: (a) a provocat sau *poate* provoca perturbări operaționale *grave ale serviciilor* sau pierderi financiare pentru entitatea în cauză; (b) a afectat sau *poate* afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau morale considerabile. (4) Statele membre se asigură că, în scopul notificării în temeiul alineatului (1), entitățile în cauză transmit *echipei CSIRT sau, după caz, autorității* competente: (a) fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care au luat cunoștință de incidentul semnificativ, o *avertizare timpurie* care, după caz, indică dacă există suspiciuni că incidentul *semnificativ* este cauzat de acțiuni ilegale sau răuvoitoare *sau ar putea avea un impact transfrontalier*;	mai târziu de 72 de ore din momentul în care a luat cunoștință despre incidentul cibernetic, o actualizare a informațiilor prezentate în conformitate cu alineatul (1) și o evaluare inițială a incidentului cibernetic cu impact semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili. (3) În cazul în care rețeaua sau sistemul informatic al furnizorului de servicii este administrat și/sau găzduit de un terț, furnizorul de servicii trebuie să se asigure că terțul îl informează în termenii stabiliți la alineatele (1) și (2) despre un incident cibernetic, specificat în alineatul (1) sau că terțul informează concomitent în aceiași termeni autoritatea competentă despre faptul producerii unui astfel de incident cibernetic. (4) Un incident cibernetic are un impact semnificativ dacă este îndeplinită cel puțin una dintre următoarele condiții: a) impactul incidentului cibernetic este sever conform gradului de consecințe determinat în raportul de evaluare a riscurilor rețelei și sistemului informatic întocmit în conformitate cu prevederile articolul 11 alineatului (2) literele a) - c) și a cerințelor prevăzute de actele menționate la articolul 11 alineatul (4); b) din cauza incidentului cibernetic prestarea serviciului este întreruptă pentru o perioadă mai mare decât perioada maximă de timp permisă pentru întrerupere, prevăzută în acordul corespunzător privind nivelul agreat al serviciilor, stabilit în cadrul relațiilor contractuale ale furnizorului de servicii, sau cerințele privind continuitatea serviciului stabilite în documentația prevăzută la articolul 11 alineatul (2) litere a) - c);				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(b) *fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore din momentul în care au luat cunoștință de incidentul semnificativ, o notificare a incidentului, care, după caz, actualizează informațiile menționate la litera (a) și prezintă o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili;* (c) la cererea unei *echipe CSIRT sau, după caz, a* autorității competente, un raport intermediar privind actualizarea relevantă a situației; (d) un raport final, în termen de cel mult o lună de la transmiterea *notificării incidentului* în temeiul literei (*b*), care să includă următoarele elemente: (i) o descriere detaliată a incidentului, inclusiv a gravității și a impactului acestuia; (ii) tipul de amenințare sau de cauză principală care probabil că a declanșat incidentul; (iii) măsurile de atenuare aplicate și în curs*;* (iv) *dacă este cazul, impactul transfrontalier al incidentului;* (e) *în cazul unui incident în desfășurare la momentul prezentării raportului final menționat la litera (d), statele membre se asigură că entitățile în cauză prezintă la momentul respectiv un raport privind progresele înregistrate și un raport final în termen de o lună de la gestionarea incidentului.* *Prin derogare de la primul paragraf, în ceea ce privește incidentele semnificative care afectează prestarea serviciilor sale de încredere, prestatorul de servicii de încredere notifică echipa CSIRT sau, după caz, autoritatea competentă, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care a luat cunoștință de incidentul semnificativ.*	c) continuitatea serviciului unui terț este perturbată de incidentul cibernetic; d) furnizorului de servicii, furnizorului altui serviciu sau utilizatorilor serviciilor le-au fost cauzate sau le-ar putea fi cauzate prejudicii materiale sau non-materiale considerabile din cauza incidentului cibernetic. (5) Furnizorul de servicii este obligat să notifice într-o perioadă rezonabilă de timp, însă nu mai mult de 3 zile: a) persoanele potențial afectate de incidentul cibernetic cu impact semnificativ sau publicul, dacă persoanele afectate nu pot fi notificate individual; b) destinatarii serviciilor lor care ar putea fi afectați de o amenințare cibernetică semnificativă și orice măsuri sau măsuri corective pe care destinatarii respectivi le pot lua ca răspuns la amenințarea respectivă. Dacă este cazul, furnizorii de servicii informează, de asemenea, destinatarii în cauză despre amenințarea semnificativă propriu-zisă. (6) În cazul în care furnizorul de servicii nu realizează obligațiunile de notificare prevăzute de alineatul (5) în termenul respectiv, autoritatea competentă își poate aroga obligația de notificare a persoanelor posibil afectate sau publicul, informând despre aceasta furnizorul de servicii. (7) În cazul soluționării unui incident cibernetic cu impact semnificativ, furnizorul de servicii este obligat, în termen de 30 zile, să transmită autorității competente un raport care să includă cel puțin informații despre cauzele producerii incidentului cibernetic, timpul de soluționare a acestuia, măsurile aplicate și impactul incidentului cibernetic. (8) Procedura de notificare a incidentelor cibernetice, inclusiv				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(5) Echipa CSIRT *sau autoritatea competentă* furnizează, *fără întârzieri nejustificate și, atunci când este posibil*, în termen de 24 de ore de la primirea *alertei timpurii* menționate la alineatul (4) litera (a), un răspuns entității notificatoare, inclusiv un feedback inițial cu privire la incidentul semnificativ și, la cererea entității, orientări *sau instrucțiuni operaționale* privind punerea în aplicare a unor eventuale măsuri de atenuare. În cazul în care echipa CSIRT nu *este destinatarul inițial al notificării menționate* la alineatul (1), orientările sunt furnizate de autoritatea competentă în colaborare cu echipa CSIRT. Echipa CSIRT furnizează sprijin tehnic suplimentar în cazul în care entitatea în cauză solicită acest lucru. În cazul în care se suspectează că incidentul este de natură penală, *echipa CSIRT sau autoritatea competentă* furnizează, de asemenea, orientări privind raportarea incidentului către autoritățile de aplicare a legii. (6) După caz, și în special dacă incidentul semnificativ implică două sau mai multe state membre, *echipa CSIRT*, autoritatea competentă sau *punctul unic de contact* informează*, fără întârzieri nejustificate,* celelalte state membre afectate și ENISA cu privire la incidentul semnificativ. *Aceste informații includ tipul de informații primite în conformitate cu alineatul (4).* Astfel, *echipa CSIRT, autoritatea competentă* sau punctul unic de contact, în conformitate cu dreptul Uniunii sau dreptul intern, protejează interesele de securitate și comerciale ale entității, precum și confidențialitatea informațiilor furnizate. (7) În cazul în care sensibilizarea publicului este necesară pentru a preveni un incident semnificativ sau pentru a gestiona un incident semnificativ în curs sau în cazul în care divulgarea incidentului semnificativ este în alt mod în interesul public, *echipa CSIRT* a unui stat membru *sau, după caz,* autoritatea *sa* competentă, și, după caz,	interacțiunea dintre furnizorul de servicii și autoritatea competentă, modul de stabilire a impactului unui incident cibernetic și formatul informațiilor evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic sunt stabilite de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. (9) Furnizorul de servicii este obligat imediat, însă nu mai târziu de 24 de ore, să notifice autoritatea competentă despre impactul semnificativ al unui incident cibernetic, care a afectat un terț, asupra continuității serviciului său dacă prestarea acestui serviciu depinde de serviciile prestate de acest terț.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
echipele CSIRT *sau autoritățile competente* din alte state membre în cauză pot, după consultarea entității în cauză, să informeze publicul cu privire la incidentul semnificativ sau să solicite entității să facă acest lucru.					
Articolul 23. Obligații de raportare …… (8) La cererea *echipei CSIRT sau* a autorității competente, punctul unic de contact înaintează notificările primite în temeiul *alineatului (1)* punctelor unice de contact din celelalte state membre afectate. (9) Punctul unic de contact transmite ENISA *o dată la trei luni* un raport de sinteză care include date anonimizate și agregate privind incidentele semnificative, incidentele, amenințările cibernetice semnificative și incidentele evitate la limită notificate în conformitate cu alineatul (1) *de la prezentul articol* și cu articolul 30. Pentru a contribui la furnizarea de informații comparabile, ENISA poate adopta orientări tehnice cu privire la parametrii informațiilor care trebuie incluse în raportul de sinteză. *ENISA informează Grupul de cooperare și rețeaua CSIRT cu privire la constatările sale referitoare la notificările primite o dată la șase luni.* (10) Echipele CSIRT sau, după caz, autoritățile competente furnizează autorităților competente în temeiul Directivei (UE).../...[(53)] informații cu privire la incidentele semnificative, incidentele, amenințările cibernetice și incidentele evitate la limită notificate în conformitate cu alineatul (1) de la prezentul articol și cu articolul 30 de către entitățile identificate ca fiind entități critice în temeiul Directivei (UE).../...[+]. (11) Comisia poate adopta acte de punere în aplicare pentru a preciza mai în detaliu tipul de informații, formatul și procedura referitoare la o notificare transmisă în temeiul alineatului (1) *de la prezentul articol și al articolului 30 și*		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
la o comunicare transmisă în temeiul alineatului (2) de la prezentul articol. *Până la ... [21 de luni de la data intrării în vigoare a prezentei directive], Comisia adoptă, în ceea ce privește 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, precum și furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea,* acte de punere în aplicare pentru a preciza mai în detaliu cazurile în care un incident este considerat *a fi* semnificativ, astfel cum se menționează la alineatul (3). *Comisia poate adopta astfel de acte de punere în aplicare și pentru alte entități esențiale și entități importante.* *Comisia face schimb de opinii și cooperează cu Grupul de cooperare privind proiectele de acte de punere în aplicare menționate la primul și al doilea paragraf de la prezentul alineat, în conformitate cu articolul 14 alineatul (4) litera (e).* Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).					
