Tabel comparativ
la proiectul de Lege pentru modificarea unor acte normative
(modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică)

Nr. d/o	Prevederea actuală	Modificarea propusă	Prevederea după modificare
Legea nr. 1456/1993 cu privire la activitatea farmaceutică			
1.	**Articolul 3.** Întreprinderi şi instituţii farmaceutice şi tipurile de proprietate asupra lor (1) La întreprinderile şi instituţiile farmaceutice se raportă întreprinderile farmaceutice industriale, întreprinderile (laboratoarele) de microproducţie farmaceutică, laboratoarele de control al calităţii medicamentelor, depozitele farmaceutice, farmaciile, instituţiile de cercetări farmaceutice, instituţiile farmaceutice ştiinţifico-practice. (2) Întreprinderile şi instituţiile farmaceutice pot fi de stat, private sau cu o formă mixtă de proprietate. Schimbarea formei de proprietate a întreprinderilor farmaceutice se efectuează în conformitate cu legislaţia în vigoare. Statul garantează, în conformitate cu legislaţia în vigoare, condiţii egale de funcţionare a întreprinderilor farmaceutice, indiferent de forma de proprietate a acestora. (3) Întreprinderile şi instituţiile farmaceutice pot înfiinţa filiale în conformitate cu legislaţia în vigoare.	Articolul 3 se completează cu alineatul (5), cu următorul cuprins: „(5) Întreprinderile şi instituţiile farmaceutice, identificate ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligaţiilor de asigurare a securităţii cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare şi de alte acte normative care stabilesc cerinţe specifice de securitate a reţelelor şi sistemelor informatice.”	**Articolul 3.** Întreprinderi şi instituţii farmaceutice şi tipurile de proprietate asupra lor (1) La întreprinderile şi instituţiile farmaceutice se raportă întreprinderile farmaceutice industriale, întreprinderile (laboratoarele) de microproducţie farmaceutică, laboratoarele de control al calităţii medicamentelor, depozitele farmaceutice, farmaciile, instituţiile de cercetări farmaceutice, instituţiile farmaceutice ştiinţifico-practice. (2) Întreprinderile şi instituţiile farmaceutice pot fi de stat, private sau cu o formă mixtă de proprietate. Schimbarea formei de proprietate a întreprinderilor farmaceutice se efectuează în conformitate cu legislaţia în vigoare. Statul garantează, în conformitate cu legislaţia în vigoare, condiţii egale de funcţionare a întreprinderilor farmaceutice, indiferent de forma de proprietate a acestora. (3) Întreprinderile şi instituţiile farmaceutice pot înfiinţa filiale în conformitate cu legislaţia în vigoare.

	(4) Întreprinderile şi instituţiile farmaceutice vor activa în conformitate cu prevederile Regulilor de bune practici, aprobate de către Guvern.		(4) Întreprinderile şi instituţiile farmaceutice vor activa în conformitate cu prevederile Regulilor de bune practici, aprobate de către Guvern. (5) Întreprinderile şi instituţiile farmaceutice, identificate ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.
2.	**Articolul 9.** Cercetări farmacologice şi farmaceutice (1) În scopul creării de medicamente noi se faccercetări orientate spre depistarea de substanţe active din punct de vedere biologic, studierea calităţilor lor farmacologice şi a acţiunii secundare, aprecierea inocuităţii, eficacităţii terapeutice, elaborarea formelor medicamentoase, metodelor de analiză a lor, a criteriilor de standardizare şi a documentaţiei analitico-normative. (2) Investigaţiile în vederea creării Medicamentelor noi se efectuează în instituţii de cercetări ştiinţifice, ştiinţifice de producţie, ştiinţifico-practice, de învăţământ, precum şi de către persoane fizice.	Articolul 9 se completează cu alineatul (3) cu următorul cuprins: „(3) Persoanele care efectuează investigații în vederea creării medicamentelor noi, identificate ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.”	**Articolul 9.** Cercetări farmacologice şi farmaceutice (1) În scopul creării de medicamente noi se faccercetări orientate spre depistarea de substanţe active din punct de vedere biologic, studierea calităţilor lor farmacologice şi a acţiunii secundare, aprecierea inocuităţii, eficacităţii terapeutice, elaborarea formelor medicamentoase, metodelor de analiză a lor, a criteriilor de standardizare şi a documentaţiei analitico-normative. (2) Investigaţiile în vederea creării medicamentelor noi se efectuează în instituţii de cercetări ştiinţifice, ştiinţifice de producţie, ştiinţifico-practice, de învăţământ, precum şi de către persoane fizice. (3) Persoanele care efectuează investigații în vederea creării medicamentelor noi, identificate ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt

			responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.
3.	**Articolul 16.** Modul de efectuare a controlului de stat (1) Controlul de stat al calităţii medicamentelor şi produselor parafarmaceutice produse la întreprinderile şi instituţiile farmaceutice din republică se efectuează în conformitate cu cerinţele Farmacopeei şi altei documentaţii analitico-normative aprobate de Ministerul Sănătăţii. (2) Controlul calităţii medicamentelor, materiei prime medicamentoase şi produselor parafarmaceutice importate se efectuează în conformitate cu prevederile farmacopeelor în vigoare sau în corespundere cu cerinţele documentelor analitico-normative aprobate în modul stabilit de Ministerul Sănătăţii. (3) Controlul de stat al calităţii medicamentelor autohtone şi de import este exercitat de către Agenţia Medicamentului şi Dispozitivelor Medicale. (4) Organele abilitate de Guvern elaborează şi implementează sisteme informaţionale automatizate ce asigură plasarea pe piaţa farmaceutică doar a medicamentelor supuse controlului calităţii şi fabricate sau importate în mod legal.	Articolul 16 se completează cu alineatul (5) cu următorul cuprins: „(5) Supravegherea şi controlul de stat al respectării de către întreprinderile și instituțiile farmaceutice a obligațiilor stabilite la art. 3 alin. (5), precum şi de către persoanele care efectuează investigații în vederea creării medicamentelor noi a obligațiilor stabilite la art. 9 alin. (3), se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”	**Articolul 16.** Modul de efectuare a controlului de stat (1) Controlul de stat al calităţii medicamentelor şi produselor parafarmaceutice produse la întreprinderile şi instituţiile farmaceutice din republică se efectuează în conformitate cu cerinţele Farmacopeei şi altei documentaţii analitico-normative aprobate de Ministerul Sănătăţii. (2) Controlul calităţii medicamentelor, materiei prime medicamentoase şi produselor parafarmaceutice importate se efectuează în conformitate cu prevederile farmacopeelor în vigoare sau în corespundere cu cerinţele documentelor analitico-normative aprobate în modul stabilit de Ministerul Sănătăţii. (3) Controlul de stat al calităţii medicamentelor autohtone şi de import este exercitat de către Agenţia Medicamentului şi Dispozitivelor Medicale. (4) Organele abilitate de Guvern elaborează şi implementează sisteme informaţionale automatizate ce asigură plasarea pe piaţa farmaceutică doar a medicamentelor supuse controlului calităţii şi fabricate sau importate în mod legal.

			(5) Supravegherea și controlul de stat al respectării de către întreprinderile și instituțiile farmaceutice a obligațiilor stabilite la art. 3 alin. (5), precum și de către persoanele care efectuează investigații în vederea creării medicamentelor noi a obligațiilor stabilite la art. 9 alin. (3), se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.
Articolul 4 din Legea ocrotirii sănătății nr. 411/1995			
1.	**Articolul 4.** Prestatorii de servicii medicale (1) Prestatorii de servicii medicale pot fi publici sau privați. Prestatorii publici de servicii medicale sînt instituțiile medico-sanitare publice și autoritățile/instituțiile bugetare. (2) Instituţia medico-sanitară publică se instituie prin decizie a Ministerului Sănătății sau a autorității administrației publice locale, în baza nomenclatorului prestatorilor de servicii medicale aprobat conform alin. (5). Instituţia medico-sanitară publică departamentală se instituie prin decizie a autorității centrale de specialitate. (2^1) Conducătorii instituţiilor medico-sanitare publice republicane, municipale, raionale sînt selectaţi prin concurs organizat de Ministerul Sănătății şi sînt numiţi în funcţie de către persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, președinte de raion). Eliberarea din funcție a	Se completează cu alineatele (8) și (9), cu următorul cuprins: „(8) Prestatorii de servicii medicale, identificați în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică ca furnizori de servicii, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice. (9) Supravegherea și controlul de stat al respectării de către prestatorii de servicii medicale a obligațiilor prevăzute la alin. (8) se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”	**Articolul 4.** Prestatorii de servicii medicale (1) Prestatorii de servicii medicale pot fi publici sau privați. Prestatorii publici de servicii medicale sînt instituțiile medico-sanitare publice și autoritățile/instituțiile bugetare. (2) Instituţia medico-sanitară publică se instituie prin decizie a Ministerului Sănătății sau a autorității administrației publice locale, în baza nomenclatorului prestatorilor de servicii medicale aprobat conform alin. (5). Instituţia medico-sanitară publică departamentală se instituie prin decizie a autorității centrale de specialitate. (2^1) Conducătorii instituţiilor medico-sanitare publice republicane, municipale, raionale sînt selectaţi prin concurs organizat de Ministerul Sănătății şi sînt numiţi în funcţie de către persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, președinte de raion). Eliberarea din funcție a conducătorilor instituţiilor medico-sanitare publice republicane,

	conducătorilor instituţiilor medico-sanitare publice republicane, municipale, raionale se efectuează de către persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, preşedinte de raion). Regulamentul privind numirea în funcţie a conducătorilor instituţiilor medico-sanitare publice în bază de concurs se aprobă de Guvern. (2^2) Conducătorul instituţiei medico-sanitare publice gestionează instituţia în baza unui contract de management încheiat cu persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, preşedinte de raion) pe o durată de 5 ani, conform contractului-tip de management al instituţiei medico-sanitare publice aprobat de Guvern. La expirarea termenului de 5 ani, funcţia de conducător al instituţiei medico-sanitare publice devine vacantă. Funcţia de conducător al instituţiei medico-sanitare publice nu poate fi ocupată de către persoana care activează concomitent în cadrul unui prestator privat de servicii medicale sau farmaceutice. (3) Persoanele fizice şi persoanele juridice au dreptul să fondeze prestatori privaţi de servicii medicale şi poartă răspundere pentru asigurarea lor financiară şi tehnico-materială, pentru organizarea de asistenţă medicală şi pentru calitatea ei, conform legislaţiei în vigoare. (4) Prestatorii privaţi de servicii medicale şi farmaceutice, cu excepţia celor prevăzuţi la art. 365, îşi desfăşoară activitatea în spaţiile		municipale, raionale se efectuează de către persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, preşedinte de raion). Regulamentul privind numirea în funcţie a conducătorilor instituţiilor medico-sanitare publice în bază de concurs se aprobă de Guvern. (2^2) Conducătorul instituţiei medico-sanitare publice gestionează instituţia în baza unui contract de management încheiat cu persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, preşedinte de raion) pe o durată de 5 ani, conform contractului-tip de management al instituţiei medico-sanitare publice aprobat de Guvern. La expirarea termenului de 5 ani, funcţia de conducător al instituţiei medico-sanitare publice devine vacantă. Funcţia de conducător al instituţiei medico-sanitare publice nu poate fi ocupată de către persoana care activează concomitent în cadrul unui prestator privat de servicii medicale sau farmaceutice. (3) Persoanele fizice şi persoanele juridice au dreptul să fondeze prestatori privaţi de servicii medicale şi poartă răspundere pentru asigurarea lor financiară şi tehnico-materială, pentru organizarea de asistenţă medicală şi pentru calitatea ei, conform legislaţiei în vigoare. (4) Prestatorii privaţi de servicii medicale şi farmaceutice, cu excepţia celor prevăzuţi la art. 365, îşi desfăşoară activitatea în spaţiile ce le aparţin cu drept de proprietate privată sau în alte spaţii luate în locaţiune, inclusiv ale instituţiilor medico-sanitare publice, cu gen de activitate în domeniul ocrotirii sănătăţii, care corespund

	ce le aparţin cu drept de proprietate privată sau în alte spaţii luate în locaţiune, inclusiv ale instituţiilor medico-sanitare publice, cu gen de activitate în domeniul ocrotirii sănătăţii, care corespund cerinţelor actelor legislative şi normative în vigoare privind parteneriatul public-privat. (5) Regulamentele şi nomenclatorul prestatorilor de servicii medicale, indiferent de tipul de proprietate şi forma juridică de organizare, precum şi lista serviciilor prestate de acestea, sînt aprobate de Ministerul Sănătăţii, cu excepţia celor ale organelor de drept şi ale organelor militare. (6) Parlamentul reorganizează, prin acte legislative, sistemul naţional de sănătate, domeniul medicamentului şi al activităţii farmaceutice. (7) Persoana responsabilă a fondatorului aprobă organigrama şi statele de personal ale prestatorului de servicii medicale.		cerinţelor actelor legislative şi normative în vigoare privind parteneriatul public-privat. (5) Regulamentele şi nomenclatorul prestatorilor de servicii medicale, indiferent de tipul de proprietate şi forma juridică de organizare, precum şi lista serviciilor prestate de acestea, sînt aprobate de Ministerul Sănătăţii, cu excepţia celor ale organelor de drept şi ale organelor militare. (6) Parlamentul reorganizează, prin acte legislative, sistemul naţional de sănătate, domeniul medicamentului şi al activităţii farmaceutice. (7) Persoana responsabilă a fondatorului aprobă organigrama şi statele de personal ale prestatorului de servicii medicale. (8) Prestatorii de servicii medicale, identificați în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică ca furnizori de servicii, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice. (9) Supravegherea și controlul de stat al respectării de către prestatorii de servicii medicale a obligațiilor prevăzute la alin. (8) se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice

			potrivit Legii nr. 48/2023 privind securitatea cibernetică.
Codul navigației maritime comerciale nr. 599/1999			
1.	-	Se completează cu art. 9^1 cu următorul cuprins: „Articolul 9^1. Asigurarea securității rețelelor și sistemelor informatice în navigația maritimă comercială (1) Persoanele juridice care desfășoară activitatea de navigație maritimă comercială pentru transportul de mărfuri și/sau de pasageri, căpităniile porturilor, administrațiile porturilor maritime și întreprinderile și unitățile economice menționate la art. 80 alin. (2), precum și persoanele juridice care operează serviciul de trafic maritim, identificate ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia.”	**Articolul 9^1.** Asigurarea securității rețelelor și sistemelor informatice în navigația maritimă comercială (1) Persoanele juridice care desfășoară activitatea de navigație maritimă comercială pentru transportul de mărfuri și/sau de pasageri, căpităniile porturilor, administrațiile porturilor maritime și întreprinderile și unitățile economice menționate la art. 80 alin. (2), precum și persoanele juridice care operează serviciul de trafic maritim, identificate ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia.
Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat			
1.	**Articolul 3.** Noțiuni principale	La articolul 3, definiția noțiunii „securitate cibernetică” va avea următorul cuprins „ – astfel	**Articolul 3.** Noțiuni principale

	securitate cibernetică – stare de normalitate a sistemului și resursei informaționale, rezultată în urma aplicării unui ansamblu de măsuri prin care este asigurată autenticitatea, integritatea, confidențialitatea, disponibilitatea și nonrepudierea datelor;	cum este definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică”;	*securitate cibernetică* — astfel cum este definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică
2.	**Articolul 10.** Securitatea sistemelor și resurselor informaționale de stat (1) Securitatea, inclusiv securitatea cibernetică, a sistemelor și resurselor informaționale de stat este asigurată de către autoritățile publice, instituțiile publice și alte entități de stat, în limita competențelor acestora și în conformitate cu reglementările stabilite de către Guvern.	La articolul 10, alineatul (1), va avea următorul cuprins: „(1) În scopul asigurării securității sistemelor și resurselor informaționale de stat, autoritățile publice, instituțiile publice și alte entități de stat sunt responsabile de realizarea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere în aplicare a acesteia și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.”	**Articolul 10.** Securitatea sistemelor și resurselor informaționale de stat (1) În scopul asigurării securității sistemelor și resurselor informaționale de stat, autoritățile publice, instituțiile publice și alte entități de stat sunt responsabile de realizarea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere în aplicare a acesteia și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.
3.	**Articolul 22.** Atribuțiile Guvernului În vederea executării prezentei legi, Guvernul: a) aprobă documente de politici și reglementări în domeniul informatizării, al sistemelor și resurselor informaționale de stat; b) stabilește împuternicirile autorităților și instituțiilor publice în domeniul creării, administrării, mentenanței, dezvoltării și utilizării sistemelor și resurselor informaționale de stat; c) aprobă crearea sistemelor și resurselor informaționale de stat; d) aprobă conceptele sistemelor informaționale de stat și regulamentele resurselor informaționale de stat;	La articolul 22, litera e) va avea următorul cuprins: „e) aprobă regulile și modul de găzduire a sistemelor și resurselor informaționale de stat în cadrul centrelor de date amplasate în Republica Moldova sau pe teritoriul statelor membre ale Uniunii Europene;”	**Articolul 22.** Atribuțiile Guvernului În vederea executării prezentei legi, Guvernul: a) asigură realizarea politicii statului în domeniul informatizării și resurselor informaționale de stat prin intermediul ministerelor și altor autorități administrative centrale; b) determină competența ministerelor, a altor autorități administrative centrale, a structurilor organizaționale din sfera de competență ale acestora și a altor autorități și instituții publice; c) aprobă crearea sistemelor și resurselor informaționale de stat; d) aprobă conceptele sistemelor informaționale de stat și regulamentele resurselor informaționale de stat;

	e) aprobă regulile și modul de găzduire a sistemelor informaționale de stat.		e) aprobă regulile și modul de găzduire a sistemelor și resurselor informaționale de stat în cadrul centrelor de date amplasate în Republica Moldova sau pe teritoriul statelor membre ale Uniunii Europene.
Legea comunicațiilor electronice nr. 241/2007			
1.	**Art. 21. -** (1) În scopul asigurării securității și integrității rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului, furnizorii au obligația: a) de a lua toate măsurile tehnice și organizatorice adecvate pentru a administra riscurile care pot afecta securitatea rețelelor și serviciilor. Măsurile luate trebuie să asigure un nivel de securitate corespunzător riscului identificat și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și rețelelor interconectate, avînd în vedere cele mai noi tehnologii; b) de a lua măsurile necesare pentru a garanta integritatea rețelelor și pentru a asigura continuitatea furnizării serviciilor prin intermediul acestor rețele; c) de a notifica Agenția și, după caz, organele împuternicite, în cel mai scurt timp, cu privire la orice caz de încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra furnizării rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului; d) de a colabora între ei, după caz, pentru implementarea măsurilor prevăzute la lit. a) și b).	Articolul 21 va avea următorul cuprins: „(1) În scopul asigurării securității și integrității rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului, furnizorii sunt responsabili de realizarea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere în aplicare a acesteia și de alte acte normative care stabilesc cerințele specifice de asigurare a securității cibernetice. (2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia. (3) În exercitarea supravegherii și controlului respectării prevederilor Legii nr. 48/2023 privind securitatea cibernetică, autoritatea competentă în temeiul acestei legi informează, în termen de 5 zile, Agenția despre încălcările depistate și eventualele sancțiuni aplicate.”	**Articolul 21.** (1) În scopul asigurării securității și integrității rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului, furnizorii sunt responsabili de realizarea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere în aplicare a acesteia și de alte acte normative care stabilesc cerințele specifice de asigurare a securității cibernetice. (2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia. (3) În exercitarea supravegherii și controlului respectării prevederilor Legii nr. 48/2023 privind securitatea cibernetică, autoritatea competentă în temeiul acestei legi informează, în termen de 5 zile, Agenția despre încălcările depistate și eventualele sancțiuni aplicate.

