TABEL DE CONCORDANȚĂ

1	**Titlul actului Uniunii Europene, inclusiv cele mai recente amendamente incluse: Directiva (UE) 2022/2555 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)***
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) 2022/2557; (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 gestionarea incidentelor cibernetice.	**Compatibil**	-		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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;	**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) este 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;	**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. Conform prevederilor art. 23 alineatele (2) și (3) , Guvernul urmează într-un termen maxim de 12 luni din data publicării legii să adopte actele normative de punere a acestea în aplicare.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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; (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) 2022/2557, 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	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 persoane juridice de drept public. (3) Prezenta lege nu se aplică a) activităților desfășurate de autoritățile publice în domeniul protecției secretului de stat în legătură cu mentenanța rețelelor și sistemelor informatice care sunt destinate prelucrării unor astfel de informații; b) activităților desfășurate de autoritățile publice în domeniile securității naționale, apărării naționale, activității speciale de investigații și urmării penale în legătură cu mentenanța rețelelor și sistemelor informatice destinate prelucrării informațiilor din aceste domenii. (4) 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. (5) În cazul în care legile care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele stabilite de Guvern prevăd implementarea unor măsuri de gestionare a riscurilor sau obligații de notificare a incidentelor cu impact semnificativ, 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. (6) În cazul în care obligațiile, prevăzute la alineatul (5), stabilite de legile care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele stabilite de Guvern, sunt aplicabile unui cerc mai restrâns de persoane juridice decât cel prevăzut de prezenta lege și de actele normative de punere în aplicare a acesteia, prevederile prezentei legi se aplică persoanelor juridice care nu cad sub incidența obligațiilor impuse de legile respective. (7) Prevederile alineatelor (5) și (6) se aplică de către autoritatea competentă pentru fiecare caz în				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 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. (10) Prezenta directivă nu se aplică entităților pe care statele membre le-au exclus din domeniul de aplicare al Regulamentului (UE) 2022/2554 în conformitate cu articolul 2 alineatul (4) din regulamentul respectiv.	parte în procesul de identificare a furnizorilor de servicii în conformitate cu prevederile actului normativ stabilit la articolul 4 alineatul (2).				
(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)	**Articolul 3. Domeniul de aplicare** (3) Prezenta lege nu se aplică a) activităților desfășurate de autoritățile publice în domeniul protecției secretului de stat în legătură cu mentenanța rețelelor și sistemelor informatice care sunt destinate prelucrării unor astfel de informații;	**Compatibil**			

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
2016/679, Directivei 2002/58/CE, Directivelor 2011/93/UE (27) și 2013/40/UE (28) ale Parlamentului European și ale Consiliului și Directivei (UE) 2022/2557.	b) activităților desfășurate de autoritățile publice în domeniile securității naționale, apărării naționale, activității speciale de investigații și urmării penale în legătură cu mentenanța rețelelor și sistemelor informatice destinate prelucrării informațiilor din aceste domenii.				
(13) Fără a aduce atingere articolului 346 din TFUE, informațiile confidențiale în conformitate cu normele Uniunii sau cu cele naționale, precum cele privind secretul 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.		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
(14) Entitățile, autoritățile competente, punctele unice de contact și echipele CSIRT prelucrează datele 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 respectivul regulament. 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.	**Articolul 20. Protecția datelor cu caracter personal** (1) În exercitarea competenței cu care este învestită prin prezenta lege autoritatea competentă prelucrează date cu caracter personal în condițiile stabilite de legislația în acest domeniu. (2) În cazul în care, în procesul exercitării funcțiilor sale 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.	**compatibil**			

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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; (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) 2022/2557, 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 16 ianuarie 2023 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	**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) este 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;	**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 identificarea furnizorilor de servicii și aprobarea sectoarelor, suubsectoarelor și tipurilor de furnizori de servicii. Actul respectiv urmează a fi aprobat de către Guvern în termen de 12 luni din data publicării legii, conform art. 23 alin. (2) lit. c)	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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).	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 persoane juridice de drept public. (3) Prezenta lege nu se aplică a) activităților desfășurate de autoritățile publice în domeniul protecției secretului de stat în legătură cu mentenanța rețelelor și sistemelor informatice care sunt destinate prelucrării unor astfel de informații; b) activităților desfășurate de autoritățile publice în domeniile securității naționale, apărării naționale, activității speciale de investigații și urmării penale în legătură cu mentenanța rețelelor și sistemelor informatice destinate prelucrării informațiilor din aceste domenii. (4) 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. (5) În cazul în care legile care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele stabilite de Guvern prevăd implementarea unor măsuri de gestionare a riscurilor sau obligații de notificare a incidentelor cu impact semnificativ, 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. (6) În cazul în care obligațiile, prevăzute la alineatul (5), stabilite de legile care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele stabilite de Guvern, sunt aplicabile unui cerc mai restrâns de persoane juridice decât cel prevăzut de prezenta lege și de actele normative de punere în aplicare a acesteia, prevederile prezentei legi se aplică persoanelor juridice care nu cad sub incidența obligațiilor impuse de legile respective. (7) Prevederile alineatelor (5) și (6) se aplică de către autoritatea competentă pentru fiecare caz în				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	parte în procesul de identificare a furnizorilor de servicii în conformitate cu prevederile actului normativ stabilit la articolul 4 alineatul (2).				
(3) Până la 17 aprilie 2025, 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. (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, în termen de două săptămâni de la data modificării.	**Articolul 4. Identificarea furnizorilor de servicii** (1) Autoritatea competentă întocmește și ține lista furnizorilor de servicii, care cuprinde cel puțin tipul, categoria furnizorului de servicii și sectorul și subsectorul critic 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 critice și, corespunzător, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și subsectoare, stabilește cadrul metodologic privind identificarea persoanelor juridice de drept public și celor de drept privat ca fiind furnizori de servicii, precum și modul de întocmire, ținere și actualizare a listei furnizorilor de servicii. (3) La solicitarea autorității competente, Serviciul de Informații și Securitate furnizează acesteia lista operatorilor care au în gestiunea lor obiective ale infrastructurii critice. (4) Autoritățile publice responsabile de realizarea politicii de stat în sectoarele sau subsectoarele critice, 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, asigură suportul necesar autorității competente, la solicitarea acesteia, în procesul de identificare a furnizorilor de servicii.	**Parțial compatibil**		Adițional transpunerea integrală a acestor prevederi din actul UE se va realiza prin aprobarea de către Guvern a cadrului metodologic privind identificarea furnizorilor de servicii și lista sectoarelor, subsectoarelor, a categoriilor și tipurilor de furnizori de servicii, care potrivit art. 23 alin. (2), lit. c) urmează a fi adoptat în cel mult 12 luni de la data publicării Legii.	Ministerul Dezvoltării Economice și Digitalizării
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.		**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	5	6	7	8	9
(5) Până la 17 aprilie 2025 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 17 aprilie 2025 și la cererea Comisiei, statele membre pot notifica Comisiei denumirile entităților esențiale și ale entităților importante menționate la alineatul (5) litera (b).					
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 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	**Articolul 3 Domeniul de aplicare** (5) În cazul în care legile care reglementează activitatea furnizorilor de servicii, precum și sectoarele și subsectoarele, stabilite de Guvern, prevăd implementarea unor măsuri de gestionare a riscurilor sau obligații de notificare a incidentelor cu impact semnificativ, 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. (6) În cazul în care obligațiile, prevăzute la alineatul (5), stabilite de legile care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele stabilite de Guvern, sunt aplicabile unui cerc mai restrâns de persoane juridice decât cel prevăzut de prezenta lege și de actele normative de punere în aplicare a acesteia, prevederile prezentei legi se aplică persoanelor juridice care nu	Compatibil		Adițional implementarea acestor prevederi se va realiza prin aprobarea de către Guvern a cadrului metodologic privind identificarea furnizorilor de servicii și lista sectoarelor, subsectoarelor, a categoriilor și tipurilor de furnizori de servicii, care potrivit art. 23 alin. (2), lit. c) urmează a fi adoptat în cel mult 12 luni de la data publicării Legii.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
ale prezentei directive se aplică în continuare entităților care nu fac obiectul respectivelor acte juridice sectoriale ale Uniunii.	cad sub incidența obligațiilor impuse de legile respective.				
(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.	**Articolul 3. Domeniul de aplicare** (7) Prevederile alineatelor (5) și (6) 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).	Parțial compatibil		Criteriile de aplicare a caracterului echivalent al legislației sectoriale în raport cu prevederile proiectului de lege vor fi stabilite în actul normative, aprobat de Guvern în temeiul art. 4 alin. (2) din proiectul de lege. Acest act, potrivit art. 23 alin. (2) lit. c) urmează a fi adoptat în cel mult 12 luni de la data publicării Legii.	Ministerul Dezvoltării Economice și Digitalizării
(3) Comisia, până la 17 iulie 2023, 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 fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii.		**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	5	6	7	8	9
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** ***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 a unor astfel de date.	**Compatibil**			Ministerul Dezvoltării Economice și Digitalizării
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;	***Articolul 2. Principalele noțiuni și definițiile lor*** ***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 oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora	Compatibil			Ministerul Dezvoltării Economice și Digitalizării
3. **„securitate cibernetică"** înseamnă securitate cibernetică astfel cum este definită la articolul 2 alineatul (1) din Regulamentul (UE) 2019/881; (articolul 2 alineatul (1) din Regulamentul (UE) 2019/881 „securitate cibernetică" înseamnă activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice)	***Articolul 2. Principalele noțiuni și definițiile lor*** ***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;	Compatibil			Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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** (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 către Parlament la propunerea Guvernului.	**Compatibil**			Ministerul Dezvoltării Economice și Digitalizării
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. Principalele noțiuni și definițiile lor*** ***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;	**Compatibil**			Ministerul Dezvoltării Economice și Digitalizării
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;	***Articolul 2. Principalele noțiuni și definițiile lor*** ***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;	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării
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;	***Articolul 2. Principalele noțiuni și definițiile lor*** **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;	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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;	***Articolul 2. Principalele noțiuni și definițiile lor*** ***11) 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;	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării
10. ***„amenințare cibernetică"*** înseamnă o amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881 (art. 2 punctul 8 din Regulamentul (UE) 2019/881 „amenințare cibernetică" înseamnă 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;)	***Articolul 2. Principalele noțiuni și definițiile lor*** ***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**			Ministerul Dezvoltării Economice și Digitalizării
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;	***Articolul 2. Principalele noțiuni și definițiile lor*** **2) amenințare cibernetică semnificativă** - amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor sale tehnice, că are potențialul de a afecta grav rețelele și sistemele informatice ale unei persoane juridice care prestează servicii sau utilizatorii serviciilor furnizate de aceasta, cauzând prejudicii materiale sau morale considerabile;	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării
12. **„produs TIC"** înseamnă un produs astfel cum este definit la articolul 2 punctul 12 din Regulamentul (UE) 2019/881; (articolul 2 punctul 12 din Regulamentul (UE) 2019/881: „produs TIC" - înseamnă un element sau un grup de elemente al unei rețele sau al unui sistem informatic).	***Articolul 2. Principalele noțiuni și definițiile lor*** ***10) produs de tehnologie a informației și comunicații (produs TIC)*** - un element sau un grup de elemente al unei rețele sau al unui sistem informatic;	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării
13. **„serviciu TIC"** înseamnă un serviciu TIC astfel cum este definit la	***Articolul 2. Principalele noțiuni și definițiile lor*** ***15) serviciu de tehnologie a informației și comunicații (serviciu TIC)*** - un serviciu care constă	**compatibil**			Ministerul Dezvoltării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
articolul 2 punctul 13 din Regulamentul (UE) 2019/881; (articolul 2 punctul 13 din Regulamentul (UE) 2019/881: „serviciu TIC" înseamnă un serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice;)	integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice;				Economice și Digitalizării
14. **„proces TIC"** înseamnă un proces TIC astfel cum este definit la articolul 2 punctul 14 din Regulamentul (UE) 2019/881; (articolul 2 punctul 14 din Regulamentul (UE) 2019/881: „proces TIC" înseamnă un set de activități desfășurate pentru a concepe, a dezvolta, a furniza sau a întreține un produs TIC sau un serviciu TIC;)	***Articolul 2. Principalele noțiuni și definițiile lor*** ***9) proces de tehnologie a informației și comunicații (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**			Ministerul Dezvoltării Economice și Digitalizării
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;	***Articolul 2. Principalele noțiuni și definițiile lor*** ***17) 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**			Ministerul Dezvoltării Economice și Digitalizării
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; (articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012: „standard" înseamnă o specificație tehnică, adoptată de un organism de standardizare recunoscut, pentru aplicare repetată sau continuă, a cărei respectare nu este obligatorie și poate fi unul dintre următoarele: a) „standard internațional" înseamnă un standard adoptat de un organism de standardizare internațional; b) „standard european" înseamnă un standard adoptat de o organizație de standardizare europeană;	***Legea nr. 20/2016 cu privire la standardizarea națională*** ***Articolul 2. Noțiuni principale*** **standard** – specificație tehnică stabilită prin consens, adoptată de un organism de standardizare recunoscut, pentru aplicare repetată sau continuă, a cărei respectare nu este obligatorie; **standard moldovenesc** – standard aprobat sau adoptat de organismul național de standardizare din Republica Moldova; **standard european** – standard adoptat de o organizație europeană de standardizare; **standard armonizat** – standard european adoptat pe baza unei solicitări din partea Comisiei Europene pentru aplicarea legislației de armonizare a Uniunii Europene; **standard internațional** – standard adoptat de o organizație internațională de standardizare;	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
c) „standard armonizat" înseamnă un standard european adoptat pe baza unei solicitări din partea Comisiei pentru aplicarea legislației de armonizare a Uniunii; d) „standard național" înseamnă un standard adoptat de un organism de standardizare național."					
17. **„specificație tehnică"** înseamnă o specificație tehnică astfel cum este definită la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012; (articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012: „specificație tehnică" înseamnă un document în care sunt prevăzute cerințele tehnice pe care trebuie să le îndeplinească un produs, un proces, un serviciu sau un sistem și care stabilește unul sau mai multe dintre următoarele aspecte: (a) caracteristici necesare ale unui produs, inclusiv nivelurile de calitate, performanță, interoperabilitate, protecție a mediului, sănătate, siguranță sau dimensiuni, precum și cerințele aplicabile produsului în ceea ce privește denumirea sub care este vândut, terminologia, simbolurile, încercările și metodele de încercare, ambalarea, marcarea sau etichetarea și procedurile de evaluare a conformității; (b) metode și procese de producție utilizate în ceea ce privește produsele agricole astfel cum sunt definite la articolul 38 alineatul (1) din TFUE, produsele destinate consumului uman și animal și produsele medicamentoase, precum și metodele și procesele de producție aferente altor produse, în cazul în care au un efect asupra caracteristicilor acestora;	***Legea nr. 20/2016 cu privire la standardizarea națională*** ***Articolul 2. Noțiuni principale*** ***specificație tehnică*** – document în care sînt prevăzute cerințele tehnice pe care trebuie să le îndeplinească un produs, un proces, un serviciu sau un sistem și care stabilește unul sau mai multe dintre următoarele aspecte: a) caracteristici necesare ale unui produs, inclusiv nivelurile de calitate, performanță, interoperabilitate, protecție a mediului, sănătate, siguranță sau dimensiuni, precum și cerințele aplicabile produsului în ceea ce privește denumirea comercială, terminologia, simbolurile, încercările și metodele de încercare, ambalarea, marcarea sau etichetarea și procedurile de evaluare a conformității; b) metode și procese de producție utilizate în ceea ce privește produsele agricole, produsele destinate consumului uman și animal și produsele medicamentoase, precum și metode și procese de producție aferente altor produse, în cazul în care au un efect asupra caracteristicilor acestora; c) caracteristici necesare ale unui serviciu, inclusiv nivelurile de calitate, performanță, interoperabilitate, protecție a mediului, sănătate, siguranță, precum și cerințe aplicabile furnizorului în ceea ce privește informațiile care trebuie puse la dispoziția beneficiarului; d) metode și criterii de evaluare a performanței produselor pentru construcții, de stabilire a unor condiții armonizate pentru comercializarea produselor pentru construcții, în legătură cu caracteristicile esențiale ale acestora;	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(c) caracteristici necesare ale unui serviciu, inclusiv nivelurile de calitate, performanță, interoperabilitate, protecție a mediului, sănătate publică sau siguranță, precum și cerințe aplicabile furnizorului în ceea ce privește informațiile care trebuie puse la dispoziția beneficiarului astfel cum se specifică la articolul 22 alineatele (1)-(3) din Directiva 2006/123/CE; (d)metode și criterii de evaluare a performanței produselor de construcție, astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 305/2011 al Parlamentului European și al Consiliului din 9 martie 2011 de stabilire a unor condiții armonizate pentru comercializarea produselor pentru construcții (37), în legătură cu caracteristicile esențiale ale acestora.)	***specificație tehnică TIC*** – specificație tehnică din domeniul tehnologiilor informației și comunicațiilor;				
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**		Urmează a fi transpus prin proiectul de lege pentru modificarea unor acte normative, care urmează a fi aprobat de Guvern și prezentat Parlamentului spre examinare în termen de 6 luni din data publicării legii (art. 23 alin. (2) lit. b)).	Ministerul Dezvoltării Economice și Digitalizării
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 superior .md,	**Parțial compatibil**		Pentru necesitățile de reglementare normativă ale proiectului, la nivel de norme juridice primare, această noțiune nu este relevantă. În procesul elaborării proiectului de lege privind modificarea unor acte normative în vederea executării prevederilor art. 23 alin. (2) lit. b), urmează a fi efectuată o	Ministerul Dezvoltării Economice și Digitalizării; Agenția Națională pentru Reglementare în Comunicații Electronice și