Articolul 24. Utilizarea sistemelor europene de certificare a securității cibernetice (1) Pentru a demonstra conformitatea cu anumite cerințe de la articolul 21, statele membre le pot solicita entităților esențiale și entităților importante să *utilizeze* anumite produse TIC, servicii TIC și procese TIC, *dezvoltate de entități esențiale sau de entități importante ori achiziționate de la părți terțe, care sunt certificate* în cadrul sistemelor europene de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881. *De asemenea, statele membre încurajează entitățile esențiale*	**Articolul 10. Măsurile de securitate ale rețelelor și sistemelor informatice ale furnizorilor de servicii** (4) În vederea asigurării îndeplinirii obligațiilor prevăzute în prezentul articol și a securității rețelelor și sistemelor informatice ale furnizorilor de servicii, Guvernul: a) prin intermediul organismului național de standardizare și în cooperare cu autoritatea competentă, asigură aprobarea Standardului Moldovenesc în domeniul securității informațiilor, securității cibernetice și protecția confidențialității în baza standardelor și	**compatibil**			Institutul național pentru Standardizare Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
și entitățile importante să utilizeze servicii de încredere calificate. (2) Comisia este împuternicită să adopte acte delegate*, în conformitate cu articolul 38, pentru a completa prezenta directivă prin specificarea categoriilor* de entități esențiale *și de entități importante care* au obligația *de a utiliza anumite produse TIC, servicii TIC și procese TIC certificate sau* de a obține un certificat în cadrul *unui sistem european* de certificare a securității cibernetice *adoptat* în temeiul *articolului 49 din Regulamentul (UE) 2019/88*1. *Respectivele* acte delegate se adoptă *atunci când se identifică niveluri insuficiente de securitate cibernetică și includ o perioadă de punere în aplicare*. *Înainte de a adopta astfel de acte delegate, Comisia efectuează o evaluare a impactului și desfășoară consultări în conformitate cu articolul 56 din Regulamentul (UE) 2019/881.* (3) În cazurile în care nu este disponibil niciun sistem european adecvat de certificare a securității cibernetice în sensul alineatului (2) de la prezentul articol, Comisia poate solicita ENISA să pregătească o propunere de sistem în temeiul articolului 48 alineatul (2) din Regulamentul (UE) 2019/881*, după consultarea Grupului de cooperare și a Grupului european pentru certificarea securității cibernetice*.	a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice; b) la propunerea autorității competente, aprobă cerințele specifice privind măsurile de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.				
Articolul 25. Standardizarea (1) Pentru promovarea punerii în aplicare convergente a articolului 21 alineatele (1) și (2), statele membre, fără a impune un anumit tip de tehnologie sau a discrimina în favoarea utilizării acestuia, încurajează utilizarea standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice. (2) ENISA, în cooperare cu statele membre *și, după caz, după consultarea părților interesate relevante,* elaborează avize și orientări în ceea ce privește domeniile tehnice care ar trebui să fie examinate în	**Articolul 10. Măsurile de securitate ale rețelelor și sistemelor informatice ale furnizorilor de servicii** (4) În vederea asigurării îndeplinirii obligațiilor prevăzute în prezentul articol și a securității rețelelor și sistemelor informatice ale furnizorilor de servicii, Guvernul: a) prin intermediul organismului național de standardizare și în cooperare cu autoritatea competentă, asigură aprobarea Standardului Moldovenesc în domeniul securității informațiilor, securității cibernetice și protecția	**Compatibil**		**Suplimentar această prevedere a Directivei va fi transpusă în mod continuu prin aplicarea standardelor și specificațiilor tehnice europene în mod special.**	Institutul național pentru Standardizare Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
legătură cu alineatul (1), precum și în ceea ce privește standardele deja existente, inclusiv standardele naționale, care ar permite reglementarea respectivelor domenii.	confidențialității în baza standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice; b) la propunerea autorității competente, aprobă cerințele specifice privind măsurile de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.				
CAPITOLUL V. JURISDICȚIE ȘI ÎNREGISTRARE **Articolul 26. Jurisdicție și teritorialitate** (1) *Entitățile care intră în domeniul de aplicare al prezentei directive sunt considerate ca fiind sub jurisdicția statului membru în care sunt stabilite, cu următoarele excepții:* (a) *furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului, care se consideră că intră sub jurisdicția statului membru în care își prestează serviciile;* (b) furnizorii de servicii DNS, registrele de nume TLD, *entitățile care furnizează 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, *care* se consideră că se află sub jurisdicția statului membru în care își au sediul principal în Uniune în temeiul alineatului (2); (c) *entitățile administrației publice, care se consideră că intră sub jurisdicția statului membru care le-a instituit.* (2) În sensul prezentei directive, se consideră că o entitate, astfel cum este menționată la alineatul (1) *litera (b),* își are sediul principal din Uniune în statul membru în		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
care se iau *în mod predominant* deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică. Dacă un astfel de stat membru *nu poate fi stabilit sau dacă* astfel de decizii nu sunt luate în Uniune, sediul principal este considerat a fi în statul membru în care *se desfășoară operațiunile de securitate cibernetică*. *Dacă un astfel de stat membru nu poate fi stabilit, sediul principal este considerat a fi în statul membru în care* entitatea în cauză își are sediul cu cel mai mare număr de angajați din Uniune. (3) În cazul în care o entitate, astfel cum este menționată la alineatul (1) *litera (b)*, nu este stabilită în Uniune, dar oferă servicii în Uniune, aceasta desemnează un reprezentant în Uniune. Reprezentantul se stabilește în unul dintre statele membre în care se oferă serviciile. O astfel de entitate se consideră a fi sub jurisdicția statului membru în care este stabilit reprezentantul. În absența unui reprezentant în Uniune desemnat în temeiul prezentului alineat, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității pentru încălcarea prezentei directive. (4) Desemnarea unui reprezentant de către o entitate, astfel cum este menționată la alineatul (1) *litera (b)*, nu aduce atingere acțiunilor în justiție care ar putea fi inițiate împotriva entității înseși. (5) *Statele membre care au primit o cerere de asistență reciprocă în legătură cu o entitate, astfel cum este menționată la alineatul (1) litera (b), pot, în limitele cererii respective, să ia măsuri adecvate de supraveghere și de asigurare a respectării legii în ceea ce privește entitatea în cauză care furnizează servicii sau care are o rețea și un sistem informatic pe teritoriul lor.*					
Articolul 27. Registrul entităților (1) ENISA creează și păstrează un registru al furnizorilor de servicii DNS, registrelor de nume TLD, al entităților care		Norme UE neaplicabile	Transpunerea este condiționată de aderarea		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
prestează servicii de înregistrare a numelor de domenii, al furnizorilor de servicii de cloud computing, al furnizorilor de servicii de centre de date, al furnizorilor de rețele de furnizare de conținut, al furnizorilor de servicii gestionate, al furnizorilor de servicii de securitate gestionate, precum și al furnizorilor de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, *pe baza informațiilor primite de la punctele unice de contact în conformitate cu alineatul (4) La cerere, ENISA permite accesul autorităților competente la registrul respectiv, asigurându-se în același timp că confidențialitatea informațiilor este protejată, după caz*. (2) *Până la ... [24 de luni de la data intrării în vigoare a prezentei directive], statele membre solicită entităților menționate la alineatul (1) să transmită autorităților competente următoarele informații*: (a) denumirea entității; (b) *sectorul, subsectorul relevant și tipul de entitate menționate în anexa I sau II, după caz;* (c) adresa sediului principal al entității și a celorlalte sedii legale ale sale din Uniune sau, dacă nu este stabilită în Uniune, adresa reprezentantului său desemnat în temeiul articolului 26 alineatul (3); (d) datele de contact actualizate, inclusiv adresele de e-mail și numerele de telefon ale *entității și, după caz, ale reprezentantului său desemnat în temeiul articolului 26 alineatul (3)*; (e) *statele membre în care entitatea furnizează servicii; și* (f) *gamele de adrese IP ale entității.* (3) *Statele membre se asigură că* entitățile menționate la alineatul (1) notifică *autorității competente* 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 alineatului *(2)*. (4) *După ce primește informațiile menționate la alineatele (2) și (3), cu excepția*			Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
celor menționate la alineatul (2) litera (f), punctul unic de contact al statului membru în cauză le înaintează către ENISA, fără întârzieri nejustificate. (5) *După caz, informațiile menționate la alineatele (2) și (3) de la prezentul articol se transmit prin mecanismul național menționat la articolul 3 alineatul (4) al patrulea paragraf.*					