	(2) Măsurile minime de securitate pe care trebuie să le stabilească și să le implementeze furnizorii astfel încît să îndeplinească obligațiile prevăzute la alin. (1) lit. a) și b) vor viza cel puțin următoarele domenii: a) politica de securitate și managementul riscului; b) securitatea resurselor umane; c) securitatea și integritatea rețelelor, infrastructurii asociate și informațiilor; d) managementul operațiunilor; e) managementul incidentelor; f) managementul continuității afacerii; g) monitorizare, testare și audit. (3) Agenția poate informa publicul cu privire la existența cazului specificat la alin. (1) lit. c) sau poate solicita furnizorului să informeze publicul cu privire la existența acestui caz atunci cînd consideră că este în interesul publicului. (4) Agenția poate stabili modalitatea de implementare a prevederilor alin. (1)–(3), inclusiv în legătură cu termenele de punere în aplicare, cu respectarea procedurii de consultare publică.		
2.	**Art. 22.** - (1) În vederea aplicării prevederilor art. 21, Agenția poate solicita furnizorilor de rețele publice de comunicații electronice și/sau servicii de comunicații electronice accesibile publicului: a) să furnizeze toate informațiile necesare evaluării securității și integrității rețelelor și serviciilor, inclusiv a politicilor interne de securitate aplicabile;	Articolul 22 se abrogă.	**Articolul 22.** – *abrogat.*

<table>
<tr><td></td><td>b) să inițieze, pe cont propriu, dar nu mai des decît o dată pe an, un audit de securitate realizat de un organism calificat, independent și să transmită Agenției rezultatele auditului.

(2) Agenția poate verifica și evalua măsurile stabilite de furnizori pentru a garanta securitatea și integritatea rețelelor și/sau serviciilor, precum și respectarea acestora în cazurile de încălcare a securității rețelelor și/sau serviciilor ori de pierdere a integrității rețelelor, avînd posibilitatea de a impune în acest sens măsuri care vor viza stabilirea politicilor, strategiilor, proceselor și procedurilor de asigurare a securității și integrității rețelelor, infrastructurii asociate și informațiilor, resurselor umane, de asemenea poate verifica și evalua managementul operațiunilor, incidentelor, continuității afacerii și procesul de monitorizare.</td><td></td><td></td></tr>
<tr><td colspan="4">Punctul 1 din anexa la Legea nr. 131/2012 privind controlul de stat asupra activității de întreprinzător</td></tr>
<tr><td>1.</td><td>-</td><td>Se completează cu poziția 13[1] cu următorul cuprins:
<table><tr><td>13[1]</td><td>Agenția pentru Securitate Cibernetică</td><td>Supravegherea și controlul de stat al respectării de către furnizorii de servicii a obligațiilor privind asigurarea securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative pentru punerea acesteia în aplicare</td></tr></table></td><td><table><tr><td>13[1]</td><td>Agenția pentru Securitate Cibernetică</td><td>Supravegherea și controlul de stat al respectării de către furnizorii de servicii a obligațiilor privind asigurarea securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative pentru punerea acesteia în aplicare</td></tr></table></td></tr>
</table>

Legea nr. 171/2012 privind piața de capital			
1.	**Articolul 41.** Cerinţe organizatorice generale (1) Societatea de investiţii este obligată să îndeplinească următoarele cerinţe: a) să stabilească, să aplice şi să menţină proceduri decizionale şi o structură organizatorică care să specifice în mod exact şi documentat structurile ierarhice şi să repartizeze funcţii şi responsabilităţi; b) să garanteze că persoanele relevante ale societăţii de investiţii cunosc procedurile ce trebuie urmate pentru îndeplinirea adecvată a responsabilităţilor ce le revin; c) să stabilească, să aplice şi să menţină mecanisme adecvate de control intern concepute pentru a asigura respectarea deciziilor şi procedurilor existente la toate nivelurile societăţii de investiţii; d) să angajeze şi să menţină personal care posedă cunoştinţe, experienţă şi competenţe profesionale, conform cerinţelor stabilite de actele normative ale Comisiei Naţionale; e) să stabilească, să aplice şi să menţină la toate nivelurile importante ale societăţii de investiţii un sistem eficient de raportare internă şi de comunicare a informaţiilor; f) să păstreze o înregistrare adecvată şi ordonată a operaţiunilor efectuate şi a organizării interne; g) să garanteze că îndeplinirea de către persoanele competente a mai multor funcţii nu împiedică şi nu este probabil să împiedice persoanele respective să îndeplinească o anumită funcţie în mod corect, onest şi profesionist;	Se modifică după cum urmează: Articolul 41 se completează cu alineatele (9) şi (10) cu următorul cuprins: „(9) Societăţile de investiţii, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligaţiilor care le revin conform acestei legi, a actelor normative de punere a acesteia în aplicare şi a altor acte normative care stabilesc cerinţe specifice de asigurare a securităţii cibernetice. (10) Supravegherea şi controlul de stat al modului în care societăţile de investiţii îndeplinesc obligaţiile prevăzute la alin. (9) se realizează de către autoritatea competentă în domeniul securităţii cibernetice la nivel naţional în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică”	**Articolul 41.** Cerinţe organizatorice generale (1) Societatea de investiţii este obligată să îndeplinească următoarele cerinţe: a) să stabilească, să aplice şi să menţină proceduri decizionale şi o structură organizatorică care să specifice în mod exact şi documentat structurile ierarhice şi să repartizeze funcţii şi responsabilităţi; b) să garanteze că persoanele relevante ale societăţii de investiţii cunosc procedurile ce trebuie urmate pentru îndeplinirea adecvată a responsabilităţilor ce le revin; c) să stabilească, să aplice şi să menţină mecanisme adecvate de control intern concepute pentru a asigura respectarea deciziilor şi procedurilor existente la toate nivelurile societăţii de investiţii; d) să angajeze şi să menţină personal care posedă cunoştinţe, experienţă şi competenţe profesionale, conform cerinţelor stabilite de actele normative ale Comisiei Naţionale; e) să stabilească, să aplice şi să menţină la toate nivelurile importante ale societăţii de investiţii un sistem eficient de raportare internă şi de comunicare a informaţiilor; f) să păstreze o înregistrare adecvată şi ordonată a operaţiunilor efectuate şi a organizării interne; g) să garanteze că îndeplinirea de către persoanele competente a mai multor funcţii nu împiedică şi nu este probabil să împiedice persoanele respective să îndeplinească o anumită funcţie în mod corect, onest şi profesionist; h) să stabilească, să aplice şi să menţină politici şi practici de remunerare care să promoveze şi

	h) să stabilească, să aplice şi să menţină politici şi practici de remunerare care să promoveze şi să fie în concordanţă cu o gestiune adecvată şi eficace a riscurilor; i) la cererea Comisiei Naţionale sau cel puţin o dată la 4 ani, să efectueze, în conformitate cu actele normative ale Comisiei Naţionale, auditul tehnic al sistemelor informaţionale utilizate. (2) Pentru îndeplinirea cerinţelor stabilite la alin. (1) lit. g), societăţile de investiţii iau în considerare natura, amploarea şi complexitatea activităţilor desfăşurate de ele, precum şi natura şi gama serviciilor şi activităţilor de investiţii întreprinse în cadrul activităţilor respective. (3) Societatea de investiţii este obligată să stabilească, să aplice şi să menţină sisteme şi proceduri adecvate pentru păstrarea securităţii, integrităţii şi confidenţialităţii informaţiilor, ţinînd seama de natura informaţiilor în cauză. (4) Societăţile de investiţii sînt obligate să stabilească, să aplice şi să menţină o politică adecvată de continuitate a activităţii comerciale pentru a asigura, în caz de întrerupere a sistemelor şi a procedurilor lor, conservarea datelor şi funcţiilor fundamentale, precum şi continuarea serviciilor şi activităţilor de investiţii sau, în cazul cînd acest lucru nu este posibil, recuperarea la timp a datelor şi a funcţiilor respective şi reluarea în timp util a serviciilor şi a activităţilor de investiţii.		să fie în concordanţă cu o gestiune adecvată şi eficace a riscurilor; i) la cererea Comisiei Naţionale sau cel puţin o dată la 4 ani, să efectueze, în conformitate cu actele normative ale Comisiei Naţionale, auditul tehnic al sistemelor informaţionale utilizate. (2) Pentru îndeplinirea cerinţelor stabilite la alin. (1) lit. g), societăţile de investiţii iau în considerare natura, amploarea şi complexitatea activităţilor desfăşurate de ele, precum şi natura şi gama serviciilor şi activităţilor de investiţii întreprinse în cadrul activităţilor respective. (3) Societatea de investiţii este obligată să stabilească, să aplice şi să menţină sisteme şi proceduri adecvate pentru păstrarea securităţii, integrităţii şi confidenţialităţii informaţiilor, ţinînd seama de natura informaţiilor în cauză. (4) Societăţile de investiţii sînt obligate să stabilească, să aplice şi să menţină o politică adecvată de continuitate a activităţii comerciale pentru a asigura, în caz de întrerupere a sistemelor şi a procedurilor lor, conservarea datelor şi funcţiilor fundamentale, precum şi continuarea serviciilor şi activităţilor de investiţii sau, în cazul cînd acest lucru nu este posibil, recuperarea la timp a datelor şi a funcţiilor respective şi reluarea în timp util a serviciilor şi a activităţilor de investiţii. (5) Societăţile de investiţii sînt obligate să stabilească, să aplice şi să menţină politici şi proceduri contabile care să le permită să furnizeze, în timp util, autorităţii competente, la cererea acesteia, situaţiile financiare ce ar

	(5) Societăţile de investiţii sînt obligate să stabilească, să aplice şi să menţină politici şi proceduri contabile care să le permită să furnizeze, în timp util, autorităţii competente, la cererea acesteia, situaţiile financiare ce ar reflecta imaginea fidelă şi onestă a situaţiei financiare a societăţilor respective şi ar respecta toate standardele şi normele de contabilitate în vigoare. (6) Societăţile de investiţii sînt obligate să monitorizeze şi să evalueze periodic caracterul adecvat şi eficienţa sistemelor şi mecanismelor lor de control intern şi ale acordurilor încheiate în conformitate cu alin. (1), (3)–(5) şi să adopte măsuri adecvate pentru remedierea eventualelor deficienţe. (7) Cadrele de conducere ale societăţii de investiţii şi, după caz, cadrele de supraveghere a cadrelor de conducere trebuie să evalueze şi să verifice periodic eficienţa politicilor, dispoziţiilor şi procedurilor puse în aplicare şi să adopte măsurile adecvate pentru remedierea eventualelor deficienţe. Această evaluare şi/sau verificare se va efectua în temeiul rapoartelor scrise prezentate de către persoanele responsabile cel puţin o dată pe an. (8) Societatea de investiţii este obligată să stabilească, să aplice şi să menţină proceduri eficiente şi transparente pentru soluţionarea rezonabilă şi promptă a reclamaţiilor primite de la clienţii obişnuiţi sau potenţialii clienţi obişnuiţi şi să înregistreze fiecare reclamaţie		reflecta imaginea fidelă şi onestă a situaţiei financiare a societăţilor respective şi ar respecta toate standardele şi normele de contabilitate în vigoare. (6) Societăţile de investiţii sînt obligate să monitorizeze şi să evalueze periodic caracterul adecvat şi eficienţa sistemelor şi mecanismelor lor de control intern şi ale acordurilor încheiate în conformitate cu alin. (1), (3)–(5) şi să adopte măsuri adecvate pentru remedierea eventualelor deficienţe. (7) Cadrele de conducere ale societăţii de investiţii şi, după caz, cadrele de supraveghere a cadrelor de conducere trebuie să evalueze şi să verifice periodic eficienţa politicilor, dispoziţiilor şi procedurilor puse în aplicare şi să adopte măsurile adecvate pentru remedierea eventualelor deficienţe. Această evaluare şi/sau verificare se va efectua în temeiul rapoartelor scrise prezentate de către persoanele responsabile cel puţin o dată pe an. (8) Societatea de investiţii este obligată să stabilească, să aplice şi să menţină proceduri eficiente şi transparente pentru soluţionarea rezonabilă şi promptă a reclamaţiilor primite de la clienţii obişnuiţi sau potenţialii clienţi obişnuiţi şi să înregistreze fiecare reclamaţie şi măsurile adoptate în vederea soluţionării acesteia. „(9) Societăţile de investiţii, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea

	şi măsurile adoptate în vederea soluţionării acesteia.		cibernetică, sunt responsabile pentru îndeplinirea obligațiilor care le revin conform acestei legi, a actelor normative de punere a acesteia în aplicare și a altor acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (10) Supravegherea și controlul de stat al modului în care societățile de investiții îndeplinesc obligațiile prevăzute la alin. (9) se realizează de către autoritatea competentă în domeniul securității cibernetice la nivel național în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.
2.	**Articolul 62.** Cerinţe privind activitatea operatorilor de piaţă (1) Operatorul de piaţă este obligat să elaboreze şi să aplice politici în scopul prestării serviciilor şi menţinerii activităţii la cele mai bune condiţii, inclusiv: a) de identificare şi administrare a conflictelor de interese ce pot apărea între deţinătorii de acţiuni în capitalul social al operatorului de piaţă, angajaţii operatorului de piaţă, membrii pieţei reglementate şi clienţii acestora, şi participanţii pieţei reglementate; b) de audit intern; c) privind securitatea, integritatea şi confidenţialitatea informaţiilor interne; d) privind identificarea şi gestionarea riscurilor. (2) Operatorul de piaţă este obligat:	Se modifică după cum urmează: Articolul 62 se completează cu alineatele (4) și (5) cu următorul cuprins: „(4) Operatorii de piață, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor care le revin conform acestei legi, conform actelor normative de punere a acesteia în aplicare și conform altor acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (5) Supravegherea și controlul de stat al modului în care operatorii de piață îndeplinesc obligațiile respective se realizează de către autoritatea competentă în domeniul securității cibernetice la nivel național în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.”	**Articolul 62.** Cerinţe privind activitatea operatorilor de piaţă (1) Operatorul de piaţă este obligat să elaboreze şi să aplice politici în scopul prestării serviciilor şi menţinerii activităţii la cele mai bune condiţii, inclusiv: a) de identificare şi administrare a conflictelor de interese ce pot apărea între deţinătorii de acţiuni în capitalul social al operatorului de piaţă, angajaţii operatorului de piaţă, membrii pieţei reglementate şi clienţii acestora, şi participanţii pieţei reglementate; b) de audit intern; c) privind securitatea, integritatea şi confidenţialitatea informaţiilor interne; d) privind identificarea şi gestionarea riscurilor. (2) Operatorul de piaţă este obligat: a) să dispună de dotarea tehnică corespunzătoare pentru a menţine funcţionarea sistemelor de

	a) să dispună de dotarea tehnică corespunzătoare pentru a menţine funcţionarea sistemelor de tranzacţionare şi de finalizare a tranzacţiilor cu instrumente financiare; b) să dispună de resursele necesare pentru a asigura activitatea ordonată şi continuă a pieţei reglementate, avîndu-se în vedere natura, volumul şi periodicitatea tranzacţiilor, precum şi riscurile la care sînt expuse; c) să elaboreze şi, în caz de necesitate, să aplice un plan de urgenţă privind recuperarea datelor în caz de disfuncţiuni şi de testare periodică a sistemelor backup; d) să instituie mecanisme şi proceduri ce vor asigura finalizarea eficientă şi la timp a tranzacţiilor încheiate în cadrul pieţei reglementate; e) să efectueze auditul obligatoriu al situațiilor financiare; f) la cererea Comisiei Naționale sau cel puțin o dată la 4 ani, să efectueze, în conformitate cu actele normative ale Comisiei Naționale, auditul tehnic al sistemelor informaționale utilizate. (3) Prevederile art. 39 alin. (4)–(6) şi art. 40 se aplică corespunzător operatorilor de piață.		tranzacţionare şi de finalizare a tranzacţiilor cu instrumente financiare; b) să dispună de resursele necesare pentru a asigura activitatea ordonată şi continuă a pieţei reglementate, avîndu-se în vedere natura, volumul şi periodicitatea tranzacţiilor, precum şi riscurile la care sînt expuse; c) să elaboreze şi, în caz de necesitate, să aplice un plan de urgenţă privind recuperarea datelor în caz de disfuncţiuni şi de testare periodică a sistemelor backup; d) să instituie mecanisme şi proceduri ce vor asigura finalizarea eficientă şi la timp a tranzacţiilor încheiate în cadrul pieţei reglementate; e) să efectueze auditul obligatoriu al situațiilor financiare; f) la cererea Comisiei Naționale sau cel puțin o dată la 4 ani, să efectueze, în conformitate cu actele normative ale Comisiei Naționale, auditul tehnic al sistemelor informaționale utilizate. (3) Prevederile art. 39 alin. (4)–(6) şi art. 40 se aplică corespunzător operatorilor de piață. (4) Operatorii de piață, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor care le revin conform acestei legi, conform actelor normative de punere a acesteia în aplicare și conform altor acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

			(5) Supravegherea și controlul de stat al modului în care operatorii de piață îndeplinesc obligațiile respective se realizează de către autoritatea competentă în domeniul securității cibernetice la nivel național în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.
Legea nr. 176/2013 privind transportul naval intern al Republicii Moldova			
1.	-	Se completează cu articolul 37[1], cu următorul cuprins: **„Articolul 37[1]. Asigurarea securității cibernetice** (1) Persoanele juridice care prestează servicii de transport de încărcături și/sau de pasageri și bagaje în domeniul transportului naval intern al Republicii Moldova și administrațiile portuare de stat ale transportului naval intern, identificate ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea	**Articolul 37[1].** Asigurarea securității cibernetice (1) Persoanele juridice care prestează servicii de transport de încărcături și/sau de pasageri și bagaje în domeniul transportului naval intern al Republicii Moldova și administrațiile portuare de stat ale transportului naval intern, identificate ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia.