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	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			analiză a legilor în domeniul comerțului electronic, protecției consumatorilor, a Codului civil etc pentru a stabili dacă este necesară reglementarea unei astfel de noțiuni. Totodată, în vederea asigurării procesului de adecvat de identificare a furnizorilor de servicii, în cadrul normativ al Guvernului ce urmează a fi adoptat întru executarea prevederilor art. 23 alin. (2) lit. c), aceste noțiuni urmează a fi preluate din perspectivă terminologică și determinare a cercului de subiecți.	Tehnologia Informației (ANRCETI)
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. **Hotărârea ANRCETI nr. 42/2020** privind aprobarea Regulamentului cu privire la gestionarea domeniului de nivel superior .md	**Parțial compatibil**			MIDR ANRCETI Viceprm-ministru pentru digitalizare
21. **„registru de nume de domenii de prim nivel"** sau **„registru de nume**	**Art.3 alineatul (5) din Legea comunicațiilor electronice nr. 241/2004**	**compatibil**			MIDR ANRCETI;

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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;	(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. **Hotărârea ANRCETI nr. 42/2020** privind aprobarea Regulamentului cu privire la gestionarea domeniului de nivel superior .md				
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. ***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;	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării ANRCETI;
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; (articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535: „serviciu" înseamnă orice serviciu al societății informaționale, adică orice	***Legea nr. 284/2004 privind comerțul electronic*** ***Articolul 4. Noțiuni principale*** ***serviciu al societății informaționale*** – orice serviciu prestat în scopul obținerii unei remunerații, la distanță, prin mijloace electronice și la cererea individuală a destinatarului serviciului, inclusiv vînzări de bunuri on-line. Serviciile societății informaționale nu se limitează exclusiv la servicii în. urma cărora se încheie contracte on-line, ci, în	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
serviciu prestat în mod normal în schimbul unei remunerații, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului. În sensul prezentei definiții: (i) „la distanță" înseamnă că serviciul este prestat fără ca părțile să fie prezente simultan; (ii) „prin mijloace electronice" înseamnă că serviciul este transmis inițial și primit la destinație prin intermediul echipamentului electronic pentru prelucrarea (inclusiv arhivarea digitală) și stocarea datelor și este transmis integral, transferat și recepționat prin cablu, radio, mijloace optice sau alte mijloace electromagnetice; (iii) „la solicitarea individuală a beneficiarului serviciilor" înseamnă că serviciul este prestat prin transmiterea datelor în urma solicitării individuale. În anexa I este prevăzută o listă orientativă a serviciilor care nu intră sub incidența prezentei definiții.)	măsura în care acestea reprezintă o activitate economică, se extind la servicii care nu sînt remunerate de cei care le primesc, cum ar fi serviciile care furnizează informații on-line ori comunicări comerciale sau cele care furnizează instrumente de căutare, accesare și recuperare a datelor. Servicii ale societății informaționale sînt de asemenea serviciile care constau în transmiterea informațiilor printr-o rețea de comunicații electronice, furnizarea accesului la o rețea de comunicații electronice sau găzduirea informațiilor furnizate de un destinatar al serviciului. Serviciile transmise punct cu punct, precum video la cerere sau furnizarea de comunicări comerciale prin poșta electronică, sînt de asemenea servicii ale societății informaționale. Nu constituie servicii ale societății informaționale, în sensul prezentei legi, următoarele activități: a) serviciile furnizate în prezența fizică a furnizorului și a destinatarului, chiar dacă acest lucru presupune utilizarea echipamentului electronic; b) serviciile cu un conținut material, chiar dacă sînt furnizate prin intermediul dispozitivelor electronice; c) serviciile prestate fără utilizarea rețelei de internet (serviciile off-line), cum ar fi distribuirea de programe pe dispozitive de stocare; d) serviciile care nu sînt furnizate prin intermediul sistemelor de prelucrare și stocare electronică a datelor, cum ar fi: – serviciile de telefonie vocală, serviciile de fax/telex; – serviciile prestate prin telefonie vocală sau fax; – comercializarea directă prin telefon/fax; e) serviciile furnizate prin transmiterea de date, fără solicitare individuală, în scopul recepționării simultane de către un număr nelimitat de destinatari individuali (transmisiune punct-multipunct), cum ar fi: – serviciile de transmisiune sau retransmisiune a serviciilor de programe audiovizuale; – teletextul;				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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**			Ministerul Dezvoltării Economice și Digitalizării 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 încredere ca prestator de servicii de încredere calificat sau necalificat;	**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**			Ministerul Dezvoltării Economice și Digitalizării Serviciul de Informații și Securitate
26. **„serviciu de încredere calificat"** „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	**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**			Ministerul Dezvoltării Economice și Digitalizării Serviciul de Informații și Securitate