Articolul 28. *Baza* de date pentru datele de înregistrare a numelor de domenii (1) Pentru a contribui la securitatea, stabilitatea și reziliența DNS, statele membre *solicită 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. (2) *În sensul alineatului (1),* statele membre *solicită ca baza* de date cu datele de înregistrare a numelor de domenii *să conțină informațiile necesare* pentru identificarea și contactarea titularilor numelor de domenii și a punctelor de contact care administrează numele de domenii în cadrul TLD-urilor. *Informațiile includ:* (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.* (3) Statele membre *solicită ca* registrele *de nume* TLD și entitățile care prestează servicii de înregistrare a numelor de domenii *să dispună* de politici și proceduri, *inclusiv proceduri de verificare,* care să asigure că bazele de date menționate la alineatul (1)	Art. 3 din Legea comunicațiilor electronice nr. 241/2007 Hotărârea ANRCETI nr. 42/2020 privind aprobarea Regulamentului cu privire la gestionarea domeniului de nivel superior .md	**Parțial compatibil**		Autoritățile responsabile naționale urmează să examineze legislația relevantă la acest capitol și, dacă e cazul, să înainteze propunerile de rigoare pentru asigurarea transpunerii în legislația națională a prevederilor respective	ANRCETI Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
conțin informații exacte și complete. Statele membre *solicită ca* aceste politici și proceduri *să fie* puse la dispoziția publicului. (4) Statele membre *solicită ca* registrele *de nume* TLD și entitățile care prestează servicii de înregistrare a numelor de domenii *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. (5) Statele membre *solicită ca* registrele *de nume* TLD și entitățile care prestează servicii de înregistrare a numelor de domenii *să ofere* acces la datele de înregistrare a numelor de domenii specifice în baza unor cereri legale și justificate în mod corespunzător ale solicitanților de acces legitimi, în conformitate cu dreptul Uniunii în materie de protecție a datelor. Statele membre *solicită ca* registrele *de nume* TLD și entitățile care prestează servicii de înregistrare a numelor de domenii *să răspundă* fără întârzieri nejustificate *și, în orice caz, în termen de 72 de ore de la primirea cererilor* de acces. Statele membre *solicită ca* politicile și procedurile de divulgare a unor astfel de date *să fie* puse la dispoziția publicului. (6) *Respectarea obligațiilor prevăzute la alineatele (1)-(5) nu trebuie să ducă la o suprapunere în colectarea datelor de înregistrare a numelor de domenii. În acest scop, statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să coopereze între ele.*					
Capitolul VI. Schimbul de informații **Articolul 29. Acorduri privind schimbul de informații în materie de securitate cibernetică** (1) Statele membre se asigură că entitățile care intră în domeniul de aplicare al prezentei directive *și, după caz, alte entități care nu intră în domeniul de aplicare al prezentei directive* pot face schimb reciproc de informații	**Articolul 16. Schimbul de informații** (1) Furnizorii de servicii și, după caz, alte persoane juridice care nu intră în domeniul de aplicare al prezentei legi pot face schimb reciproc de informații relevante în materie de securitate cibernetică, în mod voluntar, inclusiv de informații referitoare la amenințări	Compatibil		Suplimentar urmează a fi aprobat cadrul normativ de punere în aplicare a aspectelor ce țin de schimbul de informații între furnizorii de servicii și alte persoane juridice interesate, precum și privind condițiile și modul de semnare a unor	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
relevante în materie de securitate cibernetică, *pe bază voluntară*, inclusiv de informații referitoare la amenințări cibernetice, *incidente evitate la limită,* vulnerabilități, *tehnici și proceduri,* indicatori de compromitere, tactici *adversariale*, *informații specifice actorului care generează amenințări,* alerte de securitate cibernetică și *recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice*, în cazul în care un astfel de schimb de informații: (a) vizează prevenirea și detectarea incidentelor, răspunsul la incidente sau redresarea în urma acestora sau atenuarea impactului lor; (b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de *limitare și prevenire* a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare *sau promovarea colaborării dintre entitățile publice și private în domeniul cercetării amenințărilor cibernetice*. (2) Statele membre se asigură că schimbul de informații are loc în cadrul unor comunități ale entităților esențiale și ale entităților importante *și, după caz, ale prestatorilor sau furnizorilor lor de servicii*. Un astfel de schimb este pus în aplicare prin acorduri privind schimbul de informații în materie de securitate cibernetică, în considerarea caracterului potențial sensibil al informațiilor partajate. (3) Statele membre *facilitează instituirea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) de la prezentul articol. Astfel de acorduri pot specifica* elemente operaționale, inclusiv utilizarea platformelor TIC dedicate *și a instrumentelor de automatizare*, conținutul și	cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice, în cazul în care un astfel de schimb de informații: a) vizează prevenirea și detectarea incidentelor, răspunsul la incidente sau redresarea în urma acestora sau atenuarea impactului lor; b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de limitare și prevenire a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare sau promovarea colaborării dintre persoanele juridice de drept public și cel de drept privat în domeniul cercetării amenințărilor cibernetice. (2) Autoritatea competentă intermediază schimbul de informații între persoanele juridice menționate la alineatul (1) prin crearea și gestionarea unor platforme, inclusiv tehnico-tehnologice, și comunități de încredere. Pentru a asigura protecția informațiilor ce au un caracter potențial sensibil, autoritatea competentă facilitează semnarea acordurilor de schimb de informații între participanții la astfel de platforme și comunități. Modul de semnare, conținutul și alte aspecte privind acordurile de schimb de			acorduri de schimb de informații de către autoritățile și instituțiile publice.	

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
condițiile acordurilor privind schimbul de informații. *Atunci când* stabilesc detaliile implicării autorităților publice în astfel de acorduri, *statele membre pot impune condiții cu privire la informațiile puse la dispoziție de autoritățile competente sau de echipele CSIRT*. Statele membre oferă asistență pentru aplicarea unor astfel de acorduri în conformitate cu politicile lor menționate la articolul 7 alineatul (2) litera (h). (4) Statele membre se asigură că entitățile esențiale și entitățile importante informează autoritățile competente cu privire la participarea lor la acordurile privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2), odată cu încheierea unor astfel de acorduri sau, după caz, cu retragerea din astfel de acorduri, după ce retragerea intră în vigoare. (5) ENISA oferă asistență pentru instituirea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) prin schimbul de bune practici și oferind orientări.	informații se stabilesc de autoritatea competentă. (3) Autoritățile și instituțiile publice pot semna acorduri de schimb de informații în materie de securitate cibernetică în condițiile stabilite de regulamentul aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii statului în domeniul securității cibernetice. (4) Furnizorii de servicii sunt obligați să informeze autoritatea competentă despre semnarea sau acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) sau retragerea din astfel de acorduri, în termen de 3 zile din data semnării sau, după caz, a retragerii.				
Articolul 30. Notificarea voluntară a informațiilor relevante (1) Statele membre se asigură că, *pe lângă obligația de notificare prevăzută la articolul 23, notificările pot fi transmise echipelor CSIRT sau, după caz, autorităților competente*, în mod voluntar, *de către:* (a) *entitățile esențiale și entitățile importante,* cu privire la incidente, amenințări cibernetice *și* incidente evitate la limită*;* (b) *alte entități decât cele menționate la litera (a), indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, cu privire la incidente semnificative, amenințări cibernetice și incidente evitate la limită.* (2) Statele membre prelucrează notificările menționate la alineatul (1) de la prezentul articol în conformitate cu procedura prevăzută la articolul 23. Statele membre pot	**Articolul 12. Notificarea voluntară din proiectul de lege** (1) Furnizorii de servicii pot notifica autoritatea competentă cu privire la incidente cibernetice, amenințări cibernetice și incidente evitate la limită. (2) Persoanele juridice de drept public sau de drept privat care nu sunt identificate de autoritatea competentă ca furnizori de servicii pot transmite acesteia notificări cu privire la incidente cibernetice semnificative, amenințări cibernetice și incidente evitate la limită. (3) Notificările menționate la alineatele (1) și (2) din prezentul articol, sunt soluționate de către autoritatea competentă conform procedurilor stabilite de prezenta lege și a actului aprobat în temeiul articolului 12 alineatului (8), acordând prioritate	**Compatibil**			Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
trata notificările obligatorii cu prioritate față de notificările voluntare. *Dacă este necesar, echipele CSIRT și, după caz, autoritățile competente furnizează punctelor unice de contact informațiile despre notificările primite în temeiul prezentului articol, asigurând totodată confidențialitatea și protecția adecvată a informațiilor furnizate de entitatea notificatoare. Fără a aduce atingere prevenirii, investigării, depistării și urmăririi penale a infracțiunilor,* raportarea voluntară nu impune entității notificatoare nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis notificarea.	examinării și soluționării notificărilor obligatorii conform prevederilor prezentei legi și asigurând confidențialitatea și protecția adecvată a informațiilor furnizate de către persoana care a notificat. (4) Notificarea voluntară nu impune persoanelor menționate la alineatele (1) și (2) nicio obligație suplimentară care nu le-ar fi revenit dacă nu ar fi transmis notificarea, exceptând obligațiile care le revin sau le-ar putea reveni conform legislației corespunzătoare în contextul desfășurării acțiunilor de prevenire, investigare, depistare și urmărire penală a infracțiunilor.				