		cibernetică şi actele normative de punere în aplicare a acesteia.”	
Legea nr. 303/2013 privind serviciul public de alimentare cu apă și de canalizare			
1.	**Articolul 9.** Supravegherea şi controlul de stat al serviciului public de alimentare cu apă şi de canalizare Supravegherea şi controlul de stat al serviciului public de alimentare cu apă şi de canalizare se efectuează de către: a) serviciul supravegherii de stat a sănătăţii publice; b) organul de protecţie a mediului înconjurător; c) serviciul de administrare şi de supraveghere a resurselor de apă; d) organul de control asupra aplicării legislaţiei şi a documentelor normative în construcţii.	Articolul 9 se completează cu litera e) cu următorul cuprins: „e) autoritatea competentă la nivel național să exercite supravegherea și controlul de stat a respectării legislației în domeniul securității cibernetice.”;	**Articolul 9.** Supravegherea şi controlul de stat al serviciului public de alimentare cu apă şi de canalizare Supravegherea şi controlul de stat al serviciului public de alimentare cu apă şi de canalizare se efectuează de către: a) serviciul supravegherii de stat a sănătăţii publice; b) organul de protecţie a mediului înconjurător; c) serviciul de administrare şi de supraveghere a resurselor de apă; d) organul de control asupra aplicării legislaţiei şi a documentelor normative în construcţii; e) autoritatea competentă la nivel național să exercite supravegherea și controlul de stat a respectării legislației în domeniul securității cibernetice.
2.	**Articolul 9[1].** Efectuarea controalelor (1) Agenția monitorizează și verifică, prin control, activitatea operatorilor pentru asigurarea respectării legislației din domeniu în desfășurarea activității licențiate, a respectării principiului costurilor necesare și justificate la calcularea tarifelor pentru serviciul de alimentare cu apă și de canalizare, având și alte competențe acordate prin prezenta lege. (2) În vederea asigurării prevederilor alin. (1), Agenția efectuează controale și stabilește, în funcție de complexitate, durata necesară	Articolul 9[I] se completează cu alineatul (4) cu următorul cuprins: „(4) Supravegherea și controlul de stat al respectării de către operatori a obligațiilor stabilite la art. 15 alin. (3)1 se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”	**Articolul 9[1].** Efectuarea controalelor (1) Agenția monitorizează și verifică, prin control, activitatea operatorilor pentru asigurarea respectării legislației din domeniu în desfășurarea activității licențiate, a respectării principiului costurilor necesare și justificate la calcularea tarifelor pentru serviciul de alimentare cu apă și de canalizare, având și alte competențe acordate prin prezenta lege. (2) În vederea asigurării prevederilor alin. (1), Agenția efectuează controale și stabilește, în funcție de complexitate, durata necesară pentru efectuarea acestora, care nu trebuie să

	pentru efectuarea acestora, care nu trebuie să depășească 90 de zile. Perioada de întocmire a raportului de control și de prezentare a acestuia operatorilor supuși controlului nu poate depăși 30 de zile lucrătoare de la data încheierii controlului. Rapoartele privind rezultatele controlului, întocmite de angajații Agenției, se înaintează Consiliului de administrație spre examinare, care, prin hotărîre, se pronunță pe marginea acestora și dispune, după caz, luarea de măsuri pentru înlăturarea abaterilor constatate și/sau pentru aplicarea unor sancțiuni. (3) Agenția efectuează controale planificate sau controale inopinate, din oficiu sau la cerere, în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat asupra activității de întreprinzător.		depășească 90 de zile. Perioada de întocmire a raportului de control și de prezentare a acestuia operatorilor supuși controlului nu poate depăși 30 de zile lucrătoare de la data încheierii controlului. Rapoartele privind rezultatele controlului, întocmite de angajații Agenției, se înaintează Consiliului de administrație spre examinare, care, prin hotărîre, se pronunță pe marginea acestora și dispune, după caz, luarea de măsuri pentru înlăturarea abaterilor constatate și/sau pentru aplicarea unor sancțiuni. (3) Agenția efectuează controale planificate sau controale inopinate, din oficiu sau la cerere, în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat asupra activității de întreprinzător. (4) Supravegherea și controlul de stat al respectării de către operatori a obligațiilor stabilite la art. 15 alin. (3)[1] se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.
3.	**Articolul 15.** Obligațiile operatorului (1) Operatorul este obligat: a) să îndeplinească condițiile stipulate în licență; b) să prezinte Agenției sau autorității administrației publice locale, după caz, calculele argumentate ale cheltuielilor suportate; c) să nu întrerupă furnizarea/prestarea serviciului public de alimentare cu apă și de canalizare, cu excepția cazurilor de neplată, a	Articolul 15 se completează cu alineatul (3)[1], cu următorul cuprins: „(3)[1] Operatorii, identificați ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare și de	**Articolul 15.** Obligațiile operatorului (1) Operatorul este obligat: a) să îndeplinească condițiile stipulate în licență; b) să prezinte Agenției sau autorității administrației publice locale, după caz, calculele argumentate ale cheltuielilor suportate; c) să nu întrerupă furnizarea/prestarea serviciului public de alimentare cu apă și de canalizare, cu excepția cazurilor de neplată, a motivelor tehnice și de securitate prevăzute în lege, în licență și în contracte;

	motivelor tehnice şi de securitate prevăzute în lege, în licenţă şi în contracte; d) să ţină contabilitatea în modul şi în condiţiile prevăzute de lege; e) să prezinte, în termenele stabilite, autorităţii administraţiei publice locale, autorităţii centrale de specialitate, precum şi Agenţiei, informaţia solicitată de acestea, să asigure accesul reprezentanţilor acestora la toate documentele ce conţin informaţii necesare pentru verificarea şi evaluarea funcţionării şi dezvoltării serviciului, să prezinte în termen Agenţiei şi autorităţii administraţiei publice locale rapoarte privind activitatea desfăşurată; f) să nu transmită altor persoane fizice sau juridice drepturi şi obligaţii aferente activităţii pe care operatorul o desfăşoară şi pentru care i s-a acordat licenţă şi s-a încheiat contract de delegare a gestiunii; g) să achite plăţile regulatorii în termenele stabilite prin lege; h) să prezinte anual spre avizare și aprobare tarifele pentru serviciul public de alimentare cu apă potabilă, pentru serviciul public de canalizare și de epurare a apelor uzate. (2) În raport cu consumatorii, operatorul are următoarele obligaţii: a) să asigure furnizarea/prestarea serviciului public de alimentare cu apă şi de canalizare tuturor consumatorilor din teritoriul în ale cărui limite a fost autorizat, cu respectarea prevederilor Regulamentului de organizare și furnizare/prestare a serviciului public de alimentare cu apă şi de canalizare și ale legislației în vigoare;	alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.”	d) să ţină contabilitatea în modul şi în condiţiile prevăzute de lege; e) să prezinte, în termenele stabilite, autorităţii administraţiei publice locale, autorităţii centrale de specialitate, precum şi Agenţiei, informaţia solicitată de acestea, să asigure accesul reprezentanţilor acestora la toate documentele ce conţin informaţii necesare pentru verificarea şi evaluarea funcţionării şi dezvoltării serviciului, să prezinte în termen Agenţiei şi autorităţii administraţiei publice locale rapoarte privind activitatea desfăşurată; f) să nu transmită altor persoane fizice sau juridice drepturi şi obligaţii aferente activităţii pe care operatorul o desfăşoară şi pentru care i s-a acordat licenţă şi s-a încheiat contract de delegare a gestiunii; g) să achite plăţile regulatorii în termenele stabilite prin lege; h) să prezinte anual spre avizare și aprobare tarifele pentru serviciul public de alimentare cu apă potabilă, pentru serviciul public de canalizare și de epurare a apelor uzate. (2) În raport cu consumatorii, operatorul are următoarele obligaţii: a) să asigure furnizarea/prestarea serviciului public de alimentare cu apă şi de canalizare tuturor consumatorilor din teritoriul în ale cărui limite a fost autorizat, cu respectarea prevederilor Regulamentului de organizare și furnizare/prestare a serviciului public de alimentare cu apă şi de canalizare și ale legislației în vigoare; b) să furnizeze serviciul public de alimentare cu apă şi de canalizare în locurile autorizate, ţinînd cont de punctele de delimitare a reţelelor şi

	b) să furnizeze serviciul public de alimentare cu apă şi de canalizare în locurile autorizate, ţinînd cont de punctele de delimitare a reţelelor şi instalaţiilor, în baza unui contract încheiat cu consumatorul, şi să respecte angajamentele contractuale; c) să asigure funcţionarea, la parametrii proiectaţi, a sistemelor publice de alimentare cu apă şi de canalizare, să respecte indicatorii de performanță a serviciului public de alimentare cu apă şi de canalizare stabiliţi de autoritatea publică locală şi să asigure continuitatea serviciului respectiv la punctul de delimitare a reţelelor la parametrii fizici şi calitativi; d) să elibereze avize de racordare/branşare la reţeaua publică de apă şi de canalizare în termen de cel mult 20 de zile calendaristice din momentul de depunere a solicitării şi a prezentării documentelor necesare indicate în Regulamentul de organizare şi funcționare a serviciului public de alimentare cu apă şi de canalizare; e) să informeze consumatorii, cel puţin cu 3 zile înainte, prin mass-media şi/sau prin afişare la scările blocurilor locative, despre orice întrerupere a furnizării apei şi/sau a preluării apelor uzate în cazul unor lucrări planificate de modernizare, reparaţie şi întreţinere; f) să întreprindă măsuri de remediere, în termenele stabilite prin actele normative în domeniu, a defecţiunilor produse în reţelele sale; g) să instaleze, să repare, să înlocuiască şi să verifice metrologic contoarele de apă conform prevederilor art. 26;		instalaţiilor, în baza unui contract încheiat cu consumatorul, şi să respecte angajamentele contractuale; c) să asigure funcţionarea, la parametrii proiectaţi, a sistemelor publice de alimentare cu apă şi de canalizare, să respecte indicatorii de performanță a serviciului public de alimentare cu apă şi de canalizare stabiliţi de autoritatea publică locală şi să asigure continuitatea serviciului respectiv la punctul de delimitare a reţelelor la parametrii fizici şi calitativi; d) să elibereze avize de racordare/branşare la reţeaua publică de apă şi de canalizare în termen de cel mult 20 de zile calendaristice din momentul de depunere a solicitării şi a prezentării documentelor necesare indicate în Regulamentul de organizare şi funcționare a serviciului public de alimentare cu apă şi de canalizare; e) să informeze consumatorii, cel puţin cu 3 zile înainte, prin mass-media şi/sau prin afişare la scările blocurilor locative, despre orice întrerupere a furnizării apei şi/sau a preluării apelor uzate în cazul unor lucrări planificate de modernizare, reparaţie şi întreţinere; f) să întreprindă măsuri de remediere, în termenele stabilite prin actele normative în domeniu, a defecţiunilor produse în reţelele sale; g) să instaleze, să repare, să înlocuiască şi să verifice metrologic contoarele de apă conform prevederilor art. 26; h) să nu admită discriminarea consumatorilor, să calculeze plata pentru serviciul furnizat/prestat în baza tarifelor aprobate, a indicaţiilor contoarelor de apă, iar în lipsa acestora, pe durata verificării metrologice periodice, sau în

	h) să nu admită discriminarea consumatorilor, să calculeze plata pentru serviciul furnizat/prestat în baza tarifelor aprobate, a indicaţiilor contoarelor de apă, iar în lipsa acestora, pe durata verificării metrologice periodice, sau în cazul deteriorării din motive ce nu pot fi imputate consumatorului, să calculeze plata pentru volumul de apă consumată, reieşind din volumul mediu lunar, înregistrat în ultimele 3 luni pînă la verificare (deteriorare); i) să informeze consumatorii cu privire la serviciul furnizat/prestat, inclusiv cu privire la eventualele riscuri, calitatea serviciului, condiţiile calitative şi cantitative de deversare a apelor uzate, modificările tarifului şi să prezinte, la cerere, consumatorilor informaţii cu privire la volumul de apă consumată şi referitor la eventualele penalităţi plătite de aceştia; j) să restituie consumatorilor plăţile facturate incorect şi să achite despăgubiri pentru prejudiciile cauzate din vina sa, în conformitate cu actele legislative şi cu alte acte normative în vigoare; k) să achite, în condiţiile legii, proprietarilor din vecinătatea sistemelor publice de alimentare cu apă şi de canalizare prejudiciile cauzate în rezultatul intervenţiilor de retehnologizare, reparaţie, revizie sau în caz de avarii. Proprietarul terenului afectat de exercitarea dreptului de servitute va fi despăgubit pentru prejudiciile cauzate. (3) La desfăşurarea activităţii, operatorul trebuie să respecte obligaţiile referitoare la securitatea, calitatea, eficienţa şi continuitatea		cazul deteriorării din motive ce nu pot fi imputate consumatorului, să calculeze plata pentru volumul de apă consumată, reieşind din volumul mediu lunar, înregistrat în ultimele 3 luni pînă la verificare (deteriorare); i) să informeze consumatorii cu privire la serviciul furnizat/prestat, inclusiv cu privire la eventualele riscuri, calitatea serviciului, condiţiile calitative şi cantitative de deversare a apelor uzate, modificările tarifului şi să prezinte, la cerere, consumatorilor informaţii cu privire la volumul de apă consumată şi referitor la eventualele penalităţi plătite de aceştia; j) să restituie consumatorilor plăţile facturate incorect şi să achite despăgubiri pentru prejudiciile cauzate din vina sa, în conformitate cu actele legislative şi cu alte acte normative în vigoare; k) să achite, în condiţiile legii, proprietarilor din vecinătatea sistemelor publice de alimentare cu apă şi de canalizare prejudiciile cauzate în rezultatul intervenţiilor de retehnologizare, reparaţie, revizie sau în caz de avarii. Proprietarul terenului afectat de exercitarea dreptului de servitute va fi despăgubit pentru prejudiciile cauzate. (3) La desfăşurarea activităţii, operatorul trebuie să respecte obligaţiile referitoare la securitatea, calitatea, eficienţa şi continuitatea furnizării serviciului public de alimentare cu apă şi de canalizare, normele de securitate şi de sănătate a muncii, normele de protecţie a mediului, precum şi prevederile contractelor încheiate cu consumatorii.

	furnizării serviciului public de alimentare cu apă şi de canalizare, normele de securitate şi de sănătate a muncii, normele de protecţie a mediului, precum şi prevederile contractelor încheiate cu consumatorii. (4) Operatorul este obligat să utilizeze mijloace electronice de comunicație, în măsura în care acestea sunt disponibile, funcționale și adecvate circumstanțelor, în raport cu consumatorii și potențialii consumatori, în procesul de comunicare, de soluționare a petițiilor, de negociere, încheiere, executare, modificare și încetare a contractelor. Operatorul nu poate refuza sau ignora examinarea cererilor, reclamațiilor și sesizărilor din motiv că au fost depuse în formă electronică, dacă acestea întrunesc cerințele prevăzute de legislația ce reglementează documentele electronice.		„(3)[1] Operatorii, identificați ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice. (4) Operatorul este obligat să utilizeze mijloace electronice de comunicație, în măsura în care acestea sunt disponibile, funcționale și adecvate circumstanțelor, în raport cu consumatorii și potențialii consumatori, în procesul de comunicare, de soluționare a petițiilor, de negociere, încheiere, executare, modificare și încetare a contractelor. Operatorul nu poate refuza sau ignora examinarea cererilor, reclamațiilor și sesizărilor din motiv că au fost depuse în formă electronică, dacă acestea întrunesc cerințele prevăzute de legislația ce reglementează documentele electronice.
Articolul 14 din Legea comunicațiilor poștale nr. 36/2016			
1.	**Articolul 14.** Responsabilitatea furnizorilor de servicii poştale (1) Furnizorii de servicii poştale sînt responsabili faţă de utilizatori pentru: a) furnizarea serviciilor în condiţiile prevăzute de lege şi de contractul încheiat cu expeditorul; b) paguba care rezultă din pierderea ori deteriorarea totală sau parţială a trimiterii poştale survenită din momentul depunerii	Se completează cu alineatul (7)[2], cu următorul cuprins: „(7)[2] Furnizorii de servicii poștale, identificați ca furnizori de servicii în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru realizarea obligațiilor privind asigurarea securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care	**Articolul 14.** Responsabilitatea furnizorilor de servicii poştale (1) Furnizorii de servicii poştale sînt responsabili faţă de utilizatori pentru: a) furnizarea serviciilor în condiţiile prevăzute de lege şi de contractul încheiat cu expeditorul; b) paguba care rezultă din pierderea ori deteriorarea totală sau parţială a trimiterii poştale survenită din momentul depunerii

	acesteia la oficiul poştal sau la punctul de acces şi pînă la livrarea către destinatar. (1[1]) Furnizorii de servicii poştale sunt responsabili pentru utilizarea datelor cu caracter personal ale utilizatorilor. Datele cu caracter personal se utilizează numai în scopul pentru care au fost acumulate. Accesul la datele cu caracter personal se realizează în condiţiile Legii nr. 133/2011 privind protecţia datelor cu caracter personal. Fără a aduce atingere prevederilor prezentului alineat, furnizorul de serviciu poştal universal transferă în mod electronic date cu caracter personal operatorilor desemnaţi ai ţărilor de destinaţie sau de tranzit, care au nevoie de aceste date pentru a asigura serviciul lor. (2) Pierderile indirecte, beneficiile nerealizate sau daunele morale nu vor fi luate în considerare la calcularea despăgubirii ce urmează a fi plătită de către furnizorii de servicii poştale. (3) Furnizorul de serviciu poştal universal este responsabil pentru trimiterile poştale internaţionale în conformitate cu prevederile tratatelor internaţionale la care Republica Moldova este parte, inclusiv cu obligaţiile care rezultă din actele Uniunii Poştale Universale şi prezenta lege. (4) Furnizorul de serviciu poştal universal poartă răspundere pentru trimiterile poştale interne şi acordă despăgubiri din mijloacele proprii după cum urmează:	stabilesc cerinţe specifice de securitate a reţelelor şi sistemelor informatice pe care aceştia le utilizează la prestarea serviciilor. Supravegherea şi controlul de stat al modului în care sunt îndeplinite obligaţiile stabilite de prezentul alineat se exercită de către autoritatea competentă la nivel naţional în domeniul securităţii cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”	acesteia la oficiul poştal sau la punctul de acces şi pînă la livrarea către destinatar. (1[1]) Furnizorii de servicii poştale sunt responsabili pentru utilizarea datelor cu caracter personal ale utilizatorilor. Datele cu caracter personal se utilizează numai în scopul pentru care au fost acumulate. Accesul la datele cu caracter personal se realizează în condiţiile Legii nr. 133/2011 privind protecţia datelor cu caracter personal. Fără a aduce atingere prevederilor prezentului alineat, furnizorul de serviciu poştal universal transferă în mod electronic date cu caracter personal operatorilor desemnaţi ai ţărilor de destinaţie sau de tranzit, care au nevoie de aceste date pentru a asigura serviciul lor. (2) Pierderile indirecte, beneficiile nerealizate sau daunele morale nu vor fi luate în considerare la calcularea despăgubirii ce urmează a fi plătită de către furnizorii de servicii poştale. (3) Furnizorul de serviciu poştal universal este responsabil pentru trimiterile poştale internaţionale în conformitate cu prevederile tratatelor internaţionale la care Republica Moldova este parte, inclusiv cu obligaţiile care rezultă din actele Uniunii Poştale Universale şi prezenta lege. (4) Furnizorul de serviciu poştal universal poartă răspundere pentru trimiterile poştale interne şi acordă despăgubiri din mijloacele proprii după cum urmează: 1) în caz de pierdere totală, furt total sau deteriorare totală:

	1) în caz de pierdere totală, furt total sau deteriorare totală: a) în mărimea sumei ce constituie 5 tarife de recomandare – pentru o trimitere poştală care face obiectul serviciului de trimitere recomandată; b) în mărimea sumei tarifului plătit – pentru o trimitere poştală care face obiectul serviciului de trimitere cu predare atestată; c) în mărimea valorii declarate – pentru o trimitere poştală care face obiectul serviciului de trimitere cu valoare declarată; d) în mărimea valorii declarate – pentru o trimitere poştală care face obiectul serviciului de trimitere contra ramburs, pînă la momentul livrării la destinatar; e) în mărimea valorii rambursului – pentru o trimitere poştală care face obiectul serviciului de trimitere contra ramburs, după livrarea acesteia destinatarului, cînd furnizorul de servicii poştale a omis încasarea rambursului de la destinatar; f) în mărimea sumei ce constituie 5 tarife – pentru un colet poştal care nu face obiectul serviciului de trimitere cu valoare declarată, indiferent de greutate; 2) în caz de pierdere parţială, furt parţial sau deteriorare parţială: a) în mărimea valorii declarate pentru partea lipsă sau pentru partea deteriorată, înscrisă de expeditor în nota de inventar – pentru o trimitere poştală care face obiectul serviciului de trimitere cu valoare declarată; b) în mărimea cotei-părţi corespunzătoare greutăţii lipsă din valoarea declarată – pentru o trimitere poştală depusă fără notă de		a) în mărimea sumei ce constituie 5 tarife de recomandare – pentru o trimitere poştală care face obiectul serviciului de trimitere recomandată; b) în mărimea sumei tarifului plătit – pentru o trimitere poştală care face obiectul serviciului de trimitere cu predare atestată; c) în mărimea valorii declarate – pentru o trimitere poştală care face obiectul serviciului de trimitere cu valoare declarată; d) în mărimea valorii declarate – pentru o trimitere poştală care face obiectul serviciului de trimitere contra ramburs, pînă la momentul livrării la destinatar; e) în mărimea valorii rambursului – pentru o trimitere poştală care face obiectul serviciului de trimitere contra ramburs, după livrarea acesteia destinatarului, cînd furnizorul de servicii poştale a omis încasarea rambursului de la destinatar; f) în mărimea sumei ce constituie 5 tarife – pentru un colet poştal care nu face obiectul serviciului de trimitere cu valoare declarată, indiferent de greutate; 2) în caz de pierdere parțială, furt parțial sau deteriorare parţială: a) în mărimea valorii declarate pentru partea lipsă sau pentru partea deteriorată, înscrisă de expeditor în nota de inventar – pentru o trimitere poştală care face obiectul serviciului de trimitere cu valoare declarată; b) în mărimea cotei-părţi corespunzătoare greutăţii lipsă din valoarea declarată – pentru o trimitere poştală depusă fără notă de inventar, care face obiectul serviciului de trimitere cu valoare declarată; c) în mărimea cotei-părţi din suma ce constituie 5 tarife, stabilită în raport cu greutatea lipsă sau

	inventar, care face obiectul serviciului de trimitere cu valoare declarată; c) în mărimea cotei-părţi din suma ce constituie 5 tarife, stabilită în raport cu greutatea lipsă sau cu greutatea conţinutului deteriorat – pentru un colet poştal care nu face obiectul serviciului de trimitere cu valoare declarată; 3) în caz de nerespectare a termenelor de distribuire – în mărimea sumei ce constituie 5% din suma tarifului de expediere – pentru fiecare zi de întîrziere, însă nu mai mult de suma totală a tarifului de expediere. (5) Pe lîngă despăgubirile prevăzute la alin. (4) pct. 1), se restituie şi tarifele încasate la depunerea trimiterii poştale la oficiul poştal, cu excepţia taxelor de recomandare şi de asigurare. (6) Furnizorul de servicii poştale poartă răspundere pentru prestarea necorespunzătoare a serviciilor de plăţi poştale şi acordă despăgubiri din mijloacele proprii după cum urmează: a) în caz de neplată a mandatului poştal, a sumelor referitoare la serviciile aferente transferurilor de mijloace băneşti şi a sumelor referitoare la serviciul de intermediere a transferurilor de mijloace băneşti – în mărimea sumei depuse; b) în caz de netransferare a mijloacelor băneşti pe contul bancar al destinatarului – în mărimea sumei viramentului netransferat. (7) Furnizorul de servicii poştale poartă răspundere, conform contractelor încheiate cu		cu greutatea conţinutului deteriorat – pentru un colet poştal care nu face obiectul serviciului de trimitere cu valoare declarată; 3) în caz de nerespectare a termenelor de distribuire – în mărimea sumei ce constituie 5% din suma tarifului de expediere – pentru fiecare zi de întîrziere, însă nu mai mult de suma totală a tarifului de expediere. (5) Pe lîngă despăgubirile prevăzute la alin. (4) pct. 1), se restituie şi tarifele încasate la depunerea trimiterii poştale la oficiul poştal, cu excepţia taxelor de recomandare şi de asigurare. (6) Furnizorul de servicii poştale poartă răspundere pentru prestarea necorespunzătoare a serviciilor de plăţi poştale şi acordă despăgubiri din mijloacele proprii după cum urmează: a) în caz de neplată a mandatului poştal, a sumelor referitoare la serviciile aferente transferurilor de mijloace băneşti şi a sumelor referitoare la serviciul de intermediere a transferurilor de mijloace băneşti – în mărimea sumei depuse; b) în caz de netransferare a mijloacelor băneşti pe contul bancar al destinatarului – în mărimea sumei viramentului netransferat. (7) Furnizorul de servicii poştale poartă răspundere, conform contractelor încheiate cu utilizatorii, pentru pierderea, deteriorarea, lipsa conţinutului, nelivrarea sau încălcarea termenului de livrare a trimiterilor poştale. (7^1) Furnizorul de serviciu poştal universal rămâne responsabil dacă destinatarul sau, în caz de retur la origine, expeditorul unui colet sau al

	utilizatorii, pentru pierderea, deteriorarea, lipsa conţinutului, nelivrarea sau încălcarea termenului de livrare a trimiterilor poştale. (7^1) Furnizorul de serviciu poştal universal rămâne responsabil dacă destinatarul sau, în caz de retur la origine, expeditorul unui colet sau al unei trimiteri cu valoare declarată anunță furnizorul de serviciu poştal universal care i-a înmânat trimiterea că a constatat un prejudiciu, cu condiția că destinatarul sau, după caz, expeditorul nu s-a deplasat de la ghișeul oficiului poştal care i-a înmânat trimiterea poştală. (8) Furnizorul de servicii poştale nu poartă răspundere pentru trimiterile poştale în cazul în care paguba a fost cauzată din vina expeditorului ori ca urmare a circumstanţelor de forţă majoră sau a situaţiilor excepţionale, precum şi pentru trimiterile poştale care au fost primite fără obiecţii de către destinatar.		unei trimiteri cu valoare declarată anunță furnizorul de serviciu poştal universal care i-a înmânat trimiterea că a constatat un prejudiciu, cu condiția că destinatarul sau, după caz, expeditorul nu s-a deplasat de la ghișeul oficiului poştal care i-a înmânat trimiterea poştală. ($7)^2$ Furnizorii de servicii poştale, identificați ca furnizori de servicii în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru realizarea obligațiilor privind asigurarea securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice pe care aceștia le utilizează la prestarea serviciilor. Supravegherea și controlul de stat al modului în care sunt îndeplinite obligațiile stabilite de prezentul alineat se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică. (8) Furnizorul de servicii poştale nu poartă răspundere pentru trimiterile poştale în cazul în care paguba a fost cauzată din vina expeditorului ori ca urmare a circumstanţelor de forţă majoră sau a situaţiilor excepţionale, precum şi pentru trimiterile poştale care au fost primite fără obiecţii de către destinatar.
Legea nr. 209/2016 privind deșeurile			

1.	**Articolul 18.** Obligaţiile gestionarilor de deşeuri (1) Responsabilitatea pentru gestionarea deşeurilor revine după cum urmează: a) producătorul iniţial sau alt deţinător de deşeuri are obligaţia să asigure efectuarea operaţiunii de tratare a deşeurilor prin mijloace proprii sau prin transferarea deşeurilor în vederea efectuării acestei operaţiuni unui agent, unei unităţi sau întreprinderi care desfăşoară activităţi de tratare a deşeurilor ori unei unităţi publice sau private de colectare a deşeurilor, cu respectarea art. 3 şi 4; b) producătorii şi deţinătorii de deşeuri îşi organizează sistemul propriu de tratare/eliminare a deşeurilor dacă deşeurile nu pot fi preluate de unităţi specializate din sistemul organizat în acest scop, cu respectarea art. 4. Livrarea şi primirea deşeurilor, inclusiv a deşeurilor periculoase, în vederea eliminării lor se fac numai în bază de contract. (2) Atunci cînd deşeurile sînt transferate de la producătorul sau deţinătorul iniţial către un agent, către o unitate sau o întreprindere menţionată la alin. (1) lit. a) în vederea efectuării unor operaţiuni de tratare preliminară, acesta nu este scutit, de regulă, de responsabilitatea pentru realizarea operaţiunilor de valorificare sau de eliminare completă. (3) Ţinînd cont de prevederile, procedurile şi regimurile de control pentru transferul de	Articolul 18 se completează cu alineatul (6) cu următorul cuprins: „(6) Persoanele juridice care desfășoară activități de gestionare a deșeurilor, identificate ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru realizarea obligațiilor privind asigurarea securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice pe care aceștia le utilizează la prestarea serviciilor.”	**Articolul 18.** Obligaţiile gestionarilor de deşeuri (1) Responsabilitatea pentru gestionarea deşeurilor revine după cum urmează: a) producătorul iniţial sau alt deţinător de deşeuri are obligaţia să asigure efectuarea operaţiunii de tratare a deşeurilor prin mijloace proprii sau prin transferarea deşeurilor în vederea efectuării acestei operaţiuni unui agent, unei unităţi sau întreprinderi care desfăşoară activităţi de tratare a deşeurilor ori unei unităţi publice sau private de colectare a deşeurilor, cu respectarea art. 3 şi 4; b) producătorii şi deţinătorii de deşeuri îşi organizează sistemul propriu de tratare/eliminare a deşeurilor dacă deşeurile nu pot fi preluate de unităţi specializate din sistemul organizat în acest scop, cu respectarea art. 4. Livrarea şi primirea deşeurilor, inclusiv a deşeurilor periculoase, în vederea eliminării lor se fac numai în bază de contract. (2) Atunci cînd deşeurile sînt transferate de la producătorul sau deţinătorul iniţial către un agent, către o unitate sau o întreprindere menţionată la alin. (1) lit. a) în vederea efectuării unor operaţiuni de tratare preliminară, acesta nu este scutit, de regulă, de responsabilitatea pentru realizarea operaţiunilor de valorificare sau de eliminare completă. (3) Ţinînd cont de prevederile, procedurile şi regimurile de control pentru transferul de deşeuri, în funcţie de originea, destinaţia şi itinerarul transferului, de tipul de deşeu

	deşeuri, în funcţie de originea, destinaţia şi itinerarul transferului, de tipul de deşeu transferat şi de tipul de tratament care se aplică deşeului la destinaţie, în contractul menţionat la alin. (1) se vor preciza condiţiile cu privire la responsabilitate, îndeosebi în cazurile în care producătorului iniţial îi revine responsabilitatea pentru întregul lanţ al procesului de tratare sau în cazurile în care responsabilitatea producătorului şi a deţinătorului se poate împărţi sau delega între actorii din lanţul procesului de tratare. (4) Prin actele normative aprobate de Guvern în vederea implementării prezentei legi se va stabili, în conformitate cu art. 14, dacă responsabilitatea cu privire la organizarea activităţilor de gestionare a anumitor deşeuri revine, parţial sau în totalitate, producătorului produsului din care derivă deşeul respectiv şi dacă distribuitorii respectivului produs trebuie să împartă această responsabilitate. (5) Unităţile şi întreprinderile specializate în colectarea sau transportul de deşeuri livrează deşeurile colectate la instalaţiile de tratare, respectînd prevederile art. 4 şi ale cap. VI.		transferat şi de tipul de tratament care se aplică deşeului la destinaţie, în contractul menţionat la alin. (1) se vor preciza condiţiile cu privire la responsabilitate, îndeosebi în cazurile în care producătorului iniţial îi revine responsabilitatea pentru întregul lanţ al procesului de tratare sau în cazurile în care responsabilitatea producătorului şi a deţinătorului se poate împărţi sau delega între actorii din lanţul procesului de tratare. (4) Prin actele normative aprobate de Guvern în vederea implementării prezentei legi se va stabili, în conformitate cu art. 14, dacă responsabilitatea cu privire la organizarea activităţilor de gestionare a anumitor deşeuri revine, parţial sau în totalitate, producătorului produsului din care derivă deşeul respectiv şi dacă distribuitorii respectivului produs trebuie să împartă această responsabilitate. (5) Unităţile şi întreprinderile specializate în colectarea sau transportul de deşeuri livrează deşeurile colectate la instalaţiile de tratare, respectînd prevederile art. 4 şi ale cap. VI. (6) Persoanele juridice care desfăşoară activităţi de gestionare a deşeurilor, identificate ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru realizarea obligaţiilor privind asigurarea securităţii cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare şi de alte acte normative care stabilesc cerinţe specifice de securitate a reţelelor şi sistemelor informatice pe care aceştia le utilizează la prestarea serviciilor.

2.	**Articolul 31.** Competenţele privind activităţile de control în domeniul gestionării deşeurilor (1) Autorităţile teritoriale de mediu inspectează şi iau măsuri pentru respectarea de către cei implicaţi în gestionarea deşeurilor a legislaţiei de mediu şi a condiţiilor de autorizare stabilite conform legii. (2) Autorităţile teritoriale pentru sănătate publică exercită monitorizarea departamentală a cerinţelor de gestionare a deşeurilor rezultate din activităţile medicale. (4) Autorităţile vamale şi reprezentanţii Inspectoratului pentru Protecția Mediului şi ai subdiviziunilor teritoriale ale acestuia controlează încărcăturile şi iau măsuri pentru asigurarea conformităţii cu documentele însoţitoare şi pentru respectarea prevederilor legale referitoare la îndeplinirea condițiilor de export, import și tranzit ale deşeurilor.	Articolul 31 se completează cu alineatul (5), cu următorul cuprins: „(5) Supravegherea și controlul de stat al modului în care persoanele juridice care desfășoară activități de gestionare a deșeurilor realizează obligațiile stabilite la art. 18 alin. (6) se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”	**Articolul 31.** Competenţele privind activităţile de control în domeniul gestionării deşeurilor (1) Autorităţile teritoriale de mediu inspectează şi iau măsuri pentru respectarea de către cei implicaţi în gestionarea deşeurilor a legislaţiei de mediu şi a condiţiilor de autorizare stabilite conform legii. (2) Autorităţile teritoriale pentru sănătate publică exercită monitorizarea departamentală a cerinţelor de gestionare a deşeurilor rezultate din activităţile medicale. (4) Autorităţile vamale şi reprezentanţii Inspectoratului pentru Protecția Mediului şi ai subdiviziunilor teritoriale ale acestuia controlează încărcăturile şi iau măsuri pentru asigurarea conformităţii cu documentele însoţitoare şi pentru respectarea prevederilor legale referitoare la îndeplinirea condițiilor de export, import și tranzit ale deşeurilor. (5) Supravegherea și controlul de stat al modului în care persoanele juridice care desfășoară activități de gestionare a deșeurilor realizează obligațiile stabilite la art. 18 alin. (6) se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.
Articolul 16 din Legea nr. 102/2017 cu privire la dispozitivele medicale			
1.	**Articolul 16.** Vigilența dispozitivelor medicale (1) Producătorii de dispozitive medicale, reprezentanții acestora, persoanele juridice ce	Se completează cu alineatele (1^1) și (1^2), cu următorul cuprins: „(1^1) Producătorii de dispozitive medicale, identificați ca furnizori de servicii în conformitate	**Articolul 16.** Vigilența dispozitivelor medicale (1) Producătorii de dispozitive medicale, reprezentanții acestora, persoanele juridice ce comercializează dispozitivele medicale,

	comercializează dispozitivele medicale, importatorii cu sediul înregistrat în Republica Moldova şi utilizatorii de dispozitive medicale sînt obligaţi: a) să stabilească şi să menţină un sistem propriu de vigilenţă a dispozitivelor medicale, care să asigure colectarea, evaluarea şi schimbul de date cu privire la complicaţiile legate de dispozitivele medicale sau cu privire la incidentele cu implicarea acestora, şi să colaboreze în acest sens cu Agenţia; b) în termen de 2 zile lucrătoare, să informeze Agenţia despre orice complicaţie sau incident de care sînt conştienţi. (2) Agenţia în colaborare cu producătorul evaluează, după caz, nivelul de risc al unui incident sau al unei complicaţii raportate. După efectuarea investigaţiei, Agenţia informează părţile interesate – autoritatea publică centrală, organismul recunoscut, producătorul, consumatorul şi/sau utilizatorul – despre complicaţiile sau incidentele pentru care s-au luat sau trebuie să se ia măsurile corespunzătoare, inclusiv retragerea dispozitivului de pe piaţă. (3) Reglementarea sistemului de vigilenţă a dispozitivelor medicale este aprobată prin act normativ departamental, în care se stabilesc condiţiile de funcţionare integrală şi conţinutul detaliat al raportării complicaţiilor sau incidentelor cu implicarea dispozitivelor medicale.	cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligaţiilor de asigurare a securităţii cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare şi de alte acte normative care stabilesc cerinţe specifice de securitate a reţelelor şi sistemelor informatice. (1^2) Supravegherea şi controlul de stat al respectării de către producătorii de dispozitive medicale a obligaţiilor stabilite la alin. (1^1) se exercită de către autoritatea competentă la nivel naţional în domeniul securităţii cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”	importatorii cu sediul înregistrat în Republica Moldova şi utilizatorii de dispozitive medicale sînt obligaţi: a) să stabilească şi să menţină un sistem propriu de vigilenţă a dispozitivelor medicale, care să asigure colectarea, evaluarea şi schimbul de date cu privire la complicaţiile legate de dispozitivele medicale sau cu privire la incidentele cu implicarea acestora, şi să colaboreze în acest sens cu Agenţia; b) în termen de 2 zile lucrătoare, să informeze Agenţia despre orice complicaţie sau incident de care sînt conştienţi. (1^1) Producătorii de dispozitive medicale, identificaţi ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligaţiilor de asigurare a securităţii cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare şi de alte acte normative care stabilesc cerinţe specifice de securitate a reţelelor şi sistemelor informatice. (1^2) Supravegherea şi controlul de stat al respectării de către producătorii de dispozitive medicale a obligaţiilor stabilite la alin. (1^1) se exercită de către autoritatea competentă la nivel naţional în domeniul securităţii cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.