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
îndeplinește cerințele aplicabile prevăzute de prezentul regulament;					
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**			Ministerul Dezvoltării Economice și Digitalizării 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; **(articolul 2 litera (n) din Directiva 2005/29/CE:** „piață online" înseamnă un serviciu care utilizează software, inclusiv un site de internet sau o parte a unui site de internet sau o aplicație gestionată de către comerciant sau în numele acestuia, care le permite consumatorilor să încheie contracte la distanță cu alți comercianți sau consumatori)		incompatibil		Pentru necesitățile de reglementare normativă ale proiectului, la nivel de norme juridice primare, această noțiune nu este relevantă. În procesul elaborării proiectului de lege privind modificarea unor acte normative în vederea executării prevederilor art. 23 alin. (2) lit. b), urmează a fi efectuată o analiză a legilor în domeniul comerțului electronic, protecției consumatorilor, a Codului civil etc pentru a stabili dacă este necesară reglementarea unei astfel de noțiuni. Totodată, în vederea asigurării procesului de adecvat de identificare a furnizorilor de servicii, în cadrul normativ al Guvernului ce urmează a fi adoptat întru executarea prevederilor art. 23 alin. (2) lit. c), aceste noțiuni urmează a fi preluate din perspectivă terminologică și determinare a cercului de subiecți.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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; **(articolul 2 punctul 5 din Regulamentul (UE) 2019/1150** „motor de căutare online" înseamnă un serviciu digital care permite utilizatorilor să introducă interogări pentru a căuta, în principiu, în toate site-urile internet sau site-urile internet într-o anumită limbă pe baza unei interogări privind orice subiect sub forma unui cuvânt, a unei solicitări vocale, a unei fraze sau a unui alt element introdus și care revine cu rezultate în orice format în care se pot găsi informații legate de conținutul căutat).		incompatibil		**Pentru necesitățile de reglementare normativă ale proiectului, la nivel de norme juridice primare, această noțiune nu este relevantă.** **În procesul elaborării proiectului de lege privind modificarea unor acte normative în vederea executării prevederilor art. 23 alin. (2) lit. b), urmează a fi efectuată o analiză a legilor în domeniul comerțului electronic, protecției consumatorilor, a Codului civil etc pentru a stabili dacă este necesară reglementarea unei astfel de noțiuni.** **Totodată, în vederea asigurării procesului de adecvat de identificare a furnizorilor de servicii, în cadrul normativ al Guvernului ce urmează a fi adoptat întru executarea prevederilor art. 23 alin. (2) lit. c), aceste noțiuni urmează a fi preluate din perspectivă terminologică și determinare a cercului de subiecți.**	Ministerul Dezvoltării Economice și Digitalizării
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;		incompatibil		**Pentru necesitățile de reglementare normativă ale proiectului, la nivel de norme juridice primare, această noțiune nu este relevantă.** **În procesul elaborării proiectului de lege privind modificarea unor acte normative în vederea executării prevederilor art. 23 alin. (2) lit. b), urmează a fi efectuată o analiză a legilor în domeniul comerțului electronic, protecției consumatorilor, a Codului civil etc pentru a stabili dacă este necesară**	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
				reglementarea unei astfel de noțiuni. **Totodată, în vederea asigurării procesului de adecvat de identificare a furnizorilor de servicii, în cadrul normativ al Guvernului ce urmează a fi adoptat întru executarea prevederilor art. 23 alin. (2) lit. c), aceste noțiuni urmează a fi preluate din perspectivă terminologică și determinare a cercului de subiecți.**	
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;		incompatibil		**Pentru necesitățile de reglementare normativă ale proiectului, la nivel de norme juridice primare, această noțiune nu este relevantă.** **În procesul elaborării proiectului de lege privind modificarea unor acte normative în vederea executării prevederilor art. 23 alin. (2) lit. b), urmează a fi efectuată o analiză a legilor în domeniul comerțului electronic, protecției consumatorilor, a Codului civil etc pentru a stabili dacă este necesară reglementarea unei astfel de noțiuni.** **Totodată, în vederea asigurării procesului de adecvat de identificare a furnizorilor de servicii, în cadrul normativ al Guvernului ce urmează a fi adoptat întru executarea prevederilor art. 23 alin. (2) lit. c), aceste noțiuni urmează a fi preluate din perspectivă terminologică și determinare a cercului de subiecți.**	Ministerul Dezvoltării Economice și Digitalizării
32. **„rețea de furnizare de conținut"** înseamnă o rețea de servere distribuite geografic cu scopul de a asigura o		incompatibil		**Pentru necesitățile de reglementare normativă ale proiectului, la nivel de norme**	Ministerul Dezvoltării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
disponibilitate ridicată, accesibilitate sau furnizare rapidă de conținut digital și servicii către utilizatorii de internet în numele furnizorilor de conținut și de servicii;				**juridice primare, această noțiune nu este relevantă.** **În procesul elaborării proiectului de lege privind modificarea unor acte normative în vederea executării prevederilor art. 23 alin. (2) lit. b), urmează a fi efectuată o analiză a legilor în domeniul comerțului electronic, protecției consumatorilor, a Codului civil etc pentru a stabili dacă este necesară reglementarea unei astfel de noțiuni.** **Totodată, în vederea asigurării procesului de adecvat de identificare a furnizorilor de servicii, în cadrul normativ al Guvernului ce urmează a fi adoptat întru executarea prevederilor art. 23 alin. (2) lit. c), aceste noțiuni urmează a fi preluate din perspectivă terminologică și determinare a cercului de subiecți.**	Economice și Digitalizării
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;		incompatibil		**Pentru necesitățile de reglementare normativă ale proiectului, la nivel de norme juridice primare, această noțiune nu este relevantă.** **În procesul elaborării proiectului de lege privind modificarea unor acte normative în vederea executării prevederilor art. 23 alin. (2) lit. b), urmează a fi efectuată o analiză a legilor în domeniul comerțului electronic, protecției consumatorilor, a Codului civil etc pentru a stabili dacă este necesară reglementarea unei astfel de noțiuni.** **Totodată, în vederea asigurării procesului de adecvat de**	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
				identificare a furnizorilor de servicii, în cadrul normativ al Guvernului ce urmează a fi adoptat întru executarea prevederilor art. 23 alin. (2) lit. c), aceste noțiuni urmează a fi preluate din perspectivă terminologică și determinare a cercului de subiecți.	
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		
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;	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.	**Compatibil**			

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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;	(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:** 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:***	**Articolul 2 din Legea nr. 241 comunicațiilor electronice:** rețea de comunicații electronice – sisteme de transmisie și, după caz, echipamente de comutare sau rutare, precum și alte resurse care permit transmiterea semnalelor prin suport fizic, electromagnetic sau prin orice alte mijloace, incluzînd rețele de comunicații prin satelit, rețele	**Compatibil**			

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
„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;).	fixe (cu comutare de circuite sau comutare de pachete, inclusiv Internet) și rețele mobile terestre, rețele de transport al energiei electrice, în cazul în care acestea sînt utilizate și pentru transmiterea semnalelor, rețele utilizate pentru difuzarea programelor audiovizuale, rețele de televiziune prin cablu, indiferent de tipul informației transmise; rețea publică de comunicații electronice – rețea de comunicații electronice utilizată în întregime sau în principal pentru furnizarea de servicii de comunicații electronice accesibile publicului, care asigură transferul de informații între punctele terminale ale rețelei;				
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 comunicații electronice*** – serviciu furnizat, de regulă, contra plată, care constă în întregime sau în principal în transportul semnalelor prin rețelele de comunicații electronice, inclusiv serviciile de telecomunicații și serviciile de transmisie prin rețelele utilizate pentru difuzarea de programe audiovizuale, dar fără a include serviciile prin care se furnizează conținutul informației transmise prin intermediul rețelelor sau serviciilor de comunicații electronice sau prin care se exercită controlul editorial asupra acestui conținut; de asemenea, nu se includ serviciile societății informaționale (în particular, serviciile de comerț electronic) care nu constau, în întregime sau în principal, în transportul semnalelor prin intermediul rețelelor de comunicații electronice;	**compatibil**			