Capitolul VII. Supravegherea și asigurarea respectării legii **Articolul 31. Aspecte generale privind supravegherea și asigurarea respectării legii** (1) Statele membre se asigură că autoritățile lor competente supraveghează în mod eficace și iau măsurile necesare pentru a asigura respectarea *prezentei directive*. (2) *Statele membre pot permite autorităților lor competente să acorde prioritate sarcinilor de supraveghere. O asemenea prioritizare are la bază o abordare bazată pe riscuri. În acest scop, atunci când își exercită sarcinile de supraveghere prevăzute la articolele 32 și 33, autoritățile competente pot stabili metodologii de supraveghere care să permită tratarea cu prioritate a acestor sarcini, urmând o abordare bazată pe riscuri.* (3) Autoritățile competente lucrează în strânsă cooperare cu autoritățile de supraveghere în temeiul Regulamentului (UE) 2016/679 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*.	**Capitolul IV. Supraveghere și control de stat** **Articolul 17. Supravegherea de stat în domeniul securității cibernetice** (1) Autoritatea competentă exercită funcția de supraveghere a respectării prevederilor prezentei legi de către furnizorii de servicii prin monitorizarea continuă a modului în care aceștia realizează obligațiile ce le revin conform prevederilor prezentei legi și a actelor normative de punere în aplicare a acesteia. (2) În cazul în care un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluționeze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluționarea incidentului cibernetic utilizând, dacă este necesar, asistență profesionistă terță. (3) Pentru contracararea unei amenințări grave imediate asupra securității rețelelor și sistemelor informatice sau pentru eliminarea unei perturbări grave în cazul unui incident	Parțial compatibil		Urmează a fi transpus integral prin adoptarea actelor normative de implementare prevăzute la art. 17 alin. (5) și art. 18 alin. (5), precum și în procesul aducerii legislației naționale în concordanță cu prevederile proiectului de lege	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(4) *Fără a aduce atingere cadrelor legislative și instituționale naționale, statele membre se asigură că, în ceea ce privește supravegherea respectării prezentei directive de către entitățile administrației publice și aplicarea de măsuri de asigurare a respectării legii în cazul încălcării prezentei directive, autoritățile competente au competențele corespunzătoare pentru a îndeplini astfel de sarcini cu independență operațională în raport cu entitățile administrației publice care sunt supravegheate. Statele membre pot decide impunerea unor măsuri adecvate, proporționale și efective de supraveghere și de asigurare a respectării legii în ceea ce privește respectivele entități, în conformitate cu cadrele legislative și instituționale naționale.*	cibernetic, autoritatea competentă poate restricționa utilizarea sau accesul la un sistem informatic, dacă sunt îndeplinite cumulativ următoarele condiții: a) incidentul cibernetic compromite sau dăunează securității altei rețele sau sistem informatic; b) administratorul sistemului nu este în măsură sau nu poate în timp util să contracareze amenințarea gravă sau să elimine perturbarea gravă provocată de incidentul cibernetic; c) nu este posibilă contracararea amenințării grave sau eliminarea perturbării grave provocate de incidentul cibernetic prin aplicarea unei alte măsuri; d) nu se provoacă un prejudiciu disproporționat prin contracararea amenințării grave sau prin eliminarea perturbării provenite din incidentul cibernetic. (4) Destinatarul și, în cazul unui furnizor de servicii, autoritatea publică care realizează politica de stat în domeniul respectiv și, dacă e cazul, autoritatea cu funcții regulatorii pe piața din domeniul în care se prestează serviciul respectiv, sunt notificați în cel mai scurt timp însă nu mai târziu de 24 de ore, referitor la aplicarea măsurilor prevăzute la alineatul (3). (5) Modul de aplicare a măsurilor de supraveghere se stabilesc de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. **Articolul 18. Controlul** **(**1) Autoritatea competentă exercită controlul respectării prezentei legi, aplicând următoarele principii: a) legalitatea și respectarea competenței stabilite de lege;				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	b) aplicării doar a sancțiunilor care sunt stabilite de lege; c) tratarea dubiilor în favoarea furnizorului de servicii; d) efectuarea controlului pe cheltuiala statului; e) prescrierea recomandărilor pentru înlăturarea încălcărilor constatate în urma controlului; f) dreptul furnizorului de servicii de a contesta acțiunile autorității competente, inclusiv în instanța judecătorească. (2) Autoritatea competentă realizează controlul respectării prevederilor prezentei legi exclusiv în baza unui act motivat emis în acest scop, în baza evaluării riscurilor pentru securitatea rețelelor și sistemelor informaționale ale furnizorilor de servicii, precum și cu înștiințarea în prealabil a furnizorului de servicii despre controlul preconizat. (3) În vederea efectuării controlului, autoritatea competentă are dreptul să beneficieze de acces la informațiile, bunurile și încăperile deținute de furnizorul de servicii supus controlului, care sunt necesare realizării obiectivelor controlului. (4) Autoritatea competentă efectuează controale numai în cazul în care: a) a depistat și, urmare a unei investigații preliminare, a confirmat fapte de încălcare a prevederilor prezentei legi; și/sau b) a fost sesizată cu privire la încălcări sau îndeplinirea necorespunzătoare a obligațiilor prevăzute de prezenta lege de către furnizorul de servicii. (5) Modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform prezentei legi, se stabilește de Guvern, la propunerea autorității administrației publice centrale de specialitate				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
	responsabile de realizarea politicii de stat în domeniul securității cibernetice.				

Articolul 32. Măsurile de supraveghere și de asigurare a respectării legii în ceea ce privește entitățile esențiale (1) Statele membre se asigură că măsurile de supraveghere sau de asigurare a respectării legii impuse entităților esențiale în ceea ce privește obligațiile prevăzute în prezenta directivă sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte. (2) Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile esențiale, au competența de a supune entitățile respective *cel puțin*: (a) unor inspecții la fața locului și unei supravegheri ex situ, inclusiv unor verificări aleatorii*, realizate de profesioniști cu formare corespunzătoare*; (b) unor audituri *de securitate* periodice *și specifice efectuate de un organism independent sau de o autoritate competentă*; (c) unor audituri *ad hoc, inclusiv în cazurile justificate de un incident semnificativ sau de o încălcare a prezentei directive de către entitatea esențială*; (d) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor*, după caz cu cooperarea entității în cauză*; (e) unor cereri de informații necesare pentru a evalua măsurile de gestionare a riscurilor în materie de securitate cibernetică adoptate de entitatea în cauză, inclusiv politicile de securitate cibernetică documentate, precum și respectarea obligației de a trimite informații *autorităților competente* în temeiul articolului 27; (f) unor cereri de acces la date, la documente și la orice informații necesare pentru îndeplinirea sarcinilor lor de supraveghere; (g) unor cereri de dovezi privind punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și mijloacele de probă care stau la baza acestora.	**Articolul 17. Supravegherea de stat în domeniul securității cibernetice** (1) Autoritatea competentă exercită funcția de supraveghere a respectării prevederilor prezentei legi de către furnizorii de servicii prin monitorizarea continuă a modului în care aceștia realizează obligațiile ce le revin conform prevederilor prezentei legi și a actelor normative de punere în aplicare a acesteia. (2) În cazul în care un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluționeze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluționarea incidentului cibernetic utilizând, dacă este necesar, asistență profesionistă terță. (3) Pentru contracararea unei amenințări grave imediate asupra securității rețelelor și sistemelor informatice sau pentru eliminarea unei perturbări grave în cazul unui incident cibernetic, autoritatea competentă poate restricționa utilizarea sau accesul la un sistem informatic, dacă sunt îndeplinite cumulativ următoarele condiții: a) incidentul cibernetic compromite sau dăunează securității altei rețele sau sistem informatic; b) administratorul sistemului nu este în măsură sau nu poate în timp util să contracareze amenințarea gravă sau să elimine perturbarea gravă provocată de incidentul cibernetic; c) nu este posibilă contracararea amenințării grave sau eliminarea perturbării grave provocate de incidentul cibernetic prin aplicarea unei alte măsuri;	Parțial compatibil		Urmează a fi transpus integral prin adoptarea actelor normative de implementare prevăzute la art. 14 alin. (5) și art. 15 alin. (5), precum și în procesul aducerii legislației naționale în concordanță cu prevederile proiectului de lege	Viceprim-ministru pentru digitalizare Ministerul Economiei

Auditurile de securitate specifice, menționate la primul paragraf litera (b), se bazează pe evaluări ale riscurilor efectuate de autoritatea competentă sau de entitatea auditată sau pe alte informații disponibile legate de riscuri. *Rezultatele oricărui audit de securitate specific se pun la dispoziția autorității competente. Costurile unui astfel de audit de securitate specific efectuat de un organism independent sunt plătite de entitatea auditată, în afara cazurilor justificate corespunzător, atunci când autoritatea competentă decide altfel.* (3) Atunci când își exercită competențele în temeiul alineatului (2) literele (e), (f) sau (g), autoritățile competente precizează scopul solicitării și informațiile solicitate. (4) Statele membre se asigură că, atunci când își exercită competențele de asigurare a respectării legii în ceea ce privește entitățile esențiale, autoritățile lor competente au competența *cel puțin*: (a) de a emite avertismente cu privire la încălcări ale prezentei directive de către entitățile în cauză; (b) de a adopta instrucțiuni obligatorii, *inclusiv în ceea ce privește măsurile necesare pentru a preveni sau remedia un incident, precum și termene-limită pentru punerea în aplicare a acestor măsuri și pentru a raporta cu privire la punerea lor în aplicare,* sau un ordin prin care le solicită entităților în cauză să remedieze deficiențele identificate sau încălcările prezentei directive; (c) de a dispune ca entitățile în cauză să înceteze conduita prin care încalcă prezenta directivă și să se abțină de la repetarea conduitei respective; (d) de a dispune ca entitățile în cauză să asigure că măsurile lor de gestionare a riscurilor în materie de securitate cibernetică respectă dispozițiile de la articolul 21 sau să îndeplinească obligațiile de raportare prevăzute la articolul 23, într-un anumit mod și într-o anumită perioadă; (e) de a dispune ca entitățile în cauză să informeze persoanele fizice sau juridice cu	d) nu se provoacă un prejudiciu disproporționat prin contracararea amenințării grave sau prin eliminarea perturbării provenite din incidentul cibernetic. (4) Destinatarul și, în cazul unui furnizor de servicii, autoritatea publică care realizează politica de stat în domeniul respectiv și, dacă e cazul, autoritatea cu funcții regulatorii pe piața din domeniul în care se prestează serviciul respectiv, sunt notificați în cel mai scurt timp însă nu mai târziu de 24 de ore, referitor la aplicarea măsurilor prevăzute la alineatul (3). (5) Modul de aplicare a măsurilor de supraveghere se stabilesc de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. **Articolul 18. Controlul** (1) Autoritatea competentă exercită controlul respectării prezentei legi, aplicând următoarele principii: a) legalitatea și respectarea competenței stabilite de lege; b) aplicării doar a sancțiunilor care sunt stabilite de lege; c) tratarea dubiilor în favoarea furnizorului de servicii; d) efectuarea controlului pe cheltuiala statului; e) prescrierea recomandărilor pentru înlăturarea încălcărilor constatate în urma controlului; f) dreptul furnizorului de servicii de a contesta acțiunile autorității competente, inclusiv în instanța judecătorească.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