			(2) Agenția în colaborare cu producătorul evaluează, după caz, nivelul de risc al unui incident sau al unei complicații raportate. După efectuarea investigației, Agenția informează părțile interesate – autoritatea publică centrală, organismul recunoscut, producătorul, consumatorul și/sau utilizatorul – despre complicațiile sau incidentele pentru care s-au luat sau trebuie să se ia măsurile corespunzătoare, inclusiv retragerea dispozitivului de pe piață. (3) Reglementarea sistemului de vigilență a dispozitivelor medicale este aprobată prin act normativ departamental, în care se stabilesc condițiile de funcționare integrală și conținutul detaliat al raportării complicațiilor sau incidentelor cu implicarea dispozitivelor medicale.
Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului			
1.	**Articolul 3.** Noțiuni principale În sensul prezentei legi, următoarele noțiuni principale semnifică: *act terorist* – infracțiune prevăzută la art. 278 din Codul penal al Republicii Moldova; *activitate teroristă (activități teroriste)* – activități care includ: – planificarea, pregătirea, tentativa de săvîrșire și săvîrșirea unui act terorist sau a unei alte fapte ce constituie infracțiune cu caracter terorist; – constituirea unei formațiuni armate ilegale, a unei organizații criminale, a unui grup organizat în scopul săvîrșirii uneia sau mai multor infracțiuni cu caracter terorist;	Articolul 3 se completează cu noțiunile „obiectiv al infrastructurii critice" și „operator" cu următorul cuprins: „*obiectiv al infrastructurii critice* – obiectiv de importanță vitală din domeniul administrației publice, tehnologiei informației și comunicațiilor electronice și poștale, de infrastructură, energetică, din sfera social-economică, sănătății, cultural-educativă, industrială, ecologică, din sistemul informațional al țării în ansamblu, din infrastructura complexului militar și de apărare al organelor de forță, perturbarea sau distrugerea căruia poate provoca un impact negativ pentru siguranța, securitatea, bunăstarea socială și	**Articolul 3.** Noțiuni principale În sensul prezentei legi, următoarele noțiuni principale semnifică: *act terorist* – infracțiune prevăzută la art. 278 din Codul penal al Republicii Moldova; *activitate teroristă (activități teroriste)* – activități care includ: – planificarea, pregătirea, tentativa de săvîrșire și săvîrșirea unui act terorist sau a unei alte fapte ce constituie infracțiune cu caracter terorist; – constituirea unei formațiuni armate ilegale, a unei organizații criminale, a unui grup organizat în scopul săvîrșirii uneia sau mai multor infracțiuni cu caracter terorist; – recrutarea, favorizarea, înarmarea,

	– recrutarea, favorizarea, înarmarea, instruirea şi utilizarea teroriştilor; – ralierea la organizaţiile teroriste sau participarea la activitatea acestor organizaţii; – finanţarea pregătirii sau comiterii unui act terorist ori a unei alte infracţiuni cu caracter terorist, finanţarea unei organizaţii teroriste, a unui grup terorist sau a unui terorist, precum şi acordarea de sprijin acestora pe alte căi; – acordarea de suport informaţional sau de alt ordin în procesul planificării, pregătirii sau comiterii unui act terorist ori a unei alte fapte ce constituie infracţiune cu caracter terorist; – instigarea în scop terorist, justificarea publică a terorismului, propaganda ideilor terorismului, răspîndirea de materiale sau informaţii ce îndeamnă la activităţi teroriste sau îndreptăţesc desfăşurarea unor astfel de activităţi; – oricare dintre acţiunile menţionate efectuate prin intermediul sistemelor informaţionale şi al reţelelor de comunicaţii electronice; – orice alte fapte ce constituie infracţiuni cu caracter terorist; *activitate teroristă internaţională* – activităţi teroriste înfăptuite: – de un terorist, de un grup terorist sau de o organizaţie teroristă pe teritoriul a două sau mai multor state, aducînd prejudicii intereselor acestor state şi/sau unor organizaţii internaţionale; – de cetăţenii unui stat împotriva cetăţenilor unui alt stat sau pe teritoriul unui alt stat;	economică a statului, pierderi de servicii esenţiale, pericol pentru viaţa, sănătatea oamenilor şi efecte negative asupra mediului; *operator* – ministerele, alte autorităţi sau instituţii publice şi persoanele juridice, indiferent de tipul de proprietate şi forma juridică de organizare, care au în gestiunea lor obiective incluse în Nomenclatorul naţional al infrastructurii critice;”.	instruirea şi utilizarea teroriştilor; – ralierea la organizaţiile teroriste sau participarea la activitatea acestor organizaţii; – finanţarea pregătirii sau comiterii unui act terorist ori a unei alte infracţiuni cu caracter terorist, finanţarea unei organizaţii teroriste, a unui grup terorist sau a unui terorist, precum şi acordarea de sprijin acestora pe alte căi; – acordarea de suport informaţional sau de alt ordin în procesul planificării, pregătirii sau comiterii unui act terorist ori a unei alte fapte ce constituie infracţiune cu caracter terorist; – instigarea în scop terorist, justificarea publică a terorismului, propaganda ideilor terorismului, răspîndirea de materiale sau informaţii ce îndeamnă la activităţi teroriste sau îndreptăţesc desfăşurarea unor astfel de activităţi; – oricare dintre acţiunile menţionate efectuate prin intermediul sistemelor informaţionale şi al reţelelor de comunicaţii electronice; – orice alte fapte ce constituie infracţiuni cu caracter terorist; *activitate teroristă internaţională* – activităţi teroriste înfăptuite: – de un terorist, de un grup terorist sau de o organizaţie teroristă pe teritoriul a două sau mai multor state, aducînd prejudicii intereselor acestor state şi/sau unor organizaţii internaţionale; – de cetăţenii unui stat împotriva cetăţenilor unui alt stat sau pe teritoriul unui alt stat; – în cazul în care atît teroristul, cît şi victima terorismului sînt cetăţeni ai aceluiaşi

	– în cazul în care atît teroristul, cît şi victima terorismului sînt cetăţeni ai aceluiaşi stat sau ai unor state diferite, dar infracţiunea a fost săvîrşită în afara teritoriilor acestor state; *combaterea terorismului* – măsuri şi acţiuni ofensive întreprinse de autorităţile competente în scopul descoperirii şi curmării activităţilor teroriste şi al atenuării urmărilor acestora; *criză teroristă* – situaţie creată în timpul sau ca urmare a unui act terorist sau a unei alte fapte ce constituie infracţiune cu caracter terorist, prin care se creează un pericol iminent pentru viaţa şi securitatea cetăţenilor, pentru interesele societăţii sau ale statului; *exerciţiu antiterorist* – complex de măsuri specifice, teoretice şi practice, desfăşurate de către autorităţile cu atribuţii în domeniul prevenirii şi combaterii terorismului în scopul instruirii forţelor operaţionale, determinării eficienţei măsurilor de prevenire şi combatere a activităţilor teroriste, a nivelului de pregătire a Comandamentului Operaţional Antiterorist în rezolvarea practică a unor situaţii de criză teroristă simulate; *grup terorist* – două sau mai multe persoane care s-au asociat în scopul de a desfăşura o activitate teroristă; *infracţiune cu caracter terorist* – una din infracţiunile prevăzute la art.134^{11} din Codul penal al Republicii Moldova; *infrastructură critică* – element, sistem sau o componentă a acestuia, aflat pe teritoriul Republicii Moldova, care este esenţial pentru menţinerea funcţiilor vitale ale		stat sau ai unor state diferite, dar infracţiunea a fost săvîrşită în afara teritoriilor acestor state; *combaterea terorismului* – măsuri şi acţiuni ofensive întreprinse de autorităţile competente în scopul descoperirii şi curmării activităţilor teroriste şi al atenuării urmărilor acestora; *criză teroristă* – situaţie creată în timpul sau ca urmare a unui act terorist sau a unei alte fapte ce constituie infracţiune cu caracter terorist, prin care se creează un pericol iminent pentru viaţa şi securitatea cetăţenilor, pentru interesele societăţii sau ale statului; *exerciţiu antiterorist* – complex de măsuri specifice, teoretice şi practice, desfăşurate de către autorităţile cu atribuţii în domeniul prevenirii şi combaterii terorismului în scopul instruirii forţelor operaţionale, determinării eficienţei măsurilor de prevenire şi combatere a activităţilor teroriste, a nivelului de pregătire a Comandamentului Operaţional Antiterorist în rezolvarea practică a unor situaţii de criză teroristă simulate; *grup terorist* – două sau mai multe persoane care s-au asociat în scopul de a desfăşura o activitate teroristă; *infracţiune cu caracter terorist* – una din infracţiunile prevăzute la art.134^{11} din Codul penal al Republicii Moldova; *infrastructură critică* – element, sistem sau o componentă a acestuia, aflat pe teritoriul Republicii Moldova, care este esenţial pentru menţinerea funcţiilor vitale ale societăţii, a sănătăţii, a siguranţei, a securităţii şi a bunăstării sociale şi economice a persoanelor şi a cărui perturbare sau distrugere ar avea un impact

	societăţii, a sănătăţii, a siguranţei, a securităţii şi a bunăstării sociale şi economice a persoanelor şi a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel naţional ca urmare a incapacităţii de a menţine respectivele funcţii; *intervenţie contrateroristă* – complex de măsuri ofensive realizate în cadrul unei operaţii antiteroriste, în scopul capturării sau anihilării teroriştilor şi/sau eliberării ostaticilor, în cazul în care metodele defensive de înlăturare a pericolului terorist nu au atins rezultatul scontat; *luare de ostatici* – luarea sau reţinerea unei/unor persoane în calitate de ostatic/ostatici şi ameninţarea cu omorul, cu vătămarea integrităţii corporale sau a sănătăţii acesteia/acestora ori cu reţinerea în continuare a persoanei/persoanelor în această calitate cu scopul de a sili statul, organizaţia internaţională, persoana juridică sau fizică ori un grup de persoane să săvîrşească sau să se abţină de la săvîrşirea vreunei acţiuni în calitate de condiţie pentru eliberarea ostaticului; *operaţie antiteroristă* – ansamblu de măsuri planificate şi coordonate, întreprinse de către autorităţile cu atribuţii în domeniul prevenirii şi combaterii terorismului în scopul curmării activităţii teroriste, eliberării ostaticilor şi dirijării acţiunilor urgente de răspuns la survenirea unei crize teroriste; *organizaţie teroristă* – organizaţie creată în scopul desfăşurării de activităţi teroriste sau organizaţie care admite recurgerea la terorism în activitatea sa. Organizaţia se consideră teroristă dacă măcar		semnificativ la nivel naţional ca urmare a incapacităţii de a menţine respectivele funcţii; *intervenţie contrateroristă* – complex de măsuri ofensive realizate în cadrul unei operaţii antiteroriste, în scopul capturării sau anihilării teroriştilor şi/sau eliberării ostaticilor, în cazul în care metodele defensive de înlăturare a pericolului terorist nu au atins rezultatul scontat; *luare de ostatici* – luarea sau reţinerea unei/unor persoane în calitate de ostatic/ostatici şi ameninţarea cu omorul, cu vătămarea integrităţii corporale sau a sănătăţii acesteia/acestora ori cu reţinerea în continuare a persoanei/persoanelor în această calitate cu scopul de a sili statul, organizaţia internaţională, persoana juridică sau fizică ori un grup de persoane să săvîrşească sau să se abţină de la săvîrşirea vreunei acţiuni în calitate de condiţie pentru eliberarea ostaticului; *obiectiv al infrastructurii critice* – obiectiv de importanță vitală din domeniul administrației publice, tehnologiei informației și comunicațiilor electronice și poștale, de infrastructură, energetică, din sfera social-economică, sănătății, cultural-educativă, industrială, ecologică, din sistemul informațional al țării în ansamblu, din infrastructura complexului militar și de apărare al organelor de forță, perturbarea sau distrugerea căruia poate provoca un impact negativ pentru siguranța, securitatea, bunăstarea socială și economică a statului, pierderi de servicii esențiale, pericol pentru viața, sănătatea oamenilor și efecte negative asupra mediului;

	una din subdiviziunile sale structurale desfăşoară o activitate teroristă; *paşaport antiterorist* – document complex ce cuprinde informaţii despre starea şi nivelul de protecţie, eventualele pericole şi ameninţări cu tentă teroristă la adresa obiectivelor din infrastructura critică în cazul unor eventuale acte teroriste sau al altor infracţiuni cu caracter terorist pe teritoriul Republicii Moldova. Modelul paşaportului antiterorist se aprobă prin ordin al directorului Serviciului de Informaţii şi Securitate al Republicii Moldova; *prevenirea terorismului* – ansamblu de măsuri specifice cu caracter permanent, întreprinse cu anticipaţie de către autorităţile abilitate prin lege cu atribuţii de prevenire a terorismului, bazate pe acţiuni informative, educative, organizatorice, de pază, de protecţie, de informare şi relaţii publice, de optimizare a cadrului legislativ, de cooperare naţională şi internaţională în scopul identificării şi înlăturării factorilor de risc şi a ameninţărilor cu tentă teroristă; *protecţia antiteroristă a infrastructurii critice* – ansamblu de măsuri de ordin juridic, organizatoric, economico-financiar, ingineresc, de regim, de ordin operativ, informativ, contrainformativ etc., întreprinse de către autorităţile administraţiei publice, de alte organizaţii şi întreprinderi din cadrul infrastructurii critice, precum şi de către alte subdiviziuni sau de persoane special împuternicite de către acestea, care au drept scop asigurarea funcţionalităţii, continuităţii şi integrităţii infrastructurii critice, pentru a descuraja, diminua şi neutraliza o ameninţare,		*operator* – ministerele, alte autorităţi sau instituţii publice şi persoanele juridice, indiferent de tipul de proprietate şi forma juridică de organizare, care au în gestiunea lor obiective incluse în Nomenclatorul naţional al infrastructurii critice; *operaţie antiteroristă* – ansamblu de măsuri planificate şi coordonate, întreprinse de către autorităţile cu atribuţii în domeniul prevenirii şi combaterii terorismului în scopul curmării activităţii teroriste, eliberării ostaticilor şi dirijării acţiunilor urgente de răspuns la survenirea unei crize teroriste; *organizaţie teroristă* – organizaţie creată în scopul desfăşurării de activităţi teroriste sau organizaţie care admite recurgerea la terorism în activitatea sa. Organizaţia se consideră teroristă dacă măcar una din subdiviziunile sale structurale desfăşoară o activitate teroristă; *paşaport antiterorist* – document complex ce cuprinde informaţii despre starea şi nivelul de protecţie, eventualele pericole şi ameninţări cu tentă teroristă la adresa obiectivelor din infrastructura critică în cazul unor eventuale acte teroriste sau al altor infracţiuni cu caracter terorist pe teritoriul Republicii Moldova. Modelul paşaportului antiterorist se aprobă prin ordin al directorului Serviciului de Informaţii şi Securitate al Republicii Moldova; *prevenirea terorismului* – ansamblu de măsuri specifice cu caracter permanent, întreprinse cu anticipaţie de către autorităţile abilitate prin lege cu atribuţii de prevenire a terorismului, bazate pe acţiuni informative, educative, organizatorice, de pază, de protecţie, de informare şi relaţii publice, de optimizare a

	un risc sau un punct vulnerabil; *terorism* – fenomen cu un grad înalt de pericol social, caracterizat printr-o ideologie radicală şi o practică de influenţare prin violenţă a luării unor decizii de către autorităţi şi instituţii publice sau organizaţii internaţionale, însoţite de intimidarea populaţiei şi/sau de alte acţiuni violente ilegale; *terorist* – persoană implicată sub orice formă într-o activitate teroristă; *test antiterorist* – complex de măsuri cu caracter public şi/sau secret, realizate de Serviciul de Informaţii şi Securitate al Republicii Moldova în scopul verificării şi evaluării eficienţei sistemului şi mecanismului de protecţie antiteroristă; *zonă de desfăşurare a operaţiei antiteroriste* – construcţie, mijloc de transport sau teritoriu/spaţiu geografic în limitele căruia se desfăşoară o operaţie antiteroristă şi se introduce un regim juridic special; *zonă de risc* – stat sau regiune vulnerabilă sub aspectul securităţii ca urmare a conflictelor armate derulate sau a activităţii teroriste desfăşurate în acea zonă de către organizaţii sau entităţi recunoscute drept teroriste/paramilitare de către organizaţiile internaţionale ori regionale la care Republica Moldova este parte. Statele sau regiunile care constituie zone de risc urmează a fi desemnate prin hotărîre a Parlamentului.		cadrului legislativ, de cooperare naţională şi internaţională în scopul identificării şi înlăturării factorilor de risc şi a ameninţărilor cu tentă teroristă; *protecţia antiteroristă a infrastructurii critice* – ansamblu de măsuri de ordin juridic, organizatoric, economico-financiar, ingineresc, de regim, de ordin operativ, informativ, contrainformativ etc., întreprinse de către autorităţile administraţiei publice, de alte organizaţii şi întreprinderi din cadrul infrastructurii critice, precum şi de către alte subdiviziuni sau de persoane special împuternicite de către acestea, care au drept scop asigurarea funcţionalităţii, continuităţii şi integrităţii infrastructurii critice, pentru a descuraja, diminua şi neutraliza o ameninţare, un risc sau un punct vulnerabil; *terorism* – fenomen cu un grad înalt de pericol social, caracterizat printr-o ideologie radicală şi o practică de influenţare prin violenţă a luării unor decizii de către autorităţi şi instituţii publice sau organizaţii internaţionale, însoţite de intimidarea populaţiei şi/sau de alte acţiuni violente ilegale; *terorist* – persoană implicată sub orice formă într-o activitate teroristă; *test antiterorist* – complex de măsuri cu caracter public şi/sau secret, realizate de Serviciul de Informaţii şi Securitate al Republicii Moldova în scopul verificării şi evaluării eficienţei sistemului şi mecanismului de protecţie antiteroristă; *zonă de desfăşurare a operaţiei antiteroriste* – construcţie, mijloc de transport sau teritoriu/spaţiu geografic în limitele căruia se desfăşoară o operaţie antiteroristă şi se

			introduce un regim juridic special; *zonă de risc* – stat sau regiune vulnerabilă sub aspectul securităţii ca urmare a conflictelor armate derulate sau a activităţii teroriste desfăşurate în acea zonă de către organizaţii sau entităţi recunoscute drept teroriste/paramilitare de către organizaţiile internaţionale ori regionale la care Republica Moldova este parte. Statele sau regiunile care constituie zone de risc urmează a fi desemnate prin hotărîre a Parlamentului.
2.	**Articolul 20.** Controlul privind asigurarea protecţiei antiteroriste a infrastructurii critice (1) Controlul privind asigurarea protecţiei antiteroriste a infrastructurii critice are drept scop: a) verificarea nivelului de pregătire a personalului în ceea ce priveşte asigurarea protecţiei antiteroriste; b) determinarea capacităţii de pază şi protecţie a obiectivelor infrastructurii critice; c) identificarea vulnerabilităţilor şi a factorilor de risc la adresa infrastructurii critice. (2) Controlul asupra respectării prevederilor actelor normative privind protecţia antiteroristă a infrastructurii critice se exercită planificat, inopinat şi repetat de către reprezentanţii Centrului Antiterorist, fie în mod separat, fie împreună cu reprezentanţii altor autorităţi în limitele legale. (3) Controlul se efectuează conform prevederilor legislaţiei în vigoare şi planurilor anuale aprobate de directorul Serviciului de	Articolul 20 se completează cu alineatele $(2)^1$ şi $(2)^2$, cu următorul cuprins: „$(2)^1$ Supravegherea și controlul de stat al respectării de către operatorii obiectivelor de infrastructură critică a obligațiilor de asigurare a securității cibernetice, prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia, se realizează de către autoritatea competentă în temeiul legii respective $(2)^2$ Autoritatea competentă în domeniul securității cibernetice informează, în termen de 5 zile, Centrul Antiterorist despre încălcările legislației constatate în cadrul controlului exercitat asupra operatorilor obiectivelor de infrastructură critică privind modul în care aceștia respectă obligațiile de asigurare a securității cibernetice stabilite de actele normative menționate la alineatul $(2)^1$.”	**Articolul 20.** Controlul privind asigurarea protecţiei antiteroriste a infrastructurii critice (1) Controlul privind asigurarea protecţiei antiteroriste a infrastructurii critice are drept scop: a) verificarea nivelului de pregătire a personalului în ceea ce priveşte asigurarea protecţiei antiteroriste; b) determinarea capacităţii de pază şi protecţie a obiectivelor infrastructurii critice; c) identificarea vulnerabilităţilor şi a factorilor de risc la adresa infrastructurii critice. (2) Controlul asupra respectării prevederilor actelor normative privind protecţia antiteroristă a infrastructurii critice se exercită planificat, inopinat şi repetat de către reprezentanţii Centrului Antiterorist, fie în mod separat, fie împreună cu reprezentanţii altor autorităţi în limitele legale. „$(2)^1$ Supravegherea și controlul de stat al respectării de către operatorii obiectivelor de infrastructură critică a obligațiilor de asigurare a