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 și de obligații 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 și distinct, afectat realizării unui anumit scop conform cu legea, ordinea publică și bunele moravuri. (2) Persoană juridică poate să dobândească și să exercite în nume propriu drepturi patrimoniale și personale nepatrimoniale, să-și asume obligații, poate fi reclamant și pîrît în instanța de judecată. (3) Persoana juridică poate fi organizată în mod corporativ sau în baza calității de membru, poate fi dependentă sau independentă de un anumit număr de membri, poate avea scop lucrativ sau nelucrativ. (4) În funcție de participare la constituirea patrimoniului persoanei juridice, fondatorii (membrii) au sau nu au drepturi de creanță față de ea. Persoane juridice în a căror privință fondatorii (membrii) au drepturi de creanță sunt societățile comerciale și cooperativele. Persoane juridice în a căror privință fondatorii (membrii) nu au drepturi de creanță sînt organizațiile necomerciale.	**Compatibil**			
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;		incompatibil		Pentru necesitățile de reglementare normativă ale proiectului, la nivel de norme juridice primare, această noțiune nu este relevantă. În procesul elaborării proiectului de lege privind modificarea unor acte normative în vederea executării prevederilor art. 23 alin. (2) lit. b), urmează a fi efectuată o analiză a legilor în domeniul comerțului electronic, protecției consumatorilor, a Codului civil etc pentru a stabili dacă este	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
				necesară reglementarea unei astfel de noțiuni. Totodată, în vederea asigurării procesului de adecvat de identificare a furnizorilor de servicii, în cadrul normativ al Guvernului ce urmează a fi adoptat întru executarea prevederilor art. 23 alin. (2) lit. c), aceste noțiuni urmează a fi preluate din perspectivă terminologică și determinare a cercului de subiecți.	
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;		incompatibil		Pentru necesitățile de reglementare normativă ale proiectului, la nivel de norme juridice primare, această noțiune nu este relevantă. În procesul elaborării proiectului de lege privind modificarea unor acte normative în vederea executării prevederilor art. 23 alin. (2) lit. b), urmează a fi efectuată o analiză a legilor în domeniul comerțului electronic, protecției consumatorilor, a Codului civil etc pentru a stabili dacă este necesară reglementarea unei astfel de noțiuni. Totodată, în vederea asigurării procesului de adecvat de identificare a furnizorilor de servicii, în cadrul normativ al Guvernului ce urmează a fi adoptat întru executarea prevederilor art. 23 alin. (2) lit. c), aceste noțiuni urmează a fi preluate din perspectivă terminologică și determinare a cercului de subiecți.	Ministerul Dezvoltării Economice și Digitalizării
41. ***„organizație de cercetare"*** *înseamnă o entitate care are ca obiectiv principal să desfășoare activități de cercetare aplicată sau de dezvoltare*	**Articolul 15 din Codul cu privire la știință și inovare** *Organizație din domeniile cercetării și inovării* – persoană juridică care desfășoară una dintre	Parțial compatibil prevederile actului Uniunii			Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
experimentală în vederea exploatării rezultatelor cercetării respective în scopuri comerciale, dar care nu include instituțiile de învățământ.	următoarele activități: cercetări fundamentale și/sau aplicative, dezvoltarea experimentală, implementarea rezultatelor științifice și inovațiilor, transferul tehnologic, pregătirea și perfecționarea cadrelor științifice.	Europene netranspuse nu sunt fundamentale			Ministerul Educației
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;	**Articolul 6. Planificarea și coordonarea strategică în domeniul securității cibernetice la nivel național** (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 către Parlament la propunerea Guvernului. **Articolul 23. Intrarea în vigoare a legii și măsuri de implementare** ..... (2) Guvernul: ..... d) în termen de 12 luni de la data intrării în vigoare a prezentei legi va elabora, va aproba și va prezenta Parlamentului spre examinare Strategia națională în domeniul securității cibernetice	**Compatibil**		Adițional pentru implementarea prevederilor legii În conformitate cu art. 23 alin. (2) lit.d) în termen de 12 luni de la data intrării în vigoare a legii, Guvernul va elabora, va aproba și va prezenta Parlamentului spre examinare Strategia națională în domeniul securității cibernetice.	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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 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) 2022/2557 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;					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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 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					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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.		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
(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 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.	**Legea nr. 100/2017 cu privire la actele normative.** **Articolul 24. Documentele de politici** (1) Documentele de politici, fără a fi acte normative, sunt instrumente de decizie care abordează problemele existente într-un anumit domeniu, care definesc căile de soluționare a problemelor respective și descriu impactul așteptat asupra statului și societății. Documentele de politici pot prevedea elaborarea proiectelor de acte normative. (2) La fundamentarea, elaborarea, avizarea, consultarea și aprobarea documentelor de politici se aplică regulile și cerințele înaintate față de actele normative. (3) Tipurile și structura documentelor de politici, precum și modul de elaborare, aprobare, monitorizare a implementării și de evaluare a acestora se stabilesc de către Guvern. ..... (5) Documentele de politici se aprobă prin hotărâre de Guvern. În cazul în care implementarea acestor politici presupune implicarea unor autorități administrative care nu se află în subordinea Guvernului, documentele de politici sunt aprobate de către Parlament. Documentele de politici ale autorităților publice autonome sînt aprobate de către acestea dacă nu presupun implicarea altor autorități administrative aflate în subordinea Guvernului. Documentele de politici de nivel local se aprobă prin decizia autorității reprezentative a unității administrativ-teritoriale.	**Parțial compatibil**		În conformitate cu art. 23 alin. (2) lit. d) în termen de 12 luni de la data intrării în vigoare a legii, Guvernul va elabora, va aproba și va prezenta Parlamentului spre examinare Strategia națională în domeniul securității cibernetice. Acest document de politici urmează să conțină și indicatori de monitorizare și evaluare (descrierea indicatorilor de monitorizare a activităților preconizate, prin intermediul cărora este măsurat gradul de implementare a strategiei, precum și a indicatorilor de evaluare, prin intermediul cărora este stabilit nivelul de realizare a obiectivelor);	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	Regulamentul cu privire la planificarea, elaborarea, aprobarea, implementarea, monitorizarea și evaluarea documentelor de politici publice, aprobat prin Hotărârea Guvernului nr. 386/2020 7. Strategia este un document de politici publice care definește și planifică politica publică a Guvernului pe termen lung (6-10 ani) în unul sau câteva domenii de activitate a Guvernului, stabilite conform Legii nr.136/2017 cu privire la Guvern. 57. Evaluarea se realizează în procesul de implementare a documentelor de politici publice (evaluarea intermediară) și după expirarea termenului de implementare a documentului de politici publice (evaluarea finală) în scopul prezentării unei imagini obiective în conformitate cu următoarele criterii: 1) relevanța documentului de politici publice și a măsurilor incluse pentru țară; 2) gradul de realizare a obiectivelor (efectivitatea); 3) modul de utilizare a mijloacelor bugetare alocate (eficiența); 4) capacitatea de a produce efecte de durată (durabilitatea); 5) impactul documentului de politici publice, estimat în cadrul evaluării finale.				
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	**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 și 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;	Parțial Compatibil		În conformitate cu prevederile art. 23 alin. (2) lit. a) Guvernul urmează să desemneze autoritatea competentă în termen de cel 9 luni din data publicării legii.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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.	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 în domeniul securității cibernetice 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 sau îndeplinirea necorespunzătoare a obligațiilor de către furnizorii de servicii; h) exercită atribuțiile organului constatator pentru cauze contravenționale în domeniul securității cibernetice în conformitate cu prevederile Codului contravențional; i) alte atribuții care decurg din prevederile prezentei legi și actele normative. (4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale: 1) 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) 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 rețelelor și sistemelor lor informatice;				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	3) emite avertizări timpurii, alerte, anunțuri și diseminează informații privind amenințările cibernetice, vulnerabilitățile și incidentele cibernetice; 4) recepționează notificări privind incidentele cibernetice care afectează rețelele și sistemele informatice ale furnizorilor de servicii; 5) 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; 6) colectează și analizează date criminalistice și furnizează analize dinamice de risc și de incident și conștientizare a situației în materie de securitate cibernetică; 7) 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; 8) 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 12 alineatul (8); 9) implementează în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate, precum și asigură, în conformitate cu legislația, protecția informațiilor de care ia cunoștință în procesul exercitării atribuțiilor sale; 10) 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: a) intermedierea și facilitarea interacțiunii dintre persoana fizică sau juridică care raportează o vulnerabilitate și producătorul sau				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	furnizorul de produse TIC sau servicii TIC potențial vulnerabile, la cererea oricăreia dintre aceste persoane; b) identificarea și contactarea persoanelor fizice sau juridice implicate; c) acordarea asistenței persoanelor fizice sau juridice care raportează o vulnerabilitate; d) negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități; e) 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 în materie de securitate cibernetică 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**		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 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;	**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 elaborează și aprobă planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice 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 în domeniul securității cibernetice 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.	**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. În conformitate cu art. 23 alin. (2) lit. c) acest act normativ urmează a fi aprobat de Guvern în cel mult 12 luni din data publicării legii.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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..					
(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 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.		**Norme UE neaplicabile**	**Transpunerea este condiționată de aderarea Republicii Moldova la UE**		
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	**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.	**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	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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.	(2) Autoritatea competentă exercită și 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: 1) 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) 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 rețelelor și sistemelor lor informatice; 3) emite avertizări timpurii, alerte, anunțuri și diseminează informații privind amenințările cibernetice, vulnerabilitățile și incidentele cibernetice; 4) recepționează notificări privind incidentele cibernetice care afectează rețelele și sistemele informatice ale furnizorilor de servicii; 5) 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; 6) colectează și analizează date criminalistice și furnizează analize dinamice de risc și de incident și conștientizare a situației în materie de securitate cibernetică; 7) 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; 8) efectuează, la cererea unui furnizor de servicii, scanări proactive a rețelelor și a sistemelor			respective și dotării acesteia cu resursele umane și financiare și cu mijloacele tehnice necesare asigurării îndeplinirii acestor cerințe.	

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	informatice ale solicitantului pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, în conformitate cu actul normativ aprobat de Guvern în temeiul articolului 12 alineatul (8); 9) implementează în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate, precum și asigură, în conformitate cu legislația, protecția informațiilor de care ia cunoștință în procesul exercitării atribuțiilor sale; 10) 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: a) 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 persoane; b) identificarea și contactarea persoanelor fizice sau juridice implicate; c) acordarea asistenței persoanelor fizice sau juridice care raportează o vulnerabilitate; d) negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități; e) asigurarea anonimatului persoanelor fizice sau juridice care raportează o vulnerabilitate, atunci când acestea o solicită.				
(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		**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	5	6	7	8	9
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 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	**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.	Parțial compatibil		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	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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; (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.	(2) Autoritatea competentă exercită și funcțiile de punct național unic de contact și echipă de răspuns la incidentele cibernetice la nivel național. ..... **Articolul 23. Intrarea în vigoare a legii și măsuri de implementare** (1) Guvernul: a) în termen de 9 luni de la data publicării prezentei legi, va întreprinde măsurile necesare pentru desemnarea autorității competente, precum și reglementarea modului de organizare și funcționare și stabilirea structurii și efectivului limită a acesteia; ..... (3) Pentru realizarea eficientă a sarcinii stabilite la alineatul (2) litera a), Guvernul trebuie să asigure autoritatea competentă cu resursele necesare, 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 calificat pentru a asigura disponibilitatea permanentă a serviciilor sale și se asigură că personalul său este format în mod corespunzător;			mijloacele tehnice necesare asigurării îndeplinirii acestor cerințe. Astfel potrivit art. 23 alin. (2) lit a), în termen de cel mult 9 luni Guvernul urmează să aprobe actul de reglementare a modului de organizare și funcționare a autorității competente, asigurând respectarea condițiilor de la alin. (3) al aceluiași articol.	

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	h) să dispună de sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor sale.				
(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 ale entității implicate pentru a detecta vulnerabilitățile cu un impact potențial semnificativ;	**Articolul 7 Autoritatea competentă** ..... (4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale: 1) 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) 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 rețelelor și sistemelor lor informatice; 3) emite avertizări timpurii, alerte, anunțuri și diseminează informații privind amenințările cibernetice, vulnerabilitățile și incidentele cibernetice; 4) recepționează notificări privind incidentele cibernetice care afectează rețelele și sistemele informatice ale furnizorilor de servicii; 5) 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; 6) colectează și analizează date criminalistice și furnizează analize dinamice de risc și de incident și conștientizare a situației în materie de securitate cibernetică; 7) cooperează, la nivel național și internațional, cu echipele de răspuns la incidentele	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. Astfel potrivit art. 23 alin. (2) lit a), în termen de cel mult 9 luni Guvernul urmează să aprobe actul de reglementare a modului de organizare și funcționare a autorității competente, asigurând respectarea condițiilor de la alin. (3) al aceluiași articol.	Viceprim-ministru pentru digitalizare Ministerul Economiei

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(f) participarea la rețeaua CSIRT și furnizarea de asistență reciprocă în funcție de capacitățile și competențele lor altor membri ai rețelei, la cererea acestora; (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 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	cibernetice în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații; 8) 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 12 alineatul (8); 9) implementează în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate, precum și asigură, în conformitate cu legislația, protecția informațiilor de care ia cunoștință în procesul exercitării atribuțiilor sale; 10) 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: a) 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 persoane; b) identificarea și contactarea persoanelor fizice sau juridice implicate; c) acordarea asistenței persoanelor fizice sau juridice care raportează o vulnerabilitate; d) negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități; e) asigurarea anonimatului persoanelor fizice sau juridice care raportează o vulnerabilitate, atunci când acestea o solicită.			