privire la care furnizează servicii sau desfășoară activități care sunt potențial afectate de o amenințare cibernetică semnificativă cu privire la *caracterul amenințării, precum și cu privire la* toate măsurile de protecție sau de remediere pe care le-ar putea lua persoanele fizice sau juridice în cauză ca răspuns la amenințarea respectivă; (f) de a dispune ca entitățile în cauză să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil; (g) de a desemna un ofițer de monitorizare cu sarcini bine definite pe o perioadă determinată de timp pentru a supraveghea respectarea de către entitățile în cauză a articolelor 21 și 23; (h) de a dispune ca entitățile în cauză să facă publice într-un mod specific aspectele legate de încălcări ale prezentei directive; (i) de a aplica sau a solicita aplicarea de către organismele sau instanțele relevante, în conformitate cu dreptul intern, a unei amenzi administrative în temeiul articolului 34, în plus față de *oricare dintre* măsurile menționate la literele (a)-(*h*) de la prezentul alineat. (5) În cazul în care măsurile de asigurare a respectării legii adoptate în temeiul alineatului (4) literele (a)-(d) și (f) sunt ineficiente, statele membre se asigură că autoritățile lor competente au competența de a stabili un termen în care entității esențiale i se solicită să ia măsurile necesare pentru remedierea deficiențelor sau să respecte cerințele autorităților respective. În cazul în care acțiunea solicitată nu este întreprinsă în termenul stabilit, statele membre se asigură că autoritățile competente au competența: (a) de a suspenda *temporar* sau de a solicita unui organism de certificare sau de autorizare *sau unei instanțe, în conformitate cu dreptul intern,* suspendarea *temporară a* unei certificări sau a unei autorizații privind o parte sau toate serviciile sau	(2) Autoritatea competentă realizează controlul respectării prevederilor prezentei legi exclusiv în baza unui act motivat emis în acest scop, în baza evaluării riscurilor pentru securitatea rețelelor și sistemelor informaționale ale furnizorilor de servicii, precum și cu înștiințarea în prealabil a furnizorului de servicii despre controlul preconizat. (3) În vederea efectuării controlului, autoritatea competentă are dreptul să beneficieze de acces la informațiile, bunurile și încăperile deținute de furnizorul de servicii supus controlului, care sunt necesare realizării obiectivelor controlului. (4) Autoritatea competentă efectuează controale numai în cazul în care: a) a depistat și, urmare a unei investigații preliminare, a confirmat fapte de încălcare a prevederilor prezentei legi; și/sau b) a fost sesizată cu privire la încălcări sau îndeplinirea necorespunzătoare a obligațiilor prevăzute de prezenta lege de către furnizorul de servicii. (5) Modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform prezentei legi, se stabilește de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
activitățile *relevante* furnizate de o entitate esențială; (b) de a solicita impunerea de către organismele sau instanțele relevante, în conformitate cu dreptul intern, a unei interdicții temporare de a exercita funcții de conducere în cadrul entității respective împotriva oricărei persoane fizice care exercită responsabilități de conducere la nivel de director executiv sau de reprezentant legal în entitatea esențială. *Suspendările sau interdicțiile temporare impuse în temeiul prezentului alineat* se aplică numai până în momentul în care entitatea *în cauză* ia măsurile necesare în vederea remedierii deficiențelor sau a respectării cerințelor impuse de autoritatea competentă pentru care au fost aplicate aceste măsuri de asigurare a respectării legii. *Impunerea unor astfel de suspendări sau interdicții temporare face obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu carta, inclusiv dreptul la o cale de atac eficace și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare.* *Măsurile de asigurare a respectării legii prevăzute la prezentul alineat nu se aplică entităților administrației publice care intră în domeniul de aplicare al prezentei directive.* (6) Statele membre se asigură că orice persoană fizică responsabilă de o entitate esențială sau care acționează în calitate de reprezentant legal al unei entități esențiale pe baza competenței de a o reprezenta, a autorității de a lua decizii în numele acesteia sau a autorității de a exercita controlul asupra acesteia are competența de a se asigura că aceasta respectă prezenta directivă. Statele membre se asigură că aceste persoane fizice pot fi trase la răspundere pentru încălcarea obligațiilor care le revin de a asigura respectarea prezentei directive. *În ceea ce privește entitățile administrației publice, prezentul alineat nu aduce atingere dreptului intern în ceea ce privește*					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
răspunderea funcționarilor publici și a funcționarilor aleși sau numiți. (7) Atunci când iau oricare dintre măsurile de asigurare a respectării legii menționate la alineatul (4) sau (5), autoritățile competente respectă dreptul la apărare, iau în considerare circumstanțele fiecărui caz în parte și țin seama în mod corespunzător cel puțin de: (a) gravitatea încălcării și importanța dispozițiilor încălcate, următoarele fiind considerate, printre altele, încălcări grave în orice situație: (i) încălcări repetate; (ii) o neîndeplinire a obligației de notificare sau de remediere a incidentelor semnificative; (iii) o neremediere a deficiențelor în urma instrucțiunilor obligatorii din partea autorităților competente; (iv) obstrucționarea auditurilor sau a activităților de monitorizare dispuse de autoritatea competentă în urma constatării unei încălcări; (v) furnizarea de informații false sau vădit denaturate în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate cibernetică sau obligațiile de raportare prevăzute la articolele 21 și 23; (b) durata încălcării; (c) *orice încălcare anterioară relevantă comisă de entitatea în cauză;* (d) orice prejudicii materiale sau morale cauzate, *inclusiv* pierderile financiare sau economice, efectele asupra altor servicii și numărul de utilizatori afectați; (e) orice intenție sau neglijență din partea autorului încălcării; (f) orice măsuri luate de entitate pentru a preveni sau a atenua prejudiciile materiale sau morale; (g) orice aderare la coduri de conduită aprobate sau la mecanisme de certificare aprobate;					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(h) măsura în care persoanele fizice sau juridice declarate responsabile cooperează cu autoritățile competente. (8) Autoritățile competente prezintă o motivare detaliată a măsurilor lor de asigurare a respectării legii. Înainte de a adopta astfel de măsuri, autoritățile competente notifică entităților în cauză constatările lor preliminare. *De asemenea, acestea* acordă entităților respective un termen rezonabil să prezinte observații, *cu excepția cazurilor justificate în mod corespunzător, când ar fi împiedicată o acțiune imediată pentru a preveni sau răspunde la incidente*.					
(9) Statele membre se asigură că autoritățile lor competente *în temeiul prezentei directive* informează autoritățile competente relevante *din același stat membru* în temeiul Directivei (UE) .../...(54) atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea de către o entitate identificată ca fiind entitate critică în temeiul Directivei (UE) .../...+ a prezentei directive. *După caz,* autoritățile competente în temeiul Directivei (UE) .../...+ *pot solicita* autorităților competente *în temeiul prezentei directive* să își exercite competențele de supraveghere și de asigurare a respectării legii *în legătură cu* o entitate care este identificată ca fiind entitate critică *în temeiul Directivei (UE) .../...+*. (10) *Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive cooperează cu autoritățile competente relevante din statul membru în cauză în temeiul Regulamentului (UE) .../...(55). În special, statele membre se asigură că autoritățile lor competente în temeiul prezentei directive informează Forumul de supraveghere instituit în temeiul articolului 32 alineatul (1) din Regulamentul (UE) .../...++ atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea prezentei directive de către o*		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
entitate esențială, care este desemnată ca fiind un furnizor terț de servicii TIC critice în temeiul articolului 31 din Regulamentul (UE) .../....[++].					
Articolul 33. Măsuri de supraveghere și de asigurare a respectării legii în ceea ce privește entitățile importante (1) Atunci când li se furnizează dovezi, indicii *sau informații* că o entitate importantă *nu ar respecta* prezenta directivă, în special articolele 21 și 23, statele membre se asigură că autoritățile competente iau măsuri, dacă este necesar, prin intermediul unor măsuri de supraveghere *ex post*. *Statele membre se asigură că aceste măsuri sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte.* (2) Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile importante, au competența de a supune entitățile respective *cel puțin*: (a) unor inspecții la fața locului și unei supravegheri *ex situ ex post realizate de profesioniști cu formare corespunzătoare*; (b) unor audituri de securitate specifice *efectuate de un organism independent sau de o autoritate competentă*; (c) unor scanări de securitate bazate pe criterii obiective, *nediscriminatorii*, echitabile și transparente de evaluare a riscurilor*, după caz cu cooperarea entității în cauză*; (d) unor cereri de informații necesare pentru a evalua, *ex post*, măsurile de gestionare a riscurilor în materie de securitate cibernetică adoptate de entitatea în cauză, inclusiv politicile de securitate cibernetică documentate, precum și respectarea obligației de a transmite informații *autorităților competente* în temeiul articolului 27; (e) unor cereri de acces la date, la documente și la informații necesare pentru îndeplinirea sarcinilor lor de supraveghere; (f) *unor cereri de dovezi privind punerea în aplicare a politicilor în materie de securitate*	**Articolul 17. Supravegherea de stat în domeniul securității cibernetice** (1) Autoritatea competentă exercită funcția de supraveghere a respectării prevederilor prezentei legi de către furnizorii de servicii prin monitorizarea continuă a modului în care aceștia realizează obligațiile ce le revin conform prevederilor prezentei legi și a actelor normative de punere în aplicare a acesteia. (2) În cazul în care un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluționeze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluționarea incidentului cibernetic utilizând, dacă este necesar, asistență profesionistă terță. (3) Pentru contracararea unei amenințări grave imediate asupra securității rețelelor și sistemelor informatice sau pentru eliminarea unei perturbări grave în cazul unui incident cibernetic, autoritatea competentă poate restricționa utilizarea sau accesul la un sistem informatic, dacă sunt îndeplinite cumulativ următoarele condiții: a) incidentul cibernetic compromite sau dăunează securității altei rețele sau sistem informatic; b) administratorul sistemului nu este în măsură sau nu poate în timp util să contracareze amenințarea gravă sau să elimine perturbarea gravă provocată de incidentul cibernetic; c) nu este posibilă contracararea amenințării grave sau eliminarea perturbării grave provocate de incidentul	Parțial compatibil		Urmează a fi transpus integral prin aprobarea cadrului normativ de implementare a prevederilor noii legi	Viceprim-ministru pentru digitalizare