	Informaţii şi Securitate. (4) Priorităţile şi frecvenţa controalelor obiectivelor din cadrul infrastructurii critice se stabilesc de către Serviciul de Informaţii şi Securitate. (5) Rezultatele fiecărui control se consemnează în paşaportul antiterorist al obiectivului, cu informarea gestionarului obiectivului.		securității cibernetice, prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia, se realizează de către autoritatea competentă în temeiul legii respective (2)[2] Autoritatea competentă în domeniul securității cibernetice informează, în termen de 5 zile, Centrul Antiterorist despre încălcările legislației constatate în cadrul controlului exercitat asupra operatorilor obiectivelor de infrastructură critică privind modul în care aceștia respectă obligațiile de asigurare a securității cibernetice stabilite de actele normative menționate la alineatul (2)[1]. (3) Controlul se efectuează conform prevederilor legislaţiei în vigoare şi planurilor anuale aprobate de directorul Serviciului de Informaţii şi Securitate. (4) Priorităţile şi frecvenţa controalelor obiectivelor din cadrul infrastructurii critice se stabilesc de către Serviciul de Informaţii şi Securitate. (5) Rezultatele fiecărui control se consemnează în paşaportul antiterorist al obiectivului, cu informarea gestionarului obiectivului.
Articolul 21 din Legea 174/2017 cu privire la energetică			
1.	(4) Măsurile întreprinse de Agenţie, de organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, de autorităţile de reglementare, de alte autorităţi publice, de autorităţile administraţiei publice locale în conformitate cu prezenta	La alineatul (4) cuvintele „în conformitate cu prezenta lege și legile sectoriale” se substituie cu cuvintele „în conformitate cu prezenta lege, cu legile sectoriale, precum și în temeiul altor legi”;	(4) Măsurile întreprinse de Agenţie, de organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, de autorităţile de reglementare, de alte autorităţi publice, de autorităţile administraţiei publice locale în conformitate cu prezenta lege, cu legile

	lege şi legile sectoriale, inclusiv privind licenţierea, autorizarea, monitorizarea şi supravegherea activităţii întreprinderilor energetice, nu se consideră a fi un amestec în activitatea întreprinderilor energetice în sensul alin. (2).		sectoriale, precum şi în temeiul altor legi, inclusiv privind licenţierea, autorizarea, monitorizarea şi supravegherea activităţii întreprinderilor energetice, nu se consideră a fi un amestec în activitatea întreprinderilor energetice în sensul alin. (2).
2.	**Articolul 21.** Principii de activitate (1) Toate întreprinderile energetice îşi desfăşoară activitatea în conformitate cu principiul eficienţei economice, cu respectarea parametrilor şi indicatorilor de calitate, stabiliţi în prezenta lege și în legile sectoriale. Preţurile şi tarifele, inclusiv cele reglementate, aplicate de întreprinderile energetice se stabilesc în conformitate cu legile sectoriale. (2) Organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, autorităţile de reglementare, alte autorităţi publice, autorităţile administraţiei publice locale, organizaţiile necomerciale nu au dreptul: a) să intervină în activitatea întreprinderilor energetice; b) să distragă personalul întreprinderilor energetice de la îndeplinirea atribuţiilor de serviciu; c) să se implice în relaţiile contractuale dintre întreprinderile energetice şi consumatori, utilizatorii de sistem, cu excepţiile stabilite în prezenta lege și în legile sectoriale. (3) Organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale,	Se completează cu alineatele $(7)^1$ și $(7)^2$, cu următorul cuprins: „$(7)^1$ Întreprinderile energetice, identificate ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. $(7)^2$ Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alineatul (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia.”	**Articolul 21.** Principii de activitate (1) Toate întreprinderile energetice îşi desfăşoară activitatea în conformitate cu principiul eficienţei economice, cu respectarea parametrilor şi indicatorilor de calitate, stabiliţi în prezenta lege și în legile sectoriale. Preţurile şi tarifele, inclusiv cele reglementate, aplicate de întreprinderile energetice se stabilesc în conformitate cu legile sectoriale. (2) Organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, autorităţile de reglementare, alte autorităţi publice, autorităţile administraţiei publice locale, organizaţiile necomerciale nu au dreptul: a) să intervină în activitatea întreprinderilor energetice; b) să distragă personalul întreprinderilor energetice de la îndeplinirea atribuţiilor de serviciu; c) să se implice în relaţiile contractuale dintre întreprinderile energetice şi consumatori, utilizatorii de sistem, cu excepţiile stabilite în prezenta lege şi în legile sectoriale. (3) Organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, autorităţile de reglementare, alte autorităţi publice, autorităţile administraţiei publice locale sînt obligate să notifice Guvernul cu privire la

	autorităţile de reglementare, alte autorităţi publice, autorităţile administraţiei publice locale sînt obligate să notifice Guvernul cu privire la înstrăinarea obiectelor energetice aflate în proprietatea lor cu cel puţin 6 luni înainte de încheierea actelor juridice de înstrăinare. (4) Măsurile întreprinse de Agenţie, de organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, de autorităţile de reglementare, de alte autorităţi publice, de autorităţile administraţiei publice locale în conformitate cu prezenta lege şi legile sectoriale, inclusiv privind licenţierea, autorizarea, monitorizarea şi supravegherea activităţii întreprinderilor energetice, nu se consideră a fi un amestec în activitatea întreprinderilor energetice în sensul alin. (2). (5) Obiectele energetice pot fi construite şi admise în exploatare în conformitate cu Legea nr. 163/2010 privind autorizarea executării lucrărilor de construcţie. Exploatarea obiectelor energetice se efectuează doar după obținerea de către întreprinderile energetice a licențelor, a autorizațiilor, a altor acte permisive, eliberate în termenele și în condițiile stabilite prin lege. (6) Întreprinderile energetice, indiferent de tipul de proprietate, inclusiv distribuitorii de energie termică, sînt obligate să prezinte Agenţiei planuri, informații și rapoarte în termenele și în condițiile stabilite în legile sectoriale.		înstrăinarea obiectelor energetice aflate în proprietatea lor cu cel puțin 6 luni înainte de încheierea actelor juridice de înstrăinare. (4) Măsurile întreprinse de Agenţie, de organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, de autorităţile de reglementare, de alte autorităţi publice, de autorităţile administraţiei publice locale în conformitate cu prezenta lege, cu legile sectoriale, precum și în temeiul altor legi, inclusiv privind licenţierea, autorizarea, monitorizarea şi supravegherea activității întreprinderilor energetice, nu se consideră a fi un amestec în activitatea întreprinderilor energetice în sensul alin. (2). (5) Obiectele energetice pot fi construite și admise în exploatare în conformitate cu Legea nr. 163/2010 privind autorizarea executării lucrărilor de construcţie. Exploatarea obiectelor energetice se efectuează doar după obținerea de către întreprinderile energetice a licențelor, a autorizațiilor, a altor acte permisive, eliberate în termenele și în condițiile stabilite prin lege. (6) Întreprinderile energetice, indiferent de tipul de proprietate, inclusiv distribuitorii de energie termică, sînt obligate să prezinte Agenţiei planuri, informații și rapoarte în termenele și în condițiile stabilite în legile sectoriale. (7) Întreprinderile energetice sînt obligate să efectueze în termen lucrările curente de exploatare şi de reparaţie a obiectelor energetice, cu respectarea actelor normative şi a documentelor normativ-tehnice cu privire la

	(7) Întreprinderile energetice sînt obligate să efectueze în termen lucrările curente de exploatare şi de reparaţie a obiectelor energetice, cu respectarea actelor normative şi a documentelor normativ-tehnice cu privire la calitate, securitate, inclusiv securitatea industrială, precum şi cu privire la protecţia mediului, astfel încît consumatorii să fie aprovizionaţi cu energie în mod fiabil şi continuu. (8) Întreprinderile energetice au drept de acces la terenurile terţilor, cu condiţia obţinerii acordului proprietarilor terenurilor respective, pentru efectuarea lucrărilor de construcţie, exploatare, întreţinere, reabilitare, modernizare, inclusiv de retehnologizare, a obiectelor energetice. Efectuarea lucrărilor menţionate trebuie să fie coordonată cu proprietarii terenurilor, cu excepţia lucrărilor necesare pentru prevenirea producerii avariilor, incendiilor, electrocutărilor şi/sau a exploziilor ori pentru înlăturarea consecinţelor acestora. După finalizarea lucrărilor menţionate, întreprinderile energetice sînt obligate să asigure degajarea terenului şi repunerea lui în situaţia iniţială în termenele convenite cu proprietarii terenurilor respective. Întreprinderile energetice sînt obligate să se folosească cu bună-credinţă de drepturile stabilite în prezentul articol şi să achite proprietarului de teren sau de alte bunuri proprietate privată despăgubirea cuvenită pentru pagubele produse la efectuarea lucrărilor menţionate, inclusiv în cazul înlăturării consecinţelor avariilor,	

	calitate, securitate, inclusiv securitatea industrială, precum şi cu privire la protecţia mediului, astfel încît consumatorii să fie aprovizionaţi cu energie în mod fiabil şi continuu. (7)[1] Întreprinderile energetice, identificate ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (7)[2] Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alineatul (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia. (8) Întreprinderile energetice au drept de acces la terenurile terţilor, cu condiţia obţinerii acordului proprietarilor terenurilor respective, pentru efectuarea lucrărilor de construcţie, exploatare, întreţinere, reabilitare, modernizare, inclusiv de retehnologizare, a obiectelor energetice. Efectuarea lucrărilor menţionate trebuie să fie coordonată cu proprietarii terenurilor, cu excepţia lucrărilor necesare pentru prevenirea producerii avariilor,

	incendiilor, electrocutărilor şi/sau ale exploziilor. (9) Producătorii care exploatează centralele electrice, centralele termice, care funcţionează pe bază de combustibili fosili, cu excepţia celor care desfăşoară activitate sezonieră şi/sau care produc energie electrică, energie termică exclusiv pentru necesităţi proprii, sînt obligaţi să menţină rezerve de combustibili la nivel suficient pentru a asigura securitatea aprovizionării cu energie, în condiţiile stabilite de Guvern. (10) Consumatorii care dispun de centrală electrică sînt în drept să livreze în reţelele electrice surplusul de energie electrică în condiţiile stabilite în Legea nr. 107/2016 cu privire la energia electrică şi în Legea nr. 10/2016 privind promovarea utilizării energiei din surse regenerabile.		incendiilor, electrocutărilor şi/sau a exploziilor ori pentru înlăturarea consecinţelor acestora. După finalizarea lucrărilor menţionate, întreprinderile energetice sînt obligate să asigure degajarea terenului şi repunerea lui în situaţia iniţială în termenele convenite cu proprietarii terenurilor respective. Întreprinderile energetice sînt obligate să se folosească cu bună-credinţă de drepturile stabilite în prezentul articol şi să achite proprietarului de teren sau de alte bunuri proprietate privată despăgubirea cuvenită pentru pagubele produse la efectuarea lucrărilor menţionate, inclusiv în cazul înlăturării consecinţelor avariilor, incendiilor, electrocutărilor şi/sau ale exploziilor. (9) Producătorii care exploatează centralele electrice, centralele termice, care funcţionează pe bază de combustibili fosili, cu excepţia celor care desfăşoară activitate sezonieră şi/sau care produc energie electrică, energie termică exclusiv pentru necesităţi proprii, sînt obligaţi să menţină rezerve de combustibili la nivel suficient pentru a asigura securitatea aprovizionării cu energie, în condiţiile stabilite de Guvern. (10) Consumatorii care dispun de centrală electrică sînt în drept să livreze în reţelele electrice surplusul de energie electrică în condiţiile stabilite în Legea nr. 107/2016 cu privire la energia electrică şi în Legea nr. 10/2016 privind promovarea utilizării energiei din surse regenerabile.
Legea nr. 202/2017 privind activitatea băncilor			

1.		Se completează cu articolul 38^2 , cu următorul cuprins: „Articolul 38^2. Gestionarea riscurilor de tehnologie a informației și a comunicațiilor (TIC), de securitate a informației și de continuitate a activității (1) Fiecare bancă trebuie să dispună de personal, sisteme și servicii eficiente aferente tehnologiei informației și a comunicațiilor (TIC) ce asigură, de o manieră proporțională cu natura, amploarea și complexitatea riscurilor inerente activităților și modelului de afaceri, desfășurarea activităților băncii. În acest scop, banca stabilește roluri și responsabilități, aprobă și pune în aplicare o strategie TIC și de securitate a informației și planuri de acțiuni în vederea atingerii obiectivelor acesteia. (2) Banca trebuie să stabilească un cadru de administrare a continuității activității, capabil să asigure capacitatea de a funcționa în mod continuu, cu asigurarea protejării tuturor informațiilor critice, inclusiv în vederea limitării pierderilor în cazul unei întreruperi severe a activității. În acest scop, banca va identifica riscurile de continuitate la care este expusă și va aproba și va pune în aplicare planuri de asigurare a continuității activității.	**Articolul 38^2.** Gestionarea riscurilor de tehnologie a informației și a comunicațiilor (TIC), de securitate a informației și de continuitate a activității (1) Fiecare bancă trebuie să dispună de personal, sisteme și servicii eficiente aferente tehnologiei informației și a comunicațiilor (TIC) ce asigură, de o manieră proporțională cu natura, amploarea și complexitatea riscurilor inerente activităților și modelului de afaceri, desfășurarea activităților băncii. În acest scop, banca stabilește roluri și responsabilități, aprobă și pune în aplicare o strategie TIC și de securitate a informației și planuri de acțiuni în vederea atingerii obiectivelor acesteia. (2) Banca trebuie să stabilească un cadru de administrare a continuității activității, capabil să asigure capacitatea de a funcționa în mod continuu, cu asigurarea protejării tuturor informațiilor critice, inclusiv în vederea limitării pierderilor în cazul unei întreruperi severe a activității. În acest scop, banca va identifica riscurile de continuitate la care este expusă și va aproba și va pune în aplicare planuri de asigurare a continuității activității. (3) Banca trebuie să dispună de un cadru de administrare a riscurilor aferente TIC și de securitate a informației care să conțină procese și proceduri pentru a asigura identificarea,

		(3) Banca trebuie să dispună de un cadru de administrare a riscurilor aferente TIC și de securitate a informației care să conțină procese și proceduri pentru a asigura identificarea, analiza, evaluarea, diminuarea, monitorizarea, raportarea și menținerea riscurilor în limitele apetitului la risc al băncii. (4) Banca trebuie să dispună de un cadru de administrare a securității informației care trebuie să definească principiile, normele și modalitățile de protejare a confidențialității, integrității și disponibilității datelor și informației băncii și ale clienților acesteia, instituind în baza acestuia măsuri pentru diminuarea nivelurilor riscurilor TIC și de securitate a informației la care este expusă. (5) Banca trebuie să stabilească procese de revizuire a riscurilor, de testare a securității informației și continuității activității care să valideze eficacitatea măsurilor de control și aplicabilitatea planurilor de asigurare a continuității activității. (6) Cerințe specifice privind punerea în aplicare a alin. (1)-(5) se stabilesc în actele normative ale Băncii Naționale. (7) În măsura în care gestionarea riscurilor TIC, de securitate a informației și de continuitate a activității nu este reglementată de dispozițiile	analiza, evaluarea, diminuarea, monitorizarea, raportarea și menținerea riscurilor în limitele apetitului la risc al băncii. (4) Banca trebuie să dispună de un cadru de administrare a securității informației care trebuie să definească principiile, normele și modalitățile de protejare a confidențialității, integrității și disponibilității datelor și informației băncii și ale clienților acesteia, instituind în baza acestuia măsuri pentru diminuarea nivelurilor riscurilor TIC și de securitate a informației la care este expusă. (5) Banca trebuie să stabilească procese de revizuire a riscurilor, de testare a securității informației și continuității activității care să valideze eficacitatea măsurilor de control și aplicabilitatea planurilor de asigurare a continuității activității. (6) Cerințe specifice privind punerea în aplicare a alin. (1)-(5) se stabilesc în actele normative ale Băncii Naționale. (7) În măsura în care gestionarea riscurilor TIC, de securitate a informației și de continuitate a activității nu este reglementată de dispozițiile prezentei legi și a actului normativ menționat la alineatul (6), acestea se completează cu prevederile Legii nr. 48/2023 privind securitatea

		prezentei legi și a actului normativ menționat la alineatul (6), acestea se completează cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și de actele normative de punere a acesteia în aplicare. (8) Supravegherea și controlul modului în care băncile realizează obligațiile stabilite de prezentul articol se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice, desemnată în temeiul Legii nr. 48/2023 privind securitatea cibernetică, în cooperare cu Banca Națională a Moldovei, în conformitate cu actul normativ prevăzut la alineatul (6) și actele normative de punere în aplicare a Legii nr. 48/2023 privind securitatea cibernetică."	cibernetică și de actele normative de punere a acesteia în aplicare. (8) Supravegherea și controlul modului în care băncile realizează obligațiile stabilite de prezentul articol se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice, desemnată în temeiul Legii nr. 48/2023 privind securitatea cibernetică, în cooperare cu Banca Națională a Moldovei, în conformitate cu actul normativ prevăzut la alineatul (6) și actele normative de punere în aplicare a Legii nr. 48/2023 privind securitatea cibernetică.
Articolul 8 din Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate			
1.	**Articolul 8**. Securitatea și confidențialitatea schimbului de date (1) Securitatea și confidențialitatea schimbului de date sînt asigurate de către toți participanții la schimbul de date și de către deținătorul platformei de interoperabilitate, pe domeniile lor de competență, în conformitate cu cerințele de securitate aplicabile categoriei respective de date. (2) Pentru asigurarea securității și confidențialității la realizarea schimbului de date, precum și la accesarea informației cu accesibilitate limitată, suplimentar măsurilor de securitate standard, platforma de	Se completează cu alineatul $(3)^1$ cu următorul cuprins: „$(3)^1$ Realizarea obligației stabilite la alineatul (3) nu scutește participanții la schimbul de date, identificați ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, de realizarea obligațiilor de notificare stabilite de legea respectivă."	**Articolul 8**. Securitatea și confidențialitatea schimbului de date (1) Securitatea și confidențialitatea schimbului de date sînt asigurate de către toți participanții la schimbul de date și de către deținătorul platformei de interoperabilitate, pe domeniile lor de competență, în conformitate cu cerințele de securitate aplicabile categoriei respective de date. (2) Pentru asigurarea securității și confidențialității la realizarea schimbului de date, precum și la accesarea informației cu accesibilitate limitată, suplimentar măsurilor de securitate standard, platforma de