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(c) divulgarea coordonată a vulnerabilităților în temeiul articolului 12 alineatul (1).					
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 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	**Articolul 7. Autoritatea competentă** (4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale: ..... 10) 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: a) 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 persoane; b) identificarea și contactarea persoanelor fizice sau juridice implicate; c) acordarea asistenței persoanelor fizice sau juridice care raportează o vulnerabilitate; d) negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități; e) asigurarea anonimatului persoanelor fizice sau juridice care raportează o vulnerabilitate, atunci când acestea o solicită.	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 referință în art. 7 alin. (4) pct. 10). Acest act urmează a fi aprobat, potrivit art. 23 alin. (2) lit. c), de către Guvern în termen de cel mult 12 luni de la data publicării legii.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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.					
(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 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		**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	5	6	7	8	9
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.	**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 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,	Compatibil		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. Art. 13 din Directiva NIS2 cuprinde reglementări pentru statele membre în care sunt implementate sisteme descentralizate în domeniul securității cibernetice.	

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	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.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	(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 15. Gestionarea incidentelor cibernetice** (1) În scopul asigurării securității cibernetice, autoritatea competentă monitorizează activitatea în spațiul de adrese în Internet al Republicii Moldova analizează riscurile, precum și impactul acestora asupra statului, societății și securității rețelelor și sistemelor informatice .... (3) Autoritatea competentă notifică în cel mai scurt timp însă nu mai târziu de 24 de ore, referitor la aplicarea măsurilor prevăzute la alineatul (2), destinatarul și, în cazul unui furnizor de servicii,				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	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				
(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 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) 2022/2554, autoritățile naționale de reglementare în temeiul Directivei (UE) 2018/1972, autoritățile competente în temeiul Directivei (UE) 2022/2557, 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) 2022/2557 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) 2022/ 2557, 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	**Articolul 4. Identificarea furnizorilor de servicii** .... (3) La solicitarea autorității competente, Serviciul de Informații și Securitate furnizează acesteia lista operatorilor care au în gestiunea lor obiective ale infrastructurii critice. **Articolul 7. Autoritatea competentă** .... **(3) Autoritatea competentă exercită următoarele atribuții principale:** 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 în domeniul securității cibernetice cu autoritățile și instituțiile publice naționale și cu furnizorii de servicii ..... (4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale: 1) 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 ..... 7) 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 (5) În exercitarea funcției de punct național unic de contact, autoritatea competentă exercită următoarele atribuții principale:	Parțial compatibil		Adițional aceste prevederi urmează a fi transpuse prin adoptarea proiectului de lege pentru modificarea unor acte normative pentru aducerea legislației în concordanță cu prevederile legii (6 luni de la data publicării legii) și a cadrului normativ al Guvernului (în termen de cel mult 12 luni din data publicării legii.)	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
autoritățile lor competente în temeiul Regulamentului (UE) nr. 910/2014, al Regulamentului (UE) 2022/2554 și al Directivei (UE) 2018/1972 fac schimb de informații relevante în mod periodic, inclusiv în ceea ce privește incidentele și amenințările cibernetice relevante.	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 în materie de securitate cibernetică primite din alte state sau de la organizații internaționale ori de la entitățile constituite de către acestea				
(6) Statele membre simplifică raportarea prin mijloace tehnice pentru notificările menționate la articolele 23 și 30.	**Articolul 7. Autoritatea competentă** .... (4) În exercitarea funcției de echipă de răspuns la incidentele cibernetice la nivel național, autoritatea competentă exercită următoarele atribuții principale: ..... 9) implementează în schimbul de informații cu furnizorii de servicii și alte persoane relevante instrumente și soluții tehnice securizate, precum și asigură, în conformitate cu legislația, protecția informațiilor de care ia cunoștință în procesul exercitării atribuțiilor sale. **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	Compatibil			

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
	incidentelor cibernetice și, corespunzător, a sistemului informațional destinat ținerii acestuia. (2) Accesul la registru este limitat, iar datele din registru sunt destinate utilizării interne, cu excepția cazului în care cadrul normativ prevede altfel.				
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) 2022/2554 pot participa la activitățile Grupului de cooperare în conformitate cu articolul 47 alineatul (1) din regulamentul respectiv. 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		**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	5	6	7	8	9
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; (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);					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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), precum și definirea metodologiei de autoevaluare pentru statele membre în conformitate cu					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
punere în aplicare menționate la primul paragraf de la 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) 2022/2557 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;		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	5	6	7	8	9
(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 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;					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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; (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) Până la 17 ianuarie 2025 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.					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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, 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		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	5	6	7	8	9
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. (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 17 iulie 2024 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,		Norme UE neaplicabile	Transpunerea este condiționată de		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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.			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; (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.		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	5	6	7	8	9
(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 17 ianuarie 2025, 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 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:		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	5	6	7	8	9
(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 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					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 dreptului 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					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
cibernetică desemnați este dezvăluit celorlalte state 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.	**Articolul 11. Măsurile de securitate** (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:	Compatibil			