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și mijloacele de probă care stau la baza acestora. *Auditurile de securitate specifice, menționate la primul paragraf litera (b), se bazează pe evaluări ale riscurilor efectuate de autoritatea competentă sau de entitatea auditată sau pe alte informații disponibile legate de riscuri.* *Rezultatele oricărui audit de securitate specific se pun la dispoziția autorității competente. Costurile unui astfel de audit de securitate specific efectuat de un organism independent sunt plătite de entitatea auditată, în afara cazurilor justificate corespunzător, atunci când autoritatea competentă decide altfel.* (3) Atunci când își exercită competențele în temeiul alineatului (2) literele (d), (e) *sau* (f), autoritățile competente precizează scopul solicitării și informațiile solicitate. (4) Statele membre se asigură că, atunci când își exercită sarcinile de asigurare a respectării legii în ceea ce privește entitățile importante, autoritățile competente au competența *cel puțin*: (a) de a emite avertismente cu privire la încălcări ale prezentei directive de către entitățile în cauză ; (b) de a adopta instrucțiuni obligatorii sau un ordin prin care le solicită entităților în cauză să remedieze deficiențele identificate sau încălcarea prezentei directive; (c) de a dispune ca entitățile în cauză să înceteze conduita prin care încalcă prezenta directivă și să se abțină de la repetarea conduitei respective; (d) de a dispune ca entitățile în cauză să asigure că măsurile lor de gestionare a riscurilor în materie de securitate cibernetică respectă dispozițiile de la articolul 21 sau să îndeplinească obligațiile de raportare prevăzute la articolul 23, într-un anumit mod și într-o anumită perioadă;	cibernetic prin aplicarea unei alte măsuri; d) nu se provoacă un prejudiciu disproporționat prin contracararea amenințării grave sau prin eliminarea perturbării provenite din incidentul cibernetic. (4) Destinatarul și, în cazul unui furnizor de servicii, autoritatea publică care realizează politica de stat în domeniul respectiv și, dacă e cazul, autoritatea cu funcții regulatorii pe piața din domeniul în care se prestează serviciul respectiv, sunt notificați în cel mai scurt timp însă nu mai târziu de 24 de ore, referitor la aplicarea măsurilor prevăzute la alineatul (3). (5) Modul de aplicare a măsurilor de supraveghere se stabilesc de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. **Articolul 18. Controlul** **(**1) Autoritatea competentă exercită controlul respectării prezentei legi, aplicând următoarele principii: a) legalitatea și respectarea competenței stabilite de lege; b) aplicării doar a sancțiunilor care sunt stabilite de lege; c) tratarea dubiilor în favoarea furnizorului de servicii; d) efectuarea controlului pe cheltuiala statului; e) prescrierea recomandărilor pentru înlăturarea încălcărilor constatate în urma controlului; f) dreptul furnizorului de servicii de a contesta acțiunile autorității competente, inclusiv în instanța judecătorească. (2) Autoritatea competentă realizează controlul respectării prevederilor prezentei legi exclusiv în baza unui act				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(e) de a dispune ca entitățile în cauză să informeze persoanele fizice sau juridice cu privire la care furnizează servicii sau desfășoară activități care sunt potențial afectate de o amenințare cibernetică semnificativă cu privire la *caracterul amenințării, precum și cu privire la* toate măsurile de protecție sau de remediere pe care le-ar putea lua persoanele fizice sau juridice în cauză ca răspuns la amenințarea respectivă; (f) de a dispune ca entitățile în cauză să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil; (g) de a dispune ca entitățile în cauză să facă publice într-un mod specific aspectele legate de încălcările prezentei directive; (h) de a aplica sau a solicita aplicarea de către organismele sau instanțele relevante, în conformitate cu dreptul intern, a unei amenzi administrative în temeiul articolului 34, în plus față de *oricare dintre* măsurile menționate la literele (a)-(*g*) de la prezentul alineat. (5) Articolul 32 alineatele (6), (7) și (8) se aplică, *mutatis mutandis*, măsurilor de supraveghere și de asigurare a respectării legii prevăzute în prezentul articol pentru entitățile importante.	motivat emis în acest scop, în baza evaluării riscurilor pentru securitatea rețelelor și sistemelor informaționale ale furnizorilor de servicii, precum și cu înștiințarea în prealabil a furnizorului de servicii despre controlul preconizat. (3) În vederea efectuării controlului, autoritatea competentă are dreptul să beneficieze de acces la informațiile, bunurile și încăperile deținute de furnizorul de servicii supus controlului, care sunt necesare realizării obiectivelor controlului. (4) Autoritatea competentă efectuează controale numai în cazul în care: a) a depistat și, urmare a unei investigații preliminare, a confirmat fapte de încălcare a prevederilor prezentei legi; și/sau b) a fost sesizată cu privire la încălcări sau îndeplinirea necorespunzătoare a obligațiilor prevăzute de prezenta lege de către furnizorul de servicii. (5) Modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform prezentei legi, se stabilește de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.				
(6) *Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive cooperează cu autoritățile competente relevante din statul membru în cauză în temeiul Regulamentului (UE) .../...(56). În special, statele membre se asigură că autoritățile lor competente în temeiul prezentei directive informează Forumul de supraveghere instituit în temeiul articolului 32 alineatul (1) din Regulamentul (UE) .../...++ atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea prezentei directive de către o*		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
entitate importantă, care este desemnată ca fiind un furnizor terț de servicii TIC critice în temeiul articolului 31 din Regulamentul (UE) .../....[++].					
Articolul 34. Condiții generale pentru aplicarea de amenzi administrative entităților esențiale și entităților importante (1) Statele membre se asigură că amenzile administrative aplicate entităților esențiale și entităților importante în temeiul prezentului articol în ceea ce privește încălcările prezentei directive sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte. (2) Amenzile administrative sunt aplicate în plus față de *oricare dintre măsurile* menționate la articolul 32 alineatul (4) literele (a)-(*h*), la articolul 32 alineatul (5) și la articolul 33 alineatul (4) literele (a)-(*g*). (3) Atunci când se ia decizia de a aplica o amendă administrativă și se decide cuantumul acesteia în fiecare caz în parte, se acordă atenția cuvenită cel puțin elementelor prevăzute la articolul 32 alineatul (7). (4) Statele membre se asigură că, atunci când încalcă articolul 21 sau articolul 23, *entitățile esențiale* sunt supuse, în conformitate cu alineatele (2) și (3) din prezentul articol, unor amenzi administrative având o limită superioară de cel puțin 10 000 000 EUR sau o limită superioară de cel puțin 2 % din cifra de afaceri mondială totală anuală, înregistrată în exercițiul financiar precedent, a întreprinderii căreia îi aparține entitatea esențială, luându-se în considerare valoarea cea mai mare dintre acestea. (5) *Statele membre se asigură că, atunci când încalcă articolul 21 sau articolul 23, entitățile importante sunt supuse, în conformitate cu alineatele (2) și (3) din prezentul articol, unor amenzi administrative având o limită superioară de cel puțin 7 000 000 EUR sau având o limită superioară de cel puțin 1,4 % din cifra de afaceri mondială totală anuală, înregistrată în exercițiul*	**Articolul 7 din proiectul de lege:** **(3)** Autoritatea competentă exercită următoarele atribuții principale: ..... h) exercită, atribuțiile organului constatator pentru cauze contravenționale în domeniul securității rețelelor și sistemelor informatice în conformitate cu prevederile Codului contravențional	Compatibil parțial		Urmează a fi transpus în procesul elaborării, promovării și aprobării actului normativ de aducere a legislației în concordanță cu prevederile noii legi.	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
financiar precedent, a întreprinderii căreia îi aparține entitatea importantă, luându-se în considerare valoarea cea mai mare dintre acestea. (6) Statele membre pot prevedea competența de a aplica penalități cu titlu cominatoriu pentru a obliga o entitate esențială sau o entitate importantă să înceteze o încălcare a prezentei directive în conformitate cu o decizie prealabilă a autorității competente. (7) Fără a aduce atingere competențelor autorităților competente menționate la articolele 32 și 33, fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi aplicate amenzi administrative entităților administrației publice cărora le revin obligațiile prevăzute în prezenta directivă. (8) *În cazul în care sistemul juridic al unui stat membru nu prevede amenzi administrative, statul membru respectiv se asigură că prezentul articol este aplicat astfel încât amenda să fie inițiată de autoritatea competentă și aplicată de instanțele naționale competente, garantându-se, în același timp, faptul că aceste căi de atac sunt eficiente și că au un efect echivalent cu cel al amenzilor administrative aplicate de autoritățile competente. În orice caz, amenzile aplicate sunt efective, proporționale și cu efect de descurajare. Statele membre informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul prezentului alineat până la ... [21 de luni de la data intrării în vigoare a prezentei directive], precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.*					
Articolul 35. Încălcări care implică o încălcare a securității datelor cu caracter personal (1) În cazul în care*, în cursul supravegherii sau al asigurării respectării legii*, autoritățile competente *iau cunoștință de faptul* că încălcarea de către o entitate esențială	**Articolul 18. Protecția datelor cu caracter personal** În cazul în care, procesul exercitării funcției de supraveghere și control autoritatea competentă ia cunoștință de faptul că o încălcare de către un furnizor de servicii a obligațiilor	Parțial compatibil		Prevederile alineatului (2) din Directivă urmează a fi transpuse în procesul de ajustare a cadrului normativ, în mod special a Codului Contravențional	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
sau de către o entitate importantă a obligațiilor prevăzute la articolele 21 și 23 *din prezenta directivă* poate atrage după sine o încălcare a securității datelor cu caracter personal, astfel cum este definită la articolul 4 alineatul (12) din Regulamentul (UE) 2016/679, care trebuie notificată în temeiul articolului 33 din regulamentul respectiv, acestea informează *fără întârzieri nejustificate* autoritățile de supraveghere menționate la articolele 55 sau 56 din regulamentul respectiv. (2) În cazul în care autoritățile de supraveghere menționate la articolele 55 sau 56 din Regulamentul (UE) 2016/679 aplică o amendă administrativă în temeiul articolului 58 *alineatul (2)* litera (i) din regulamentul respectiv, autoritățile competente nu aplică o amendă administrativă în conformitate cu articolul 34 din prezenta directivă pentru *o* încălcare menționată la alineatul (1) din prezentul articol rezultată *în urma aceluiași comportament* care a făcut obiectul amenzii administrative în temeiul articolului 58 alineatul (2) litera (i) din Regulamentul (UE) 2016/679. Cu toate acestea, autoritățile competente pot aplica măsurile de asigurare a respectării legii prevăzute la articolul 32 alineatul (4) literele (a)-(*h*), la articolul 32 alineatul (5) și la articolul 33 alineatul (4) literele (a)-(*g*) din prezenta directivă.	prevăzute de prezenta lege poate atrage după sine o încălcare a legislației privind protecția datelor cu caracter personal, autoritatea competentă informează imediat organul de control al prelucrărilor de date cu caracter personal.				