	interoperabilitate oferă posibilitatea transportării datelor în formă criptată. Criptarea și decriptarea datelor sînt asigurate de către furnizorul de date și, respectiv, consumatorul de date. (3) Participanții la schimbul de date sînt obligați să informeze autoritatea competentă despre vulnerabilitățile și incidentele de securitate în utilizarea platformei de interoperabilitate imediat sau în termen de cel mult 2 zile lucrătoare din momentul depistării acestora.		interoperabilitate oferă posibilitatea transportării datelor în formă criptată. Criptarea și decriptarea datelor sînt asigurate de către furnizorul de date și, respectiv, consumatorul de date. (3) Participanții la schimbul de date sînt obligați să informeze autoritatea competentă despre vulnerabilitățile și incidentele de securitate în utilizarea platformei de interoperabilitate imediat sau în termen de cel mult 2 zile lucrătoare din momentul depistării acestora. (3)[1] Realizarea obligației stabilite la alineatul (3) nu scutește participanții la schimbul de date, identificați ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, de realizarea obligațiilor de notificare stabilite de legea respectivă.
Articolul 8 din Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate			
1.		Se completează cu alineatul (4) cu următorul cuprins: „(4) Realizarea obligației stabilite la alineatul (3) nu scutește participanții la schimbul de date, identificați ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, de realizarea obligațiilor de notificare stabilite de această lege.”	**Articolul 8.** Securitatea și confidențialitatea schimbului de date (1) Securitatea și confidențialitatea schimbului de date sînt asigurate de către toți participanții la schimbul de date și de către deținătorul platformei de interoperabilitate, pe domeniile lor de competență, în conformitate cu cerințele de securitate aplicabile categoriei respective de date. (2) Pentru asigurarea securității și confidențialității la realizarea schimbului de date, precum și la accesarea informației cu accesibilitate limitată, suplimentar măsurilor de

			securitate standard, platforma de interoperabilitate oferă posibilitatea transportării datelor în formă criptată. Criptarea și decriptarea datelor sînt asigurate de către furnizorul de date și, respectiv, consumatorul de date. (3) Participanții la schimbul de date sînt obligați să informeze autoritatea competentă despre vulnerabilitățile și incidentele de securitate în utilizarea platformei de interoperabilitate imediat sau în termen de cel mult 2 zile lucrătoare din momentul depistării acestora. (4) Realizarea obligației stabilite la alineatul (3) nu scutește participanții la schimbul de date, identificați ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, de realizarea obligațiilor de notificare stabilite de această lege.
Legea nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar			
1.	**Articolul 17.** Sporuri cu caracter specific (1) Personalul din unitățile bugetare beneficiază, după caz, de sporuri specifice grupului ocupațional sau categoriei de personal în modul stabilit de Guvern. Pentru autoritatea responsabilă de exercitarea controlului parlamentar, modul de acordare a sporului cu caracter specific se aprobă de Biroul permanent al Parlamentului. (2) Suma anuală a sporurilor cu caracter specific incluse în partea variabilă a salariului lunar nu va depăși: a) pentru personalul din domeniile învățământului, cercetării, culturii, tineretului,	Articolul 17 alineatul (2) se completează cu litera b^2) cu următorul cuprins: „b^2) pentru personalul Agenției pentru Securitate Cibernetică – 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific;”	**Articolul 17.** Sporuri cu caracter specific (1) Personalul din unitățile bugetare beneficiază, după caz, de sporuri specifice grupului ocupațional sau categoriei de personal în modul stabilit de Guvern. Pentru autoritatea responsabilă de exercitarea controlului parlamentar, modul de acordare a sporului cu caracter specific se aprobă de Biroul permanent al Parlamentului. (2) Suma anuală a sporurilor cu caracter specific incluse în partea variabilă a salariului lunar nu va depăși: a) pentru personalul din domeniile învățământului, cercetării, culturii, tineretului,

	sportului, asistenței sociale – 10% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; b) pentru personalul din domeniul apărării naționale, securității statului și ordinii publice – 20% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; b[1]) prin derogare de la prevederile lit. b), pentru personalul din domeniul apărării naționale, securității statului și ordinii publice implicat în activități speciale de combatere a terorismului – 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; c) pentru personalul medical, inclusiv care deține funcții publice cu statut special, din autoritățile/ instituțiile/ structurile medicale, din Centrul de Medicină Legală și din instituțiile de asistență socială – 60% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; d) pentru personalul din autoritatea responsabilă de exercitarea controlului parlamentar, de stabilirea, coordonarea și monitorizarea implementării politicilor și priorităților Președintelui Republicii Moldova – 40% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; d[1]) - *abrogată.* e) pentru personalul din autoritatea responsabilă de controlul constituționalității – 60% din suma anuală a salariilor de bază		sportului, asistenței sociale – 10% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; b) pentru personalul din domeniul apărării naționale, securității statului și ordinii publice – 20% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; b[1]) prin derogare de la prevederile lit. b), pentru personalul din domeniul apărării naționale, securității statului și ordinii publice implicat în activități speciale de combatere a terorismului – 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; b[2]) pentru personalul Agenției pentru Securitate Cibernetică – 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; c) pentru personalul medical, inclusiv care deține funcții publice cu statut special, din autoritățile/ instituțiile/ structurile medicale, din Centrul de Medicină Legală și din instituțiile de asistență socială – 60% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; d) pentru personalul din autoritatea responsabilă de exercitarea controlului parlamentar, de stabilirea, coordonarea și monitorizarea implementării politicilor și priorităților Președintelui Republicii Moldova – 40% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; d[1]) - *abrogată.* e) pentru personalul din autoritatea responsabilă de controlul constituționalității – 60% din suma

	pentru personalul cu drept de a beneficia de spor cu caracter specific; f) pentru personalul din autoritatea responsabilă de activitatea de monitorizare informațională, comunicare strategică și combatere a dezinformării – 40% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific. (3) Pentru autoritățile responsabile de administrarea veniturilor fiscale și vamale și responsabile de certificare, supraveghere și control în domeniul aviației civile, limitele sporurilor cu caracter specific se aprobă de Guvern.		anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; f) pentru personalul din autoritatea responsabilă de activitatea de monitorizare informațională, comunicare strategică și combatere a dezinformării – 40% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific. (3) Pentru autoritățile responsabile de administrarea veniturilor fiscale și vamale și responsabile de certificare, supraveghere și control în domeniul aviației civile, limitele sporurilor cu caracter specific se aprobă de Guvern.
2.		La anexa nr. 3, notele la tabelul 2 se completează cu punctul 17 cu următorul cuprins: „17. Clasele de salarizare pentru funcțiile publice de conducere și de execuție din cadrul Direcției răspuns la incidente și crize cibernetice a Agenției pentru Securitate Cibernetică se majorează față de cele stabilite în tabel pentru aceste funcții, după cum urmează: - cu 15 clase succesive - pentru funcțiile publice de conducere de „șef de direcție” și „șef adjunct de direcție”; - cu 25 de clase succesive – pentru funcțiile publice de execuție.”	**17.** Clasele de salarizare pentru funcțiile publice de conducere și de execuție din cadrul Direcției răspuns la incidente și crize cibernetice a Agenției pentru Securitate Cibernetică se majorează față de cele stabilite în tabel pentru aceste funcții, după cum urmează: - cu 15 clase succesive - pentru funcțiile publice de conducere de „șef de direcție” și „șef adjunct de direcție”; - cu 25 de clase succesive – pentru funcțiile publice de execuție.
Legea nr. 277/2018 privind substanțele chimice			
1.	**Articolul 11.** Competențele altor autorități ale administrației publice centrale	Articolul 11 se completează cu alineatul (5) cu următorul cuprins:	**Articolul 11.** Competențele altor autorități ale administrației publice centrale

	(1) Ministerul Sănătății: a) inițiază și promovează, împreună cu celelalte autorități competente, actele normative referitoare la protecția sănătății umane, inclusiv a lucrătorilor care desfășoară activități ori se află în locuri de muncă în care sînt prezente substanțe sau amestecuri chimice periculoase, și la evaluarea și controlul riscului pe care îl prezintă pentru om substanțele și amestecurile chimice periculoase; b) identifică, evaluează și gestionează riscurile pentru sănătatea umană aferente substanțelor și amestecurilor chimice plasate pe piața Republicii Moldova; c) evaluează pericolele și riscurile pentru sănătatea umană în cadrul procedurii de autorizare a produselor de protecție a plantelor, a produselor biocide și a altor produse chimice menționate la art. 23 alin. (1) lit. a)–e), precum și în alte cazuri în care este necesară evaluarea pericolelor și riscurilor pentru sănătatea umană; d) organizează cercetări toxico-igienice ale substanțelor și amestecurilor chimice periculoase; e) asigură evaluarea eficacității în cadrul procedurii de autorizare a produselor biocide menționate la art. 23 alin. (1) lit. b); f) autorizează produsele biocide menționate la art. 23 alin. (1) lit. b), utilizînd platforma unică de autorizare a produselor chimice periculoase, stabilită în conformitate cu prezenta lege; g) asigură monitorizarea, evidența, raportarea și cercetarea cazurilor de otrăviri cu	„(5) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la art. 12 alin. (6) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia.”	(1) Ministerul Sănătății: a) inițiază și promovează, împreună cu celelalte autorități competente, actele normative referitoare la protecția sănătății umane, inclusiv a lucrătorilor care desfășoară activități ori se află în locuri de muncă în care sînt prezente substanțe sau amestecuri chimice periculoase, și la evaluarea și controlul riscului pe care îl prezintă pentru om substanțele și amestecurile chimice periculoase; b) identifică, evaluează și gestionează riscurile pentru sănătatea umană aferente substanțelor și amestecurilor chimice plasate pe piața Republicii Moldova; c) evaluează pericolele și riscurile pentru sănătatea umană în cadrul procedurii de autorizare a produselor de protecție a plantelor, a produselor biocide și a altor produse chimice menționate la art. 23 alin. (1) lit. a)–e), precum și în alte cazuri în care este necesară evaluarea pericolelor și riscurilor pentru sănătatea umană; d) organizează cercetări toxico-igienice ale substanțelor și amestecurilor chimice periculoase; e) asigură evaluarea eficacității în cadrul procedurii de autorizare a produselor biocide menționate la art. 23 alin. (1) lit. b); f) autorizează produsele biocide menționate la art. 23 alin. (1) lit. b), utilizînd platforma unică de autorizare a produselor chimice periculoase, stabilită în conformitate cu prezenta lege; g) asigură monitorizarea, evidența, raportarea și cercetarea cazurilor de otrăviri cu substanțele chimice periculoase, luînd măsuri de prevenire a acestora; h) asigură informarea și sensibilizarea publicului și a agenților economici privind pericolele și

	substanțele chimice periculoase, luînd măsuri de prevenire a acestora; h) asigură informarea și sensibilizarea publicului și a agenților economici privind pericolele și riscurile pe care le prezintă produsele menționate la art. 23 alin. (1) lit. a)–e) pentru sănătatea umană; i) cooperează, prin intermediul Agenției Naționale pentru Sănătate Publică, cu Ministerul Mediului în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; j) cooperează, prin intermediul Agenției Naționale pentru Sănătate Publică, cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și regulamentelor aprobate în temeiul acesteia; k) sesizează, prin intermediul Agenției Naționale pentru Sănătate Publică, Agenția Națională de Reglementare a Activităților Nucleare, Radiologice și Chimice și Inspectoratul pentru Protecția Mediului asupra încălcărilor prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legi speciale în domeniul sănătății publice și protecției muncii. (2) Inspectoratul General pentru Situații de Urgență al Ministerului Afacerilor Interne: a) acordă asistență specializată Serviciului Vamal și altor instituții abilitate cu atribuții în combaterea traficului și utilizării ilicite a		riscurile pe care le prezintă produsele menționate la art. 23 alin. (1) lit. a)–e) pentru sănătatea umană; i) cooperează, prin intermediul Agenției Naționale pentru Sănătate Publică, cu Ministerul Mediului în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; j) cooperează, prin intermediul Agenției Naționale pentru Sănătate Publică, cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și regulamentelor aprobate în temeiul acesteia; k) sesizează, prin intermediul Agenției Naționale pentru Sănătate Publică, Agenția Națională de Reglementare a Activităților Nucleare, Radiologice și Chimice și Inspectoratul pentru Protecția Mediului asupra încălcărilor prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legi speciale în domeniul sănătății publice și protecției muncii. (2) Inspectoratul General pentru Situații de Urgență al Ministerului Afacerilor Interne: a) acordă asistență specializată Serviciului Vamal și altor instituții abilitate cu atribuții în combaterea traficului și utilizării ilicite a substanțelor și amestecurilor chimice periculoase; b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia;

	substanțelor și amestecurilor chimice periculoase; b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra încălcărilor prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legile speciale în domeniul protecției civile; d) cooperează cu Agenția Națională în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; e) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova". (3) Serviciul Vamal al Ministerului Finanțelor: a) realizează controlul și admiterea introducerii pe/scoaterii de pe teritoriul Republicii Moldova a substanțelor și amestecurilor chimice în baza actelor permisive eliberate de Agenția Națională în conformitate cu prevederile prezentei legi și în baza procedurii menționate la art. 18 alin. (2); b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării		c) sesizează Inspectoratul pentru Protecția Mediului asupra încălcărilor prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legile speciale în domeniul protecției civile; d) cooperează cu Agenția Națională în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; e) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova". (3) Serviciul Vamal al Ministerului Finanțelor: a) realizează controlul și admiterea introducerii pe/scoaterii de pe teritoriul Republicii Moldova a substanțelor și amestecurilor chimice în baza actelor permisive eliberate de Agenția Națională în conformitate cu prevederile prezentei legi și în baza procedurii menționate la art. 18 alin. (2); b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra cazurilor de încălcare a prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de Codul vamal al Republicii Moldova; d) cooperează cu Agenția Națională în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi;

	prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra cazurilor de încălcare a prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de Codul vamal al Republicii Moldova; d) cooperează cu Agenția Națională în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; e) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova". (4) Agenția Națională pentru Siguranța Alimentelor: a) efectuează supravegherea și controlul producerii, importului, comercializării, utilizării și depozitării produselor de protecție a plantelor în conformitate cu legislația în domeniul protecției plantelor; b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra cazurilor de încălcare a prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele		e) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova". (4) Agenția Națională pentru Siguranța Alimentelor: a) efectuează supravegherea și controlul producerii, importului, comercializării, utilizării și depozitării produselor de protecție a plantelor în conformitate cu legislația în domeniul protecției plantelor; b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra cazurilor de încălcare a prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legislația specială în domeniul produselor de protecție a plantelor; d) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova". (5) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la art. 12 alin. (6) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia.

	atribuite de legislația specială în domeniul produselor de protecție a plantelor; d) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova".		
2.	**Articolul 12.** Obligațiile generale ale operatorilor din lanțul de aprovizionare (1) Producătorii și importatorii de substanțe și amestecuri chimice sînt obligați: a) să identifice și să evalueze proprietățile periculoase și posibilele riscuri pentru om și mediu ale produselor chimice pe care le furnizează; b) să dispună de informații privind identificarea, proprietățile periculoase și posibilele riscuri ale produselor chimice pe care le furnizează; c) să ofere utilizatorilor și altor persoane care manipulează produsul chimic informații privind rezultatele evaluării și alte informații disponibile și relevante privind proprietățile periculoase ale produsului chimic, privind riscurile și măsurile de siguranță; d) să actualizeze permanent informațiile disponibile privind produsele chimice. (2) Pentru a evalua proprietățile periculoase ale substanțelor și amestecurilor chimice, producătorii și importatorii de substanțe și amestecuri chimice sînt obligați să efectueze testări în laboratoare care respectă principiile bunei practici de laborator, stabilite de Guvern, în următoarele cazuri:	Articolul 12 se completează cu alineatul (6) cu următorul cuprins: „(6) Furnizorul unei substanțe sau al unui amestec, identificat ca furnizor de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, este responsabil pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice."	**Articolul 12.** Obligațiile generale ale operatorilor din lanțul de aprovizionare (1) Producătorii și importatorii de substanțe și amestecuri chimice sînt obligați: a) să identifice și să evalueze proprietățile periculoase și posibilele riscuri pentru om și mediu ale produselor chimice pe care le furnizează; b) să dispună de informații privind identificarea, proprietățile periculoase și posibilele riscuri ale produselor chimice pe care le furnizează; c) să ofere utilizatorilor și altor persoane care manipulează produsul chimic informații privind rezultatele evaluării și alte informații disponibile și relevante privind proprietățile periculoase ale produsului chimic, privind riscurile și măsurile de siguranță; d) să actualizeze permanent informațiile disponibile privind produsele chimice. (2) Pentru a evalua proprietățile periculoase ale substanțelor și amestecurilor chimice, producătorii și importatorii de substanțe și amestecuri chimice sînt obligați să efectueze testări în laboratoare care respectă principiile bunei practici de laborator, stabilite de Guvern, în următoarele cazuri: a) substanța sau amestecul chimic plasat pe piață constituie un produs nou autohton;

	a) substanța sau amestecul chimic plasat pe piață constituie un produs nou autohton; b) producătorii și importatorii nu dețin informațiile necesare conform alin. (1) lit. b) și nu există date disponibile pentru evaluarea corespunzătoare a substanței sau amestecului chimic fără efectuarea testelor de laborator; c) în literatura științifică de specialitate au apărut date cu privire la potențialele proprietăți periculoase ale substanței sau ale substanțelor componente ale amestecului chimic; d) nu există alte mijloace de obținere a informației necesare pentru evaluarea substanței sau amestecului fără efectuarea testelor. (3) Testările menționate la alin. (2) se efectuează în conformitate cu metodele indicate în Regulamentul privind stabilirea metodelor de testare a substanțelor chimice și în alte acte normative aprobate de Guvern. (4) Orice operator din lanțul de aprovizionare al unei substanțe sau al unui amestec este obligat: a) să transmită operatorului sau distribuitorului situat imediat în amontele lanțului de aprovizionare informațiile furnizate de către producători și importatori; b) să informeze operatorul sau distribuitorul situat imediat în amontele lanțului de aprovizionare despre noile informații pe care le-a identificat cu privire la pericolele și riscurile produselor chimice și măsurile de siguranță.		b) producătorii și importatorii nu dețin informațiile necesare conform alin. (1) lit. b) și nu există date disponibile pentru evaluarea corespunzătoare a substanței sau amestecului chimic fără efectuarea testelor de laborator; c) în literatura științifică de specialitate au apărut date cu privire la potențialele proprietăți periculoase ale substanței sau ale substanțelor componente ale amestecului chimic; d) nu există alte mijloace de obținere a informației necesare pentru evaluarea substanței sau amestecului fără efectuarea testelor. (3) Testările menționate la alin. (2) se efectuează în conformitate cu metodele indicate în Regulamentul privind stabilirea metodelor de testare a substanțelor chimice și în alte acte normative aprobate de Guvern. (4) Orice operator din lanțul de aprovizionare al unei substanțe sau al unui amestec este obligat: a) să transmită operatorului sau distribuitorului situat imediat în amontele lanțului de aprovizionare informațiile furnizate de către producători și importatori; b) să informeze operatorul sau distribuitorul situat imediat în amontele lanțului de aprovizionare despre noile informații pe care le-a identificat cu privire la pericolele și riscurile produselor chimice și măsurile de siguranță. (5) În scopul prevenirii sau al evitării producerii unei daune sănătății umane și mediului, toate persoanele fizice sau juridice care manipulează produse chimice trebuie să ia măsurile de protecție necesare pe care le-au identificat ele