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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. (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	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 implementeze măsuri tehnice și organizatorice corespunzătoare și proporționale riscurilor, în conformitate cu standardele menționate 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; - politici și proceduri privind gestionarea incidentelor (prevenire, detectare și răspuns la incidente) - politici și proceduri privind utilizarea criptografiei și a criptării în special a criptării de la un capăt la altul, - 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 furnizorului de servicii cu 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				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
sistemelor informatice corespunzător riscurilor prezentate. Atunci când se evaluează proporţio- nalitatea acestor măsuri, se ţine seama în mod corespunzător de gradul de expunere a entităţii la riscuri, de dimensiunea entităţii şi de probabilitatea producerii incidentelor, precum şi de gravitatea acestora, inclusiv de impactul lor societal şi economic. (2) Măsurile menţionate la alineatul (1) se bazează pe o abordare multirisc care vizează protejarea reţelelor şi a sistemelor informatice, precum şi a mediului fizic al acestor sisteme împotriva incidentelor, şi includ cel puţin următoarele: (a) politici referitoare la analiza riscurilor şi securitatea sistemelor informatice; (b) gestionarea incidentelor; (c) continuitatea activităţii, de exemplu gestionarea copiilor de rezervă şi recuperarea în caz de dezastru, precum şi gestionarea crizelor; (d) securitatea lanţului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relaţiile dintre fiecare entitate şi prestatorii sau furnizorii săi direcţi de servicii; (e) securitatea în achiziţionarea, dezvoltarea şi întreţinerea reţelelor şi a sistemelor informatice, inclusiv gestionarea vulnerabilităţilor şi divulgarea acestora; (f) politici şi proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor în materie de securitate cibernetică; (g) practici de bază în materie de igienă cibernetică şi formare în domeniul securităţii cibernetice;	text şi de sisteme securizate de comunicaţii de urgenţă în cadrul furnizorului de servicii; c) să menţină în stare de actualitate documentaţia privind măsurile de securitate; d) să asigure monitorizarea în scopul detectării serviciilor TIC, proceselor TIC sau produselor TIC care compromit securitatea reţelei sau sistemului informatic; e) să întreprindă măsuri orientate spre reducerea impactului şi a răspândirii unui incident cibernetic, inclusiv, dacă este necesar, restricţionarea utilizării sau accesului la reţeaua sau sistemul informatic; f) verifică suficienţa şi conformitatea aplicării măsurilor de securitate, inclusiv prin efectuarea auditurilor de securitate, şi documentează rezultatele acestei verificări. (3) În cazul în care furnizorul de servicii autorizează un terţ să administreze reţeaua şi/sau sistemul informatic ori utilizează serviciile unui terţ pentru găzduirea sistemului informatic, acesta este responsabil pentru aplicarea măsurilor de securitate a reţelei şi/sau sistemului informatic de către terţ. (4) În vederea asigurării îndeplinirii obligaţiilor prevăzute în prezentul articol şi a securităţii reţelelor şi sistemelor informatice ale furnizorilor de servicii, Guvernul: a) prin intermediul organismului naţional de standardizare, asigură aprobarea standardelor naţionale în domeniul securităţii informaţiilor, securităţii cibernetice şi protecţia confidenţialităţii în baza standardelor şi a specificaţiilor tehnice europene şi internaţionale relevante pentru securitatea reţelelor şi a sistemelor informatice; b) la propunerea autorităţii administraţiei publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securităţii cibernetice, aprobă cerinţele specifice de securitate a reţelelor şi sistemelor informatice, în funcţie de sectorul, subsectorul, categoria şi/sau tipul furnizorului de servicii.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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 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 de securitate 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.					
(5) Până la 17 octombrie 2024, 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,		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	5	6	7	8	9
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 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		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	5	6	7	8	9
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).					
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 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.	**Articolul 12. Obligațiile de notificare** (1) Furnizorul de servicii informează imediat autoritatea competentă, dar nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre: a) un incident cibernetic care are un impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului; b) un incident cibernetic al cărui impact semnificativ asupra securității rețelei sau sistemului informatic ori asupra continuității serviciului nu este evident, dar poate fi presupus în mod rezonabil; c) 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. (2) Autoritatea competentă prezintă, fără întârzieri nejustificate însă nu mai târziu de 24 de ore de la primirea informației menționate la alineatul (1), furnizorului de servicii un răspuns, inițial cu privire la incidentul semnificativ și, dacă furnizorul de servicii solicită, orientări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de atenuare impactului incidentului cibernetic. (3) 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	Compatibil			Ministerul Dezvo9ltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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; (b) fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore din	evaluare inițială a incidentului cibernetic cu impact semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili. (4) 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 (3) 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. (5) Un incident cibernetic are un impact semnificativ dacă este îndeplinită cel puțin una dintre următoarele condiții: a) severitatea consecințelor incidentului cibernetic este determinat ca fiind cel puțin înalt în raportul de evaluare a riscurilor rețelei și sistemului informatic, întocmit în conformitate cu prevederile articolul 11 alineatului (2) litera a) și în cerințele prevăzute de actele menționate la articolul 11 alineatul (4); b) din cauza incidentului cibernetic, prestarea serviciului nu poate fi continuată după expirarea perioadei de timp maxime admise stabilite în acordul privind nivelul agreat al serviciilor încheiat în cadrul relațiilor contractuale ale furnizorului de servicii cu alte persoane, sau de cerințele privind continuitatea serviciului stabilite în documentația prevăzută la articolul 11 alineatul (2) litere a) - c); c) continuitatea serviciului unui alt furnizor de servicii este perturbată de incidentul cibernetic; d) furnizorului de servicii care notifică incidentul cibernetic, altui furnizor de servicii sau utilizatorilor serviciilor le-au fost cauzate sau le-ar putea fi cauzate prejudicii materiale sau non-materiale considerabile din cauza incidentului cibernetic. (6) Furnizorul de servicii este obligat să informeze fără întârzieri nejustificate, însă nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre o amenințare cibernetică semnificativă, destinatarii serviciilor pe care le prestează, care ar putea fi afectați de o astfel de				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 litera (b), un prestator de servicii de încredere notifică, în ceea ce privește incidentele semnificative care afectează prestarea serviciilor sale de încredere, echipa CSIRT sau, după caz, autoritatea competentă, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de	amenințare, privind măsurile, inclusiv de ordin corectiv, pe care aceștia le-ar putea lua pentru a evita materializarea amenințării respective. În cazul în care, furnizorul de servicii este în imposibilitate de a identifica și notifica în mod individual destinatarii potențial afectați, acesta informează publicul. În cazul în care constată că materializarea amenințării cibernetice semnificative este iminentă, furnizorul de servicii informează destinatarii serviciilor sale despre amenințarea cibernetică semnificativă propriu-zisă. (7) În cazul în care furnizorul de servicii nu realizează obligațiunile de notificare prevăzute de alineatul (6) în termenul respectiv, autoritatea competentă poate solicita expres realizarea obligațiunii de către furnizorul de servicii sau își poate aroga obligația de notificare a destinatarilor posibil afectați sau publicul, informând despre aceasta furnizorul de servicii. Modul de informare a destinatarilor de către furnizorii de servicii sau de către autoritatea competentă constituie obiect de reglementare a actului normativ prevăzut de alin (9). (8) În cazul soluționării unui incident cibernetic cu impact semnificativ, furnizorul de servicii este obligat, în termen de cel mult o lună de la transmiterea informației actualizate în temeiul alineatului (3), 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. (9) 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.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
la data la care a luat cunoștință de incidentul semnificativ. (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.		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	5	6	7	8	9
(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, 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 12. Obligațiile de notificare** (6) Furnizorul de servicii este obligat să informeze fără întârzieri nejustificate, însă nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre o amenințare cibernetică semnificativă, destinatarii serviciilor pe care le prestează, care ar putea fi afectați de o astfel de amenințare, privind măsurile, inclusiv de ordin corectiv, pe care aceștia le-ar putea lua pentru a evita materializarea amenințării respective. În cazul în care, furnizorul de servicii este în imposibilitate de a identifica și notifica în mod individual destinatarii potențial afectați, acesta informează publicul. În cazul în care constată că materializarea amenințării cibernetice semnificative este iminentă, furnizorul de servicii informează destinatarii serviciilor sale despre amenințarea cibernetică semnificativă propriu-zisă. (7) În cazul în care furnizorul de servicii nu realizează obligațiunile de notificare prevăzute de alineatul (6) în termenul respectiv, autoritatea competentă poate solicita expres realizarea obligațiunii de către furnizorul de servicii sau își poate aroga obligația de notificare a destinatarilor posibil afectați sau publicul, informând despre aceasta furnizorul de servicii. Modul de informare a destinatarilor de către furnizorii de servicii sau de către autoritatea competentă constituie obiect de reglementare a actului normativ prevăzut de alin (9).	Compatibil			Ministerul Dezvoltării Economice și Digitalizării
(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		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	5	6	7	8	9
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) 2022/2557 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) 2022/2557. (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 la o comunicare transmisă în temeiul alineatului (2) de la prezentul articol. Până la 17 octombrie 2024, 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).					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 și entitățile importante să utilizeze servicii de încredere calificate.	**Articolul 11. Măsurile de securitate** (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.	**compatibil**			Ministerul Dezvoltării Economice și Digitalizării Institutul Național pentru Standardizare
(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		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	5	6	7	8	9
adoptat în temeiul articolului 49 din Regulamentul (UE) 2019/881. 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.					
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.	**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 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.	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 Ministerul Dezvoltării Economice și Digitalizării
(2) ENISA, în cooperare cu statele membre și, după caz, după consultarea părților interesate relevante, elaborează		Norme UE neaplicabile	Transpunerea este condiționată de		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
avize și orientări în ceea ce privește domeniile tehnice care ar trebui să fie examinate în legătură cu alineatul (1), precum și în ceea ce privește standardele deja existente, inclusiv standardele naționale, care ar permite reglementarea respectivelor domenii.			aderarea Republicii Moldova la UE		
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		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	5	6	7	8	9
membru în 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					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 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 17 ianuarie 2025, 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);		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	5	6	7	8	9
(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 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:	**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.	**Compatibil**		Suplimentara, 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. Astfel această analiză va fi efectuată și în contextul elaborării proiectului de lege pentru modificarea unor acte normative, în contextul executării art. 23 alin. (2) lit. b) din proiectul de lege	ANRCETI Ministerul Dezvoltării Economice Și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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) 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	Hotărârea ANRCETI nr. 42/2020 privind aprobarea Regulamentului cu privire la gestionarea domeniului de nivel superior .md				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 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	**Articolul 17. Schimbul de informații voluntar** (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 cibernetice 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	Compatibil		Suplimentar în termen de cel mult 12 luni de la data publicării proiectului de lege 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 acorduri de schimb de informații de către autoritățile și instituțiile publice.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 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).	colaborării dintre persoanele juridice de drept public și cele 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.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
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 trata notificările obligatorii cu prioritate față de notificările voluntare.	**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 cibernetice evitate la limită. (3) Notificările menționate la alineatele (1) și (2), 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	**Compatibil**			Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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.	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. (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	**Capitolul IV. SUPRAVEGHERE ȘI CONTROL DE STAT** **Articolul 18. Supravegherea** (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, inclusiv prin efectuarea auditurilor de securitate. (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) 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 19. Controlul de stat** (1) Autoritatea competentă exercită controlul respectării prezentei legi de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr.131/2012 privind controlul de stat a activității de întreprinzător. (2) Autoritatea competentă realizează controlul 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:	Parțial compatibil		Urmează a fi transpus integral prin adoptarea actelor normative de implementare prevăzute la art. 18 alin. (3) și art. 19 alin. (5), precum și în procesul aducerii legislației naționale în concordanță cu prevederile proiectului de lege. Actele respective urmează a fi adoptate de către Guvern, potrivit art. 23 alin. (2) lit. c) în termen de cel mult 12 luni de la data publicării legii.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
respectivele entități, în conformitate cu cadrele legislative și instituționale naționale.	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, neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor prevăzute de prezenta lege de către furnizorul de servicii. (5) Guvernul, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, stabilește separat, pentru furnizorii de servicii – persoane juridice de drept privat și furnizorii de servicii – persoane juridice de drept public, procedurile detaliate privind modul de efectuare a controlului de către autoritatea competentă asupra respectării de către aceștia a obligațiilor ce le revin conform prezentei legi.				

Articolul 32. Măsurile de supraveghere şi de asigurare a respectării legii în ceea ce priveşte entităţile esenţiale (1) Statele membre se asigură că măsurile de supraveghere sau de asigurare a respectării legii impuse entităţilor esenţiale în ceea ce priveşte obligaţiile prevăzute în prezenta directivă sunt efective, proporţionale şi cu efect de descurajare, ţinând seama de circumstanţele fiecărui caz în parte. (2) Statele membre se asigură că autorităţile competente, atunci când îşi exercită sarcinile de supraveghere în ceea ce priveşte entităţile esenţiale, au competenţa de a supune entităţile respective cel puţin: (a) unor inspecţii la faţa locului şi unei supravegheri ex situ, inclusiv unor verificări aleatorii, realizate de profesionişti cu formare corespunzătoare; (b) unor audituri de securitate periodice şi 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 esenţială; (d) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile şi transparente de evaluare a riscurilor, după caz cu cooperarea entităţii în cauză; (e) unor cereri de informaţii 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 şi respectarea obligaţiei de a trimite informaţii autorităţilor competente în temeiul articolului 27; (f) unor cereri de acces la date, la documente şi la orice informaţii necesare	**Capitolul IV. SUPRAVEGHERE ŞI CONTROL DE STAT** **Articolul 18. Supravegherea** (1) Autoritatea competentă exercită funcţia de supraveghere a respectării prevederilor prezentei legi de către furnizorii de servicii prin monitorizarea continuă a modului în care aceştia realizează obligaţiile ce le revin conform prevederilor prezentei legi şi a actelor normative de punere în aplicare a acesteia, inclusiv prin efectuarea auditurilor de securitate. (2) În cazul în care un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluţioneze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluţionarea incidentului cibernetic utilizând, dacă este necesar, asistenţă profesionistă terţă. (3) Modul de aplicare a măsurilor de supraveghere se stabilesc de Guvern, la propunerea autorităţii administraţiei publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul **securităţii cibernetice.** **Articolul 19. Controlul de stat** (1) Autoritatea competentă exercită controlul respectării prezentei legi de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr.131/2012 privind controlul de stat a activităţii de întreprinzător. (2) Autoritatea competentă realizează controlul exclusiv în baza unui act motivat emis în acest scop, în baza evaluării riscurilor pentru securitatea reţelelor şi sistemelor informaţionale ale furnizorilor de servicii, precum şi cu înştiinţarea în prealabil a furnizorului de servicii despre controlul preconizat. (3) În vederea efectuării controlului, autoritatea competentă are dreptul să beneficieze de acces la informaţiile, bunurile şi încăperile deţinute de furnizorul de servicii supus controlului, care sunt necesare realizării obiectivelor controlului. (4) Autoritatea competentă efectuează controale numai în cazul în care:	Parţial compatibil		Urmează a fi transpus integral prin adoptarea actelor normative de implementare prevăzute la art. 18 alin. (3) şi art. 19 alin. (5), precum şi în procesul aducerii legislaţiei naţionale în concordanţă cu prevederile proiectului de lege. Actele respective urmează a fi adoptate de către Guvern, potrivit art. 23 alin. (2) lit. c) în termen de cel mult 12 luni de la data publicării legii.	Ministerul Dezvoltării Economice şi Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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. 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	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, neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor prevăzute de prezenta lege de către furnizorul de servicii. (5) Guvernul, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, stabilește separat, pentru furnizorii de servicii – persoane juridice de drept privat și furnizorii de servicii – persoane juridice de drept public, procedurile detaliate privind modul de efectuare a controlului de către autoritatea competentă asupra respectării de către aceștia a obligațiilor ce le revin conform prezentei legi.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 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					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 lor 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 relevante furnizate sau activitățile relevante desfășurate de entitatea 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					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 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:					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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; (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					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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) 2022/2557 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) 2022/2557 a prezentei directive. După caz, autoritățile competente în temeiul Directivei (UE) 2022/2557 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) 2022/2557. (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) 2022/2554. 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) 2022/2554 atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea prezentei directive de către o entitate esențială, care este desemnată ca fiind un furnizor terț de servicii TIC critice în temeiul articolului 31 din Regulamentul (UE) 2022/ 2554.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		