(3) În cazul în care autoritatea de supraveghere competentă în temeiul Regulamentului (UE) 2016/679 este stabilită într-un alt stat membru decât autoritatea competentă, autoritatea competentă *informează* autoritatea de supraveghere stabilită în statul său membru cu privire la potențiala încălcare a securității datelor menționată la alineatul (1).		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
Articolul 36. Sancțiuni Statele membre adoptă normele privind sancțiunile care se aplică în cazul nerespectării	**Articolul 7 din proiectul de lege:** (3) Autoritatea competentă exercită următoarele atribuții principale:	Parțial compatibil		Prevederile art. 36 al Directivei urmează a fi adițional implementate prin	Viceprim-ministru pentru digitalizare

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
măsurilor naționale adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a asigura aplicarea acestora. Sancțiunile trebuie să fie efective, proporționale și cu efect de descurajare. Statele membre notifică aceste norme și aceste măsuri Comisiei până la …[*24 de luni* de la data intrării în vigoare a prezentei directive] și notifică acesteia, fără întârziere, orice modificare ulterioară a acestora.	..... g) exercită, atribuțiile organului constatator pentru cauze contravenționale în domeniul securității rețelelor și sistemelor informatice în conformitate cu prevederile Codului contravențional			adoptarea modificărilor la Codul contravențional al Republicii Moldova	Ministerul Economiei
Articolul 37. Asistență reciprocă (1) Dacă o entitate *furnizează servicii în mai multe state membre sau furnizează servicii în unul sau mai multe state membre iar* rețeaua și sistemele sale informatice sunt situate în unul sau mai multe alte state membre, autoritățile competente ale *statelor membre în cauză* cooperează și își oferă asistență reciprocă, după caz. Această cooperare implică cel puțin următoarele: (a) autoritățile competente care aplică măsuri de supraveghere sau de asigurare a respectării legii într-un stat membru informează și consultă, prin intermediul punctului unic de contact, autoritățile competente din celelalte state membre în cauză cu privire la măsurile de supraveghere și de asigurare a respectării legii luate; (b) o autoritate competentă poate solicita unei alte autorități competente să ia *măsuri* de supraveghere sau de asigurare a respectării legii; (c) la primirea unei cereri motivate din partea altei autorități competente, o autoritate competentă acordă asistență reciprocă celeilalte autorități competente *proporțional cu resursele sale, astfel încât măsurile de supraveghere sau de asigurare a respectării legii* să poată fi puse în aplicare într-un mod eficace, eficient și consecvent. Asistența reciprocă menționată la primul paragraf litera (c) poate acoperi cererile de informații și măsurile de supraveghere, inclusiv cererile de efectuare a unor inspecții la fața		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
locului, a unei supravegheri ex situ sau a unor audituri de securitate specifice. O autoritate competentă căreia i se adresează o cerere de asistență nu refuză cererea respectivă, cu excepția cazului în care se stabilește că nu are competența de a furniza asistența solicitată, asistența solicitată nu este proporțională cu sarcinile de supraveghere ale autorității competente *sau cererea privește informații sau implică activități care, dacă ar fi divulgate sau desfășurate, ar fi contrare intereselor esențiale ale statului membru respectiv în materie de securitate națională, siguranță publică sau apărare*. Înainte de a refuza o astfel de cerere, autoritatea competentă consultă celelalte autorități competente în cauză, precum și, *la cererea unuia dintre statele membre în cauză,* Comisia *și ENISA*. (2) Dacă este cazul și de comun acord, autorități competente din diferite state membre pot desfășura acțiuni comune de supraveghere					
Capitolul VIII. Acte delegate și acte de punere în aplicare **Articolul 38. Exercitarea delegării de competențe** (1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol. (2) Competența de a adopta acte delegate menționată la articolul 24 alineatul (2) se conferă Comisiei pe o perioadă de cinci ani de la... [*data intrării în vigoare a prezentei directive*]. (3) Delegarea de competențe menționată la articolul 24 alineatul (2) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare. (5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului. (6) Un act delegat adoptat în temeiul articolului 24 alineatul (2) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu, sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.					
Articolul 39. Procedura comitetului (1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011. (2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011. (3) În cazul în care avizul comitetului urmează să fie obținut prin procedură scrisă, respectiva procedură se încheie fără rezultat atunci când, în termenul stabilit pentru emiterea avizului, președintele comitetului decide în acest sens sau un membru al comitetului solicită acest lucru.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
Capitolul IX. dispoziții finale **Articolul 40. Revizuirea** *Până la ... [57 de luni de la data intrării în vigoare a prezentei directive] și, ulterior, la fiecare 36 de luni,* Comisia revizuiește funcționarea prezentei directive și prezintă un raport Parlamentului European și Consiliului. Raportul evaluează în special relevanța dimensiunii entităților vizate și sectoarele, subsectoarele și tipurile de entități menționate		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
în anexele I și II pentru funcționarea economiei și a societății în ceea ce privește securitatea cibernetică. *În acest scop* și în vederea intensificării cooperării strategice și operaționale, Comisia ține cont de rapoartele Grupului de cooperare și ale rețelei CSIRT privind experiența obținută la nivel strategic și operațional. Raportul este *însoțit, după caz, de o propunere legislativă*.					
Articolul 41. Transpunerea (1) *Până la ...* [*21 de* luni de la data intrării în vigoare a prezentei directive], *statele membre adoptă și publică* măsurile necesare pentru a se conforma prezentei directive. Statele membre informează de îndată Comisia cu privire la aceasta. Statele membre aplică măsurile respective de la … [ziua următoare datei menționate la primul paragraf]. (2) Atunci când statele membre adoptă măsurile respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a unei astfel de trimiteri.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
Articolul 42. Modificarea Regulamentului (UE) nr. 910/2014 *În* Regulamentul (UE) nr. 910/2014, *articolul 19* se elimină *de la ... [data menționată la articolul 41 alineatul (1) al doilea paragraf]*.		Incompatibil		În contextul aducerii în concordanță cu prevederile proiectului de lege a cadrului normativ urmează a fi abrogat art. 39 din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere	Viceprim-ministrul pentru digitalizare Serviciul de Informații și Securitate Ministerul Economiei
Articolul 43. Modificarea Directivei (UE) 2018/1972 *În* Directiva (UE) 2018/1972, *articolele 40 și 41* se elimină *de la ... [data menționată la articolul 41 alineatul (1) al doilea paragraf]*.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
Articolul 44. Abrogarea Directiva (UE) 2016/1148 se abrogă de la ... [data menționată la articolul 41 alineatul (1) al doilea paragraf].		Norme UE neaplicabile	Transpunerea este condiționată de aderarea		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
Trimiterile la directiva abrogată se interpretează ca trimiteri la prezenta directivă și se citesc în conformitate cu tabelul de corespondență din anexa III.			Republicii Moldova la UE		
Articolul 45. Intrarea în vigoare Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
Articolul 46. Destinatari Prezenta directivă se adresează statelor membre.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
ANEXA I ***SECTOARE CU O IMPORTANȚĂ CRITICĂ RIDICATĂ*** **ANEXA II.** ***ALTE SECTOARE DE IMPORTANȚĂ CRITICĂ***	**Articolul 4 Identificarea furnizorilor de servicii** (6) Guvernul aprobă lista sectoarelor, subsectoarelor și, respectiv, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și/sau subsectoare, precum și stabilește cadrul metodologic privind identificarea persoanelor juridice de drept public sau privat ca fiind furnizori de servicii, esențiali sau importanți.	Parțial compatibil		Guvernul urmează să adopte actul normativ respectiv pentru a asigura transpunerea totală a acestor anexe	Viceprim-ministru pentru digitalizare Ministerul Economiei

ANEXA I
SECTOARE CU O IMPORTANȚĂ CRITICĂ RIDICATĂ

Sectorul	Subsectorul	Tipul de entitate
1. Energie	(a) Electricitate	— Întreprinderile din domeniul energiei electrice, astfel cum sunt definite la articolul 2 punctul 57 din Directiva (UE) 2019/944 a Parlamentului European și a Consiliului[57], care îndeplinesc funcția de „furnizare”, astfel cum este definită la articolul 2 punctul 12 din directiva respectivă
		— Operatorii de distribuție, astfel cum sunt definiți la articolul 2 punctul 29 din Directiva (UE) 2019/944
		— Operatorii de transport și de sistem, astfel cum sunt definiți la articolul 2 punctul 35 din Directiva (UE) 2019/944
		— Producătorii, astfel cum sunt definiți la articolul 2 punctul 38 din Directiva (UE) 2019/944
		— Operatorii pieței de energie electrică desemnați, astfel cum sunt definiți la articolul 2 punctul 8 din Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului[58]
		— Participanții la piață, astfel cum sunt definiți la articolul 2 punctul 25 din Regulamentul (UE) 2019/943, care furnizează serviciile de agregare, consum dispecerizabil sau stocare de energie, astfel cum sunt definite la articolul 2 punctele 18, 20 și 59 din Directiva (UE) 2019/944 — ***Operatorii unui punct de reîncărcare care sunt responsabili cu gestionarea și exploatarea unui punct de reîncărcare care furnizează un serviciu de reîncărcare utilizatorilor finali, inclusiv în numele și în contul unui furnizor de servicii de mobilitate***