Articolul 33. Măsuri de supraveghere şi de asigurare a respectării legii în ceea ce priveşte entităţile importante (1) Atunci când li se furnizează dovezi, indicii sau informaţii că o entitate importantă nu ar respecta prezenta directivă, în special articolele 21 şi 23, statele membre se asigură că autorităţile competente iau măsuri, dacă este necesar, prin intermediul unor măsuri de supraveghere ex post. Statele membre se asigură că aceste măsuri sunt efective, proporţionale şi cu efect de descurajare, ţinând seama de circumstanţele fiecărui caz în parte. (2) Statele membre se asigură că autorităţile competente, atunci când îşi exercită sarcinile de supraveghere în ceea ce priveşte entităţile importante, au competenţa de a supune entităţile respective cel puţin: (a) unor inspecţii la faţa locului şi unei supravegheri ex situ ex post realizate de profesionişti 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 şi transparente de evaluare a riscurilor, după caz cu cooperarea entităţii în cauză; (d) unor cereri de informaţii 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 şi respectarea obligaţiei de a transmite informaţii autorităţilor competente în temeiul articolului 27; (e) unor cereri de acces la date, la documente şi la informaţii necesare pentru îndeplinirea sarcinilor lor de supraveghere;	**Capitolul IV. SUPRAVEGHERE ŞI CONTROL DE STAT** **Articolul 18. Supravegherea** (1) Autoritatea competentă exercită funcţia de supraveghere a respectării prevederilor prezentei legi de către furnizorii de servicii prin monitorizarea continuă a modului în care aceştia realizează obligaţiile ce le revin conform prevederilor prezentei legi şi a actelor normative de punere în aplicare a acesteia, inclusiv prin efectuarea auditurilor de securitate. (2) În cazul în care un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluţioneze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluţionarea incidentului cibernetic utilizând, dacă este necesar, asistenţă profesionistă terţă. (3) Modul de aplicare a măsurilor de supraveghere se stabilesc de Guvern, la propunerea autorităţii administraţiei publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul **securităţii cibernetice.** **Articolul 19. Controlul de stat** (1) Autoritatea competentă exercită controlul respectării prezentei legi de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr.131/2012 privind controlul de stat a activităţii de întreprinzător. (2) Autoritatea competentă realizează controlul exclusiv în baza unui act motivat emis în acest scop, în baza evaluării riscurilor pentru securitatea reţelelor şi sistemelor informaţionale ale furnizorilor de servicii, precum şi cu înştiinţarea în prealabil a furnizorului de servicii despre controlul preconizat. (3) În vederea efectuării controlului, autoritatea competentă are dreptul să beneficieze de acces la informaţiile, bunurile şi încăperile deţinute de furnizorul de servicii supus controlului, care sunt necesare realizării obiectivelor controlului. (4) Autoritatea competentă efectuează controale numai în cazul în care:	Parţial compatibil		Urmează a fi transpus integral prin adoptarea actelor normative de implementare prevăzute la art. 18 alin. (3) şi art. 19 alin. (5), precum şi în procesul aducerii legislaţiei naţionale în concordanţă cu prevederile proiectului de lege. Actele respective urmează a fi adoptate de către Guvern, potrivit art. 23 alin. (2) lit. c) în termen de cel mult 12 luni de la data publicării legii.	Ministerul Dezvoltării Economice şi Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(f) 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. 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	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, neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor prevăzute de prezenta lege de către furnizorul de servicii. (5) Guvernul, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice, stabilește separat, pentru furnizorii de servicii – persoane juridice de drept privat și furnizorii de servicii – persoane juridice de drept public, procedurile detaliate privind modul de efectuare a controlului de către autoritatea competentă asupra respectării de către aceștia a obligațiilor ce le revin conform prezentei legi.				

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 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.					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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) 2022/2554. 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) 2022/2554 atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea prezentei directive de către o entitate importantă, care este desemnată ca fiind un furnizor terț de servicii TIC critice în temeiul articolului 31 din Regulamentul (UE) 2022/2554.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la 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).	**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	Parțial compatibil		Totodată, în conformitate cu art. 23 alin. (2) lit. b) Guvernul urmează să prezinte în termen de 6 luni de la data publicării legii, Parlamentului un proiect de lege pentru modificarea cadrului normativ, inclusiv a Codului Contravențional în vederea completării acestuia cu componențe de contravenții specifice domeniului securității cibernetice.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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 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.					

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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 17 octombrie 2024, precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea Republicii Moldova la UE		
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 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	**Articolul 20. Protecția datelor cu caracter personal** (1) În exercitarea competenței cu care este învestită prin prezenta lege autoritatea competentă prelucrează date cu caracter personal în condițiile stabilite de legislația în acest domeniu. (2) În cazul în care, în procesul exercitării funcțiilor sale 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.	Parțial compatibil		Totodată, în conformitate cu art. 23 alin. (2) lit. b) Guvernul urmează să prezinte, în termen de 6 luni, Parlamentului un proiect de lege pentru modificarea cadrului normativ, inclusiv a Codului Contravențional în vederea completării acestuia cu componențe de contravenții specifice domeniului securității cibernetice.	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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.					
(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.		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 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 17 ianuarie 2025 și notifică acesteia, fără întârziere, orice modificare ulterioară a acestora.	**Articolul 7 din proiectul de lege:** (3) Autoritatea competentă exercită următoarele atribuții principale: ..... g) exercită, atribuțiile organului constatator pentru cauze contravenționale în domeniul securității rețelelor și sistemelor informatice în conformitate cu prevederile Codului contravențional	Parțial compatibil		În conformitate cu prevederile art. 23 alin. (2) lit. b) în termen de 6 luni de la data publicării Legii privind securitatea cibernetică Guvernul va prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege. În acest act normativ vor fi efectuate și modificările de rigoare la Codul contravențional al Republicii Moldova	Ministerul Dezvoltării Economice și Digitalizării
Articolul 37. Asistență reciprocă		Norme UE neaplicabile	Transpunerea este		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
(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 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			condiționată de aderarea Republicii Moldova la UE		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 16 ianuarie 2023. (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	5	6	7	8	9
(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 17 octombrie 2027 și, ulterior, la fiecare 36 de luni, Comisia revizuiește funcționarea prezentei		Norme UE neaplicabile	Transpunerea este condiționată de aderarea		

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
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 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.			Republicii Moldova la UE		
Articolul 41. Transpunerea (1) Până la 17 octombrie 2024, 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 18 octombrie 2024. (2) Atunci când statele membre adoptă măsurile menționate la alineatul (1), 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 18 octombrie 2024.*		Incompatibil		În conformitate cu prevederile art. 23 alin. (2) lit. b) în termen de 6 luni de la data publicării Legii privind securitatea cibernetică Guvernul va prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege. În acest act normativ vor fi efectuate și modificările de rigoare la Legea nr.	Ministerul Dezvoltării Economice și Digitalizării Serviciul de Informații și Securitate

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
				124/2022 privind identificarea electronică și serviciile de încredere, în mod special urmează a fi abrogat art. 39 din această lege.	
Articolul 43. Modificarea Directivei (UE) 2018/1972 *În Directiva (UE) 2018/1972, articolele 40 și 41 se elimină de la 18 octombrie 2024.*		Incompatibil	Transpunerea este condiționată de aderarea Republicii Moldova la UE	În conformitate cu prevederile art. 23 alin. (2) lit. b) în termen de 6 luni de la data publicării Legii privind securitatea cibernetică va prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege. În acest act normativ vor fi efectuate și modificările de rigoare la Legea nr, 241/2007 comunicațiilor electronice, în mod special art. 21 și 22.	
Articolul 44. Abrogarea Directiva (UE) 2016/1148 se abrogă de la 18 octombrie 2024. Trimiterile la directiva abrogată se interpretează ca trimiteri la prezenta directivă și se citesc în conformitate cu tabelul de corespondență din anexa III.		Norme UE neaplicabile	Transpunerea este condiționată de aderarea 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.**	**Articolul 4 Identificarea furnizorilor de servicii** (2) Guvernul aprobă lista sectoarelor, subsectoarelor critice și, corespunzător, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și subsectoare, stabilește cadrul metodologic privind identificarea	Parțial compatibil		În conformitate cu art. 23 alin. (2) lit. c) în termen de 12 luni de la data publicării legii Guvernul va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta	Ministerul Dezvoltării Economice și Digitalizării

Actul Uniunii Europene	Proiectul de act normativ național	Gradul de compatibilitate	Diferențele	Observațiile	Autoritatea/ persoana responsabilă
4	5	6	7	8	9
ALTE SECTOARE DE IMPORTANȚĂ CRITICĂ	persoanelor juridice de drept public și celor de drept privat ca fiind furnizori de servicii, precum și modul de întocmire, ținere și actualizare a listei furnizorilor de servicii. (3) La solicitarea autorității competente, Serviciul de Informații și Securitate furnizează acesteia lista operatorilor care au în gestiunea lor obiective ale infrastructurii critice. (4) Autoritățile publice responsabile de realizarea politicii de stat în sectoarele sau subsectoarele critice, 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, asigură suportul necesar autorității competente, la solicitarea acesteia, în procesul de identificare a furnizorilor de servicii.			actele normative necesare punerii în aplicare a legii, inclusiv va determina autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice. Astfel pentru punerea în aplicare a prevederilor art. 4 Guvernul î temeiul alineatului (2) din acest articol urmează să adopte lista sectoarelor, subsectoarelor, tipurilor și categoriilor de furnizori de servicii, precum și să stabilească cadrul metodologic de identificare a furnizorilor de servicii.	
ANEXA III **TABEL DE CORESPONDENȚĂ**					

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 Parla- mentului European și a Consiliului (1), 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 (2) — 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 (3)
	(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 (4)
	(d) Gaze	— Întreprinderile de furnizare, astfel cum sunt definite la articolul 2 punctul 8 din Directiva 2009/73/CE a Parlamentului European și a Consiliului (5)
		— 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
		— 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 (6), aeroporturile, astfel cum sunt definite la articolul 2 punctul 1 din directiva respectivă, inclusiv aeroportu- rile principale enumerate în secțiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului (7), 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 arti- colul 2 punctul 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului (8)
	(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 (9)

		— Întreprinderile feroviare, astfel cum sunt definite la articolul 3 punctul 1 din Directiva 2012/34/UE, inclusiv operatorii unei infrastruc- turi 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 [10] 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 Euro- pean și a Consiliului [11], 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 [12]
	(d) Transport rutier	— Autoritățile rutiere, astfel cum sunt definite la articolul 2 punctul 12 din Regulamentul delegat (UE) 2015/962 al Comisiei [13] respon- sabile 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 [14]
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 [15]
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 [16]
		— Contrapărțile centrale (CPC), astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului [17]
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 [18]
		— Laboratoarele de referință ale UE, astfel cum sunt definite la articolul 15 din Regulamentul (UE) 2022/2371 al Parlamentului European și al Consiliului [19]
		— 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 [20] — 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
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 [22] 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 și 3 din Directiva 91/271/CEE a Consiliului ([23]) 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
		— 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
		— Furnizorii de IXP (internet *exchange point*)
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

(1) Directiva (UE) 2019/944 a Parlamentului European și a Consiliului din 5 iunie 2019 privind normele comune pentru piața internă de energie electrică și de modificare a Directivei 2012/27/UE (JO L 158, 14.6.2019, p. 125).
(2) Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului din 5 iunie 2019 privind piața internă de energie electrică (JO L 158, 14.6.2019, p. 54).
(3) Directiva (UE) 2018/2001 a Parlamentului European și a Consiliului din 11 decembrie 2018 privind promovarea utilizării energiei din surse regenerabile (JO L 328, 21.12.2018, p. 82).
(4) Directiva 2009/119/CE a Consiliului din 14 septembrie 2009 privind obligația statelor membre de a menține un nivel minim de rezerve de țiței și/sau de produse petroliere (JO L 265, 9.10.2009, p. 9).
(5) Directiva 2009/73/CE a Parlamentului European și a Consiliului din 13 iulie 2009 privind normele comune pentru piața internă în sectorul gazelor naturale și de abrogare a Directivei 2003/55/CE (JO L 211, 14.8.2009, p. 94).
(6) Directiva 2009/12/CE a Parlamentului European și a Consiliului din 11 martie 2009 privind tarifele de aeroport (JO L 70, 14.3.2009, p. 11).
(7) Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului din 11 decembrie 2013 privind orientările Uniunii pentru dezvoltarea rețelei transeuropene de transport și de abrogare a Deciziei nr. 661/2010/UE (JO L 348, 20.12.2013, p. 1).
(8) Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului din 10 martie 2004 de stabilire a cadrului pentru crearea cerului unic european (regulament-cadru) (JO L 96,

31.3.2004, p. 1).

(9) Directiva 2012/34/UE a Parlamentului European și a Consiliului din 21 noiembrie 2012 privind instituirea spațiului feroviar unic european (JO L 343, 14.12.2012, p. 32).

(10) Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului din 31 martie 2004 privind consolidarea securității navelor și a instalațiilor portuare (JO L 129, 29.4.2004, p. 6).

(11) Directiva 2005/65/CE a Parlamentului European și a Consiliului din 26 octombrie 2005 privind consolidarea securității portuare (JO L 310, 25.11.2005, p. 28).

(12) Directiva 2002/59/CE a Parlamentului European și a Consiliului din 27 iunie 2002 de instituire a unui sistem comunitar de monitorizare și informare privind traficul navelor maritime și de abrogare a Directivei 93/75/CEE a Consiliului (JO L 208, 5.8.2002, p. 10).

(13) Regulamentul delegat (UE) 2015/962 al Comisiei din 18 decembrie 2014 de completare a Directivei 2010/40/UE a Parlamentului European și a Consiliului în ceea ce privește prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic (JO L 157, 23.6.2015, p. 21).

(14) Directiva 2010/40/UE a Parlamentului European și a Consiliului din 7 iulie 2010 privind cadrul pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport (JO L 207, 6.8.2010, p. 1).

(15) Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).

(16) Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (JO L 173, 12.6.2014, p. 349).

(17) Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții (JO L 201, 27.7.2012, p. 1).

(18) Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).

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 (1), 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 (2) 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 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 [3] și întreprinderile care produc articole, astfel cum sunt definite la articolul 3 punctul 3 din regulamentul respectiv, din substanțe sau amestecuri
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 [4], 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 [5], cu excepția entităților care fabrică dispozitive medicale menționate în anexa I punctul 5 a cincea liniuță din prezenta
	(b) (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
Sectorul	Subsectorul	Tipul de entitate
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

(1) Directiva 2008/98/CE a Parlamentului European și a Consiliului din 19 noiembrie 2008 privind deșeurile și de abrogare a anumitor directive (JO L 312, 22.11.2008, p. 3).

(2) Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului din 18 decembrie 2006 privind înregistrarea, evaluarea, autorizarea și restricționarea substanțelor chimice (REACH), de înființare a Agenției Europene pentru Produse Chimice, de modificare a Directivei 1999/45/CE și de abrogare a Regulamentului (CEE) nr. 793/93 al Consiliului și a Regulamentului (CE) nr. 1488/94 al Comisiei, precum și a Directivei 76/769/CEE a Consiliului și a Directivelor 91/155/CEE, 93/67/CEE, 93/105/CE și 2000/21/CE ale Comisiei (JO L 396, 30.12.2006, p. 1).

(3) Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului din 18 decembrie 2006 privind înregistrarea, evaluarea, autorizarea și restricționarea substanțelor chimice (REACH), de înființare a Agenției Europene pentru Produse Chimice, de modificare a Directivei 1999/45/CE și de abrogare a Regulamentului (CEE) nr. 793/93 al Consiliului și a Regulamentului (CE) nr. 1488/94 al Comisiei, precum și a Directivei 76/769/CEE a Consiliului și a Directivelor 91/155/CEE, 93/67/CEE, 93/105/CE și 2000/21/CE ale Comisiei (JO L 396, 30.12.2006, p. 1).

(4) Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului (JO L 117, 5.5.2017, p. 1).

(5) Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic in vitro și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5.5.2017, p. 176).

Anexa III
TABEL DE CORESPONDENȚĂ

Directiva (UE) 2016/1148	Prezenta directivă
Articolul 1 alineatul (1)	Articolul 1 alineatul (1)
Articolul 1 alineatul (2)	Articolul 1 alineatul (2)
Articolul 1 alineatul (3)	-
Articolul 1 alineatul (4)	Articolul 2 alineatul (12)
Articolul 1 alineatul (5)	Articolul 2 alineatul (13)
Articolul 1 alineatul (6)	Articolul 2 alineatele (6) și (11)
Articolul 1 alineatul (7)	Articolul 4
Articolul 2	Articolul 2 alineatul (14)

Articolul 3	Articolul 5
Articolul 4	Articolul 6
Articolul 5	–
Articolul 6	–
Articolul 7 alineatul (1)	Articolul 7 alineatele (1) și (2)
Articolul 7 alineatul (2)	Articolul 7 alineatul (4)
Articolul 7 alineatul (3)	Articolul 7 alineatul (3)
Articolul 8 alineatele (1)-(5)	Articolul 8 alineatele (1)-(5)
Articolul 8 alineatul (6)	Articolul 13 alineatul (4)
Articolul 8 alineatul (7)	Articolul 8 alineatul (6)
Articolul 9 alineatele (1), (2) și (3)	Articolul 10 alineatele (1), (2) și (3)
Articolul 9 alineatul (4)	Articolul 10 alineatul (9)
Articolul 9 alineatul (5)	Articolul 10 alineatul (10)
Articolul 10 alineatele (1), (2) și (3) primul paragraf	Articolul 13 alineatele (1), (2) și (3)
Articolul 10 alineatul (3) al doilea paragraf	Articolul 23 alineatul (9)
Articolul 11 alineatul (1)	Articolul 14 alineatele (1) și (2)
Articolul 11 alineatul (2)	Articolul 14 alineatul (3)
Articolul 11 alineatul (3)	Articolul 14 alineatul (4) primul paragraf literele (a)-(q) și (s), și alineatul (7)
Articolul 11 alineatul (4)	Articolul 14 alineatul (4) primul paragraf litera (r) și al doilea paragraf
Articolul 11 alineatul (5)	Articolul 14 alineatul (8)
Articolul 12 alineatele (1)-(5)	Articolul 15 alineatele (1)-(5)
Articolul 13	Articolul 17
Articolul 14 alineatele (1) și (2)	Articolul 21 alineatele (1)-(4)
Articolul 14 alineatul (3)	Articolul 23 alineatul (1)
Articolul 14 alineatul (4)	Articolul 23 alineatul (3)
Articolul 14 alineatul (5)	Articolul 23 alineatele (5), (6) și (8)

Articolul 14 alineatul (6)	Articolul 23 alineatul (7)
Articolul 14 alineatul (7)	Articolul 23 alineatul (11)
Articolul 15 alineatul (1)	Articolul 31 alineatul (1)
Articolul 15 alineatul (2) primul paragraf litera (a)	Articolul 32 alineatul (2) litera (e)
Articolul 15 alineatul (2) primul paragraf litera (b)	Articolul 32 alineatul (2) litera (g)
Articolul 15 alineatul (2) al doilea paragraf	Articolul 32 alineatul (3)
Articolul 15 alineatul (3)	Articolul 32 alineatul (4) litera (b)
Articolul 15 alineatul (4)	Articolul 31 alineatul (3)
Articolul 16 alineatele (1) și (2)	Articolul 21 alineatele (1)-(4)
Articolul 16 alineatul (3)	Articolul 23 alineatul (1)
Articolul 16 alineatul (4)	Articolul 23 alineatul (3)
Articolul 16 alineatul (5)	–
Articolul 16 alineatul (6)	Articolul 23 alineatul (6)
Articolul 16 alineatul (7)	Articolul 23 alineatul (7)
Articolul 16 alineatele (8) și (9)	Articolul 21 alineatul (5) și articolul 23 alineatul (11)
Articolul 16 alineatul (10)	–
Articolul 16 alineatul (11)	Articolul 2 alineatele (1), (2) și (3)
Articolul 17 alineatul (1)	Articolul 33 alineatul (1)
Articolul 17 alineatul (2) litera (a)	Articolul 32 alineatul (2) litera (e)
Articolul 17 alineatul (2) litera (b)	Articolul 32 alineatul (4) litera (b)
Articolul 17 alineatul (3)	Articolul 37 alineatul (1) literele (a) și (b)
Articolul 18 alineatul (1)	Articolul 26 alineatul (1) litera (b) și alineatul (2)
Articolul 18 alineatul (2)	Articolul 26 alineatul (3)
Articolul 18 alineatul (3)	Articolul 26 alineatul (4)

Articolul 19	Articolul 25
Articolul 20	Articolul 30
Articolul 21	Articolul 36
Articolul 22	Articolul 39
Articolul 23	Articolul 40
Articolul 24	–
Articolul 25	Articolul 41
Articolul 26	Articolul 45
Articolul 27	Articolul 46
Anexa I, punctul 1	Articolul 11 alineatul (1)
Anexa I, punctul 2 litera (a) punctele (i)-(iv)	Articolul 11 alineatul (2) literele (a)-(d)
Anexa I, punctul 2 litera (a) punctul (v)	Articolul 11 alineatul (2) litera (f)
Anexa I, punctul 2 litera (b)	Articolul 11 alineatul (4)
Anexa I, punctul 2 litera (c) punctele (i) și (ii)	Articolul 11 alineatul (5) litera (a)
Anexa II	Anexa I
Anexa III, punctele 1 și 2	Anexa II, punctul 6
Anexa III, punctul 3	Anexa I, punctul 8