	(b) Încălzire centralizată și răcire centralizată	— Operatorii de încălzire centralizată sau răcire centralizată, astfel cum este definită la articolul 2 punctul 19 din Directiva (UE) 2018/2001 a Parlamentului European și a Consiliului[59]
	(c) Petrol	— Operatorii de conducte de transport al petrolului
		— Operatorii instalațiilor de producție, de rafinare și de tratare a petrolului, de depozitare și de transport
		— Entitățile centrale de stocare, astfel cum sunt definite la articolul 2 litera (f) din Directiva 2009/119/CE a Consiliului[60]
	(d) Gaze	— Întreprinderile de furnizare, astfel cum sunt definite la articolul 2 punctul 8 din Directiva (UE) 2009/73/CE a Parlamentului European și a Consiliului[61]
		— Operatorii de distribuție, astfel cum sunt definiți la articolul 2 punctul 6 din Directiva 2009/73/CE
		— Operatorii de transport și de sistem, astfel cum sunt definiți la articolul 2 punctul 4 din Directiva 2009/73/CE
		— Operatorii de înmagazinare, astfel cum sunt definiți la articolul 2 punctul 10 din Directiva 2009/73/CE
		— Operatorii de sistem GNL, astfel cum sunt definiți la articolul 2 punctul 12 din Directiva 2009/73/CE
		— Întreprinderile din sectorul gazelor naturale, astfel cum sunt definite la articolul 2 punctul 1 din Directiva 2009/73/CE
		— Operatorii de instalație de rafinare și de tratare a gazelor naturale
	(e) Hidrogen	— Operatorii de producție, stocare și transport de hidrogen
2. Transport	(a) Transport aerian	— Transportatorii aerieni, astfel cum sunt definiți la articolul 3 punctul 4 din Regulamentul (CE) nr. 300/2008, ***utilizați în scop comercial***
		— Organele de administrare a aeroporturilor, astfel cum sunt definite la articolul 2 punctul 2 din Directiva 2009/12/CE a Parlamentului European și a Consiliului[62], aeroporturile, astfel cum sunt definite la articolul 2 punctul 1 din directiva respectivă, inclusiv aeroporturile principale enumerate în secțiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului[63], precum și entitățile care operează instalații auxiliare în cadrul aeroporturilor
		— Operatorii de control al gestionării traficului care prestează servicii de control al traficului aerian (ATC), astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului[64]
	(b) Transport feroviar	— Administratorii infrastructurii, astfel cum sunt definiți la articolul 3 punctul 2 din Directiva 2012/34/UE a Parlamentului European și a Consiliului[65]

Sectorul	Subsectorul	Tipul de entitate
		— Întreprinderile feroviare, astfel cum sunt definite la articolul 3 punctul 1 din Directiva 2012/34/UE, inclusiv operatorii unei infrastructuri de servicii, astfel cum sunt definiți la articolul 3 punctul 12 din directiva respectivă
	(c) Transport pe apă	— Companiile de transport de mărfuri și pasageri pe ape interioare, maritime și de coastă, astfel cum sunt definite pentru transportul maritim în anexa I la Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului[66], fără a include navele individuale operate de companiile respective
		— Organele de gestionare a porturilor, astfel cum sunt definite la articolul 3 punctul 1 din Directiva 2005/65/CE a Parlamentului European și a Consiliului[67], inclusiv instalațiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004, și entitățile care realizează lucrări și operează echipamente în cadrul porturilor
		— Operatorii de servicii de trafic maritim (STM), astfel cum sunt definiți la articolul 3 litera (o) din Directiva 2002/59/CE a Parlamentului European și a Consiliului[68]
	(d) Transport rutier	— Autoritățile rutiere, astfel cum sunt definite la articolul 2 punctul 12 din Regulamentul delegat (UE) 2015/962 al Comisiei[69] responsabile cu controlul gestionării traficului***, cu excepția entităților publice în cazul cărora gestionarea traficului sau exploatarea sistemelor de transport inteligente reprezintă doar o parte neesențială a activității lor generale***
		— Operatorii de sisteme de transport inteligente, astfel cum sunt definite la articolul 4 punctul 1 din Directiva 2010/40/UE a Parlamentului European și a Consiliului[70]
3. Sectorul bancar		— Instituțiile de credit, astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului[71]
4. Infrastructuri ale pieței financiare		— Operatorii de locuri de tranzacționare, astfel cum sunt definite la articolul 4 punctul 24 din Directiva 2014/65/UE a Parlamentului European și a Consiliului[72]
		— Contrapărțile centrale (CPC), astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului[73]
5. Sectorul sănătății		— Furnizorii de servicii medicale, astfel cum sunt definiți la articolul 3 litera (g) din Directiva 2011/24/UE a Parlamentului European și a Consiliului[74]
		— Laboratoarele de referință ale UE, astfel cum sunt definite la articolul 15 din Regulamentul (UE) .../... al Parlamentului European și al Consiliului[75][76]
		— Entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor, astfel cum sunt definite la articolul 1 punctul 2 din Directiva 2001/83/CE a Parlamentului European și a Consiliului[77] — Entitățile care fabrică produse farmaceutice de bază și preparate farmaceutice menționate în secțiunea C diviziunea 21 din NACE Rev. 2 — Entitățile care fabrică dispozitive medicale considerate a fi esențiale în contextul unei urgențe de sănătate publică (lista dispozitivelor esențiale pentru urgența de sănătate publică) în sensul articolului 22 din Regulamentul (UE) 2022/123 al Parlamentului European și al Consiliului[78]
6. Apă potabilă		Furnizorii și distribuitorii de apă destinată consumului uman, astfel cum este definită la articolul 2 punctul 1 litera (a) din Directiva (UE) 2020/2184 a Parlamentului European și a Consiliului[79], excluzând distribuitorii pentru care distribuția de apă destinată consumului uman reprezintă o parte ***neesențială*** din activitatea lor generală de distribuție a altor produse de bază și bunuri
7. Ape uzate		Întreprinderile care colectează, evacuează sau tratează ape urbane reziduale, ape menajere uzate sau ape industriale uzate, astfel cum sunt definite la articolul 2 punctele 1, 2 și3 din Directiva 91/271/CEE a Consiliului[80]***, cu excepția întreprinderilor pentru care colectarea, evacuarea sau tratarea apelor urbane reziduale, a apelor menajere uzate sau a apelor industriale uzate reprezintă o parte neesențială a activității lor generale***
8. Infrastructură digitală		— Furnizorii de IXP (internet exchange point)
		— Furnizorii de servicii DNS***, cu excepția operatorilor de servere pentru nume primare***
		— Registrele de nume TLD
		— Furnizorii de servicii de cloud computing
		— Furnizorii de servicii de centre de date

Sectorul	Subsectorul	Tipul de entitate
		— Furnizorii de rețele de furnizare de conținut
		— Furnizorii de servicii de încredere
		— Furnizorii de rețele publice de comunicații electronice — Furnizorii de servicii de comunicații electronice accesibile publicului
9. ***Gestionarea serviciilor TIC (business-to-business)***		— ***Furnizorii de servicii gestionate*** — ***Furnizorii de servicii de securitate gestionate***
10. ***Administrație publică***		— Entitățile de administrație publică din administrația centrală***, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern***
		— Entitățile de administrație publică ***la nivel regional, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern***
11. Spațiu		— Operatorii de infrastructură terestră deținută, gestionată și operată de statele membre sau de părți private, care sprijină furnizarea de servicii spațiale, cu excepția furnizorilor de rețele publice de comunicații electronice

ANEXA II. ***Alte sectoare de importanță critică***

Sectorul	Subsectorul	Tipul de entitate
1. Servicii poștale și de curierat		Furnizorii de servicii poștale, astfel cum sunt definiți la articolul 2 punctul 1a din Directiva 97/67/CE***, inclusiv*** furnizori de servicii de curierat
2. Gestionarea deșeurilor		Întreprinderile care efectuează gestionarea deșeurilor, astfel cum este definită la articolul 3 punctul 9 din Directiva 2008/98/CE a Parlamentului European și a Consiliului[(81)], cu excepția întreprinderilor pentru care gestionarea deșeurilor nu reprezintă principala activitate economică
3. Fabricarea, producția și distribuția de substanțe chimice		Întreprinderile care produc substanțe și distribuie substanțe sau ***amestecuri,*** astfel cum se menționează la articolul 3 punctele 9 și 14 din Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului[(82)] ***și întreprinderile care produc articole, astfel cum sunt definite la articolul 3 punctul 3 din regulamentul respectiv, din substanțe sau amestecuri***
4. Producția, prelucrarea și distribuția de alimente		Întreprinderile cu profil alimentar, astfel cum sunt definite la articolul 3 punctul 2 din Regulamentul (CE) nr. 178/2002 al Parlamentului European și al Consiliului[(83)] ***care sunt implicate în distribuția angro și producția și prelucrarea industrială***
5. Fabricare	(a) Fabricarea de dispozitive medicale și de dispozitive medicale pentru diagnostic in vitro	Entitățile care fabrică dispozitive medicale, astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului[(84)], și entități care fabrică dispozitive medicale pentru diagnostic in vitro, astfel cum sunt definite la articolul 2 punctul 2 din Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului[(85)], cu excepția entităților care fabrică dispozitive medicale menționate în anexa I punctul 5 a cincea liniuță din prezenta directivă
	(b) Fabricarea computerelor și a produselor electronice și optice	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 26 din NACE Rev. 2
	(c) Fabricarea echipamentelor electrice	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 27 din NACE Rev. 2
	(d) Fabricarea altor mașini și echipamente n.c.a.	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 28 din NACE Rev. 2
	(e) Fabricarea autovehiculelor, remorcilor și semiremorcilor	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 29 din NACE Rev. 2
	(f) Fabricarea altor echipamente de transport	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 30 din NACE Rev. 2
6. Furnizori digitali		— Furnizorii de piețe online
		— Furnizorii de motoare de căutare online

		— Furnizorii de platforme de servicii de socializare în rețea
7. ***Cercetare***		***— Organizațiile de cercetare***