	(5) În scopul prevenirii sau al evitării producerii unei daune sănătății umane și mediului, toate persoanele fizice sau juridice care manipulează produse chimice trebuie să ia măsurile de protecție necesare pe care le-au identificat ele însele sau care le-au fost comunicate în conformitate cu prezentul articol.		însele sau care le-au fost comunicate în conformitate cu prezentul articol. (6) Furnizorul unei substanțe sau al unui amestec, identificat ca furnizor de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, este responsabil pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.
Legea nr. 306/2018 privind siguranța alimentelor			
1.	**Articolul 7.** Cerințele generale privind siguranța alimentelor (1) Siguranța produselor alimentare și a materialelor care vin în contact cu produsele alimentare se asigură prin: a) reglementarea și controlul de stat în domeniul asigurării inofensivității acestora; b) luarea de către operatorii din domeniul alimentar a unor măsuri organizatorice, agrochimice, veterinare, tehnologice, sanitar-antiepidemice și fitosanitare în vederea respectării reglementărilor aplicabile în domeniul alimentar; c) controlul inofensivității produselor alimentare și a materialelor care vin în contact cu produsele alimentare, efectuat de către operatorii din domeniul alimentar pe tot lanțul alimentar, inclusiv prin aplicarea principiilor de analiză a riscurilor în punctele critice de control (HACCP – Hazard Analysis and Critical Control Points).	Articolul 7 se completează cu alineatul (13)[1] cu următorul cuprins: „(13)[1] Întreprinderile din domeniul alimentar, identificate ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor privind asigurarea securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.”	**Articolul 7.** Cerințele generale privind siguranța alimentelor (1) Siguranța produselor alimentare și a materialelor care vin în contact cu produsele alimentare se asigură prin: a) reglementarea și controlul de stat în domeniul asigurării inofensivității acestora; b) luarea de către operatorii din domeniul alimentar a unor măsuri organizatorice, agrochimice, veterinare, tehnologice, sanitar-antiepidemice și fitosanitare în vederea respectării reglementărilor aplicabile în domeniul alimentar; c) controlul inofensivității produselor alimentare și a materialelor care vin în contact cu produsele alimentare, efectuat de către operatorii din domeniul alimentar pe tot lanțul alimentar, inclusiv prin aplicarea principiilor de analiză a riscurilor în punctele critice de control (HACCP – Hazard Analysis and Critical Control Points).

	(2) Cerințele privind asigurarea inofensivității produselor alimentare sînt impuse prin Acordul privind aplicarea de măsuri sanitare și fitosanitare (SPS) al Organizației Mondiale a Comerțului, la care Republica Moldova este parte. Acestea sînt stabilite în baza evaluării riscurilor pentru sănătatea umană și sînt executorii. (3) Cerințele menționate la alin. (2) se bazează pe rezultatele cercetărilor științifice privind particularitățile de alimentație și nutriție și starea de sănătate a populației, pe identificarea și estimarea inofensivității și a pericolelor pe care le pot prezenta produsele alimentare și materialele care vin în contact cu produsele alimentare, pe evaluarea și analiza riscurilor de a periclita sănătatea umană ca urmare a consumului acestora, pe estimarea consecințelor sociale și economice ale consumului de produse alimentare periculoase și/sau nesigure. (4) Produsele alimentare și materialele care vin în contact cu produsele alimentare ce respectă reglementările din domeniul alimentar se consideră că nu prezintă riscuri pentru sănătatea umană. (5) Conformitatea unui produs alimentar cu cerințele specifice aplicabile acelui produs alimentar nu împiedică organul de control abilitat să restricționeze introducerea lui pe piață ori să solicite retragerea lui de pe piață în cazul în care există suspiciuni că, în pofida acestei conformități, produsul alimentar respectiv nu prezintă siguranță.		(2) Cerințele privind asigurarea inofensivității produselor alimentare sînt impuse prin Acordul privind aplicarea de măsuri sanitare și fitosanitare (SPS) al Organizației Mondiale a Comerțului, la care Republica Moldova este parte. Acestea sînt stabilite în baza evaluării riscurilor pentru sănătatea umană și sînt executorii. (3) Cerințele menționate la alin. (2) se bazează pe rezultatele cercetărilor științifice privind particularitățile de alimentație și nutriție și starea de sănătate a populației, pe identificarea și estimarea inofensivității și a pericolelor pe care le pot prezenta produsele alimentare și materialele care vin în contact cu produsele alimentare, pe evaluarea și analiza riscurilor de a periclita sănătatea umană ca urmare a consumului acestora, pe estimarea consecințelor sociale și economice ale consumului de produse alimentare periculoase și/sau nesigure. (4) Produsele alimentare și materialele care vin în contact cu produsele alimentare ce respectă reglementările din domeniul alimentar se consideră că nu prezintă riscuri pentru sănătatea umană. (5) Conformitatea unui produs alimentar cu cerințele specifice aplicabile acelui produs alimentar nu împiedică organul de control abilitat să restricționeze introducerea lui pe piață ori să solicite retragerea lui de pe piață în cazul în care există suspiciuni că, în pofida acestei conformități, produsul alimentar respectiv nu prezintă siguranță.

	(6) Se interzice producerea și/sau introducerea pe piață a produselor alimentare și a materialelor care vin în contact cu produsele alimentare care: a) nu corespund reglementărilor aplicabile din domeniul alimentar; b) sînt periculoase și pot afecta sănătatea umană în condiții normale de folosire a acestora de către consumator, ținînd cont de informația cuprinsă în etichetă sau pusă la dispoziția consumatorului în alt mod; c) sînt improprii consumului uman, fiind contaminate și/sau impure, sau prezentînd semne de alterare; d) sînt falsificate; e) nu au inclusă pe ambalaj sau pe etichetă informația prevăzută la art. 8 din Legea nr. 279/2017 privind informarea consumatorului cu privire la produsele alimentare; f) au termenul de valabilitate expirat; g) nu permit să le fie determinată originea și nu asigură trasabilitatea acestora; h) nu corespund cerințelor de comercializare cu amănuntul, aprobate de către Guvern. (7) Produsele alimentare și materialele care vin în contact cu produsele alimentare prevăzute la alin. (6), care se consideră neconforme reglementărilor aplicate în domeniul alimentar, sînt supuse utilizării condiționate sau nimicirii. (8) Atunci cînd se determină dacă un aliment prezintă sau nu siguranță, trebuie să se aibă în vedere:		(6) Se interzice producerea și/sau introducerea pe piață a produselor alimentare și a materialelor care vin în contact cu produsele alimentare care: a) nu corespund reglementărilor aplicabile din domeniul alimentar; b) sînt periculoase și pot afecta sănătatea umană în condiții normale de folosire a acestora de către consumator, ținînd cont de informația cuprinsă în etichetă sau pusă la dispoziția consumatorului în alt mod; c) sînt improprii consumului uman, fiind contaminate și/sau impure, sau prezentînd semne de alterare; d) sînt falsificate; e) nu au inclusă pe ambalaj sau pe etichetă informația prevăzută la art. 8 din Legea nr. 279/2017 privind informarea consumatorului cu privire la produsele alimentare; f) au termenul de valabilitate expirat; g) nu permit să le fie determinată originea și nu asigură trasabilitatea acestora; h) nu corespund cerințelor de comercializare cu amănuntul, aprobate de către Guvern. (7) Produsele alimentare și materialele care vin în contact cu produsele alimentare prevăzute la alin. (6), care se consideră neconforme reglementărilor aplicate în domeniul alimentar, sînt supuse utilizării condiționate sau nimicirii. (8) Atunci cînd se determină dacă un aliment prezintă sau nu siguranță, trebuie să se aibă în vedere: a) condițiile de folosire a alimentului de către consumator și la fiecare etapă a lanțului alimentar;

	a) condiţiile de folosire a alimentului de către consumator şi la fiecare etapă a lanţului alimentar; b) informaţiile furnizate consumatorului, inclusiv cele de pe etichetă sau alte informaţii general disponibile pentru consumator în vederea evitării unor anumite efecte negative asupra sănătăţii ale alimentului respectiv sau ale categoriei respective de alimente. (9) Atunci cînd se determină dacă un aliment dăunează sănătăţii, trebuie să se ia în considerare: a) efectul probabil imediat şi/sau de scurtă durată, şi/sau de lungă durată al acestuia atît asupra persoanei care îl consumă, cît şi asupra generaţiilor viitoare; b) efectele toxice cumulative probabile ale acestuia; c) sensibilitatea alimentară a unei anumite categorii de consumatori, în cazul în care alimentul respectiv îi este destinat. (10) Produsele alimentare trebuie să satisfacă necesităţile fiziologice ale omului în substanţe nutritive şi în energie, să fie inofensive, să nu conţină contaminanţi, microorganisme şi alte organisme ori substanţe biologice în cantităţi care să depăşească valorile-limită stabilite în reglementările din domeniu alimentar, să nu prezinte în alt mod pericol pentru om, să fie produse şi introduse pe piaţă în condiţii de igienă conform prevederilor Legii nr. 296/2017 privind cerinţele generale de igienă a produselor alimentare.		b) informaţiile furnizate consumatorului, inclusiv cele de pe etichetă sau alte informaţii general disponibile pentru consumator în vederea evitării unor anumite efecte negative asupra sănătăţii ale alimentului respectiv sau ale categoriei respective de alimente. (9) Atunci cînd se determină dacă un aliment dăunează sănătăţii, trebuie să se ia în considerare: a) efectul probabil imediat şi/sau de scurtă durată, şi/sau de lungă durată al acestuia atît asupra persoanei care îl consumă, cît şi asupra generaţiilor viitoare; b) efectele toxice cumulative probabile ale acestuia; c) sensibilitatea alimentară a unei anumite categorii de consumatori, în cazul în care alimentul respectiv îi este destinat. (10) Produsele alimentare trebuie să satisfacă necesităţile fiziologice ale omului în substanţe nutritive şi în energie, să fie inofensive, să nu conţină contaminanţi, microorganisme şi alte organisme ori substanţe biologice în cantităţi care să depăşească valorile-limită stabilite în reglementările din domeniu alimentar, să nu prezinte în alt mod pericol pentru om, să fie produse şi introduse pe piaţă în condiţii de igienă conform prevederilor Legii nr. 296/2017 privind cerinţele generale de igienă a produselor alimentare. (11) Producerea, transportul, depozitarea şi introducerea pe piaţă a produselor alimentare şi a materialelor care vin în contact cu produsele alimentare se efectuează în spaţii şi în condiţii

	(11) Producerea, transportul, depozitarea și introducerea pe piață a produselor alimentare și a materialelor care vin în contact cu produsele alimentare se efectuează în spații și în condiții ce corespund cerințelor prezentei legi, iar operatorii din domeniul alimentar dețin autorizații sanitar-veterinare de funcționare eliberate în conformitate cu art. 18 din Legea nr. 221/2007 privind activitatea sanitar-veterinară sau dețin certificate de înregistrare în domeniul siguranței alimentelor eliberate în conformitate cu art. 231 din Legea nr. 50/2013 cu privire la controalele oficiale pentru verificarea conformității cu legislația privind hrana pentru animale și produsele alimentare și cu normele de sănătate și de bunăstare a animalelor. (12) Operatorii din domeniul alimentar vor întreprinde măsurile de rigoare pentru a elimina riscul de contaminare sau de deteriorare a alimentelor și de transformare a acestora în produse periculoase pentru consumatori. (13) În cazul în care un produs alimentar care nu prezintă siguranță face parte dintr-un transport, dintr-un lot sau dintr-o livrare de mărfuri alimentare de la o sursă sau din aceeași clasă ori având aceeași descriere, se presupune că toate produsele alimentare din respectivul transport, lot sau din respectiva livrare nu prezintă siguranță, cu excepția cazurilor în care se constată, în urma unei evaluări detaliate, că nu s-a identificat nicio		ce corespund cerințelor prezentei legi, iar operatorii din domeniul alimentar dețin autorizații sanitar-veterinare de funcționare eliberate în conformitate cu art. 18 din Legea nr. 221/2007 privind activitatea sanitar-veterinară sau dețin certificate de înregistrare în domeniul siguranței alimentelor eliberate în conformitate cu art. 231 din Legea nr. 50/2013 cu privire la controalele oficiale pentru verificarea conformității cu legislația privind hrana pentru animale și produsele alimentare și cu normele de sănătate și de bunăstare a animalelor. (12) Operatorii din domeniul alimentar vor întreprinde măsurile de rigoare pentru a elimina riscul de contaminare sau de deteriorare a alimentelor și de transformare a acestora în produse periculoase pentru consumatori. (13) În cazul în care un produs alimentar care nu prezintă siguranță face parte dintr-un transport, dintr-un lot sau dintr-o livrare de mărfuri alimentare de la o sursă sau din aceeași clasă ori având aceeași descriere, se presupune că toate produsele alimentare din respectivul transport, lot sau din respectiva livrare nu prezintă siguranță, cu excepția cazurilor în care se constată, în urma unei evaluări detaliate, că nu s-a identificat nicio dovadă care să indice că restul transportului, lotului sau al livrării nu prezintă siguranță. „(13)[1] Întreprinderile din domeniul alimentar, identificate ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor privind asigurarea securității cibernetice stabilite

	dovadă care să indice că restul transportului, lotului sau al livrării nu prezintă siguranță.		de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice."
2.	**Articolul 8.** Responsabilități privind siguranța alimentelor (1) Operatorii din domeniul alimentar și operatorii din domeniul hranei pentru animale sînt responsabili pe întregul lanț alimentar de respectarea reglementărilor din domeniul alimentar. (2) În cazul în care operatorul din domeniul alimentar consideră sau are motive întemeiate să considere că un produs alimentar pe care l-a importat, produs, procesat, fabricat sau distribuit nu satisface cerințele de siguranță și poate fi dăunător pentru sănătatea umană, el inițiază imediat procedurile de retragere a produsului alimentar de pe piață, dacă produsul respectiv a ieșit de sub controlul său, și informează imediat în acest sens Agenția Națională pentru Siguranța Alimentelor. Operatorul informează, în mod eficient și precis, consumatorul în legătură cu motivul retragerii produsului alimentar și retrage de la consumator produsele deja livrate, atunci cînd alte măsuri nu sînt suficiente pentru a atinge un nivel ridicat de protecție a sănătății. (3) Operatorul din domeniul alimentar informează imediat organul de control abilitat cu privire la acțiunile întreprinse pentru prevenirea riscurilor asupra consumatorului final și nu împiedică ori descurajează orice persoană să coopereze cu autoritățile	Articolul 8 se completează cu alineatul $(9)^1$, cu următorul cuprins: „$(9)^1$ Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la art. 7 alin. (13)1 se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia."	**Articolul 8.** Responsabilități privind siguranța alimentelor (1) Operatorii din domeniul alimentar și operatorii din domeniul hranei pentru animale sînt responsabili pe întregul lanț alimentar de respectarea reglementărilor din domeniul alimentar. (2) În cazul în care operatorul din domeniul alimentar consideră sau are motive întemeiate să considere că un produs alimentar pe care l-a importat, produs, procesat, fabricat sau distribuit nu satisface cerințele de siguranță și poate fi dăunător pentru sănătatea umană, el inițiază imediat procedurile de retragere a produsului alimentar de pe piață, dacă produsul respectiv a ieșit de sub controlul său, și informează imediat în acest sens Agenția Națională pentru Siguranța Alimentelor. Operatorul informează, în mod eficient și precis, consumatorul în legătură cu motivul retragerii produsului alimentar și retrage de la consumator produsele deja livrate, atunci cînd alte măsuri nu sînt suficiente pentru a atinge un nivel ridicat de protecție a sănătății. (3) Operatorul din domeniul alimentar informează imediat organul de control abilitat cu privire la acțiunile întreprinse pentru prevenirea riscurilor asupra consumatorului final și nu împiedică ori descurajează orice persoană să coopereze cu autoritățile administrației publice în cazul în care aceasta ar

	administrației publice în cazul în care aceasta ar putea preveni, reduce sau elimina un risc prezentat de un produs alimentar. (4) Operatorii din domeniul alimentar cooperează cu organul de control abilitat la acțiunile întreprinse pentru evitarea sau reducerea riscurilor prezentate de un produs alimentar introdus pe piață. (5) Controlul de stat privind asigurarea inofensivității și a calității produselor alimentare și ale materialelor care vin în contact cu produsele alimentare aflate în uz la toate etapele lanțului alimentar se efectuează de către Agenția Națională pentru Siguranța Alimentelor. În acest scop, agenția nominalizată monitorizează și verifică respectarea cerințelor prevăzute în reglementările din domeniul alimentar de către operatorii din domeniul alimentar și operatorii din domeniul hranei pentru animale pe întregul lanț alimentar. (6) Controlul de stat al operatorilor din domeniul alimentar și operatorilor din domeniul hranei pentru animale care practică activitate de întreprinzător se planifică, se efectuează și se înregistrează în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat asupra activității de întreprinzător. (7) Prin derogare de la prevederile alin. (5), controlul și supravegherea de stat privind asigurarea inofensivității și calității produselor alimentare comercializate în		putea preveni, reduce sau elimina un risc prezentat de un produs alimentar. (4) Operatorii din domeniul alimentar cooperează cu organul de control abilitat la acțiunile întreprinse pentru evitarea sau reducerea riscurilor prezentate de un produs alimentar introdus pe piață. (5) Controlul de stat privind asigurarea inofensivității și a calității produselor alimentare și ale materialelor care vin în contact cu produsele alimentare aflate în uz la toate etapele lanțului alimentar se efectuează de către Agenția Națională pentru Siguranța Alimentelor. În acest scop, agenția nominalizată monitorizează și verifică respectarea cerințelor prevăzute în reglementările din domeniul alimentar de către operatorii din domeniul alimentar și operatorii din domeniul hranei pentru animale pe întregul lanț alimentar. (6) Controlul de stat al operatorilor din domeniul alimentar și operatorilor din domeniul hranei pentru animale care practică activitate de întreprinzător se planifică, se efectuează și se înregistrează în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat asupra activității de întreprinzător. (7) Prin derogare de la prevederile alin. (5), controlul și supravegherea de stat privind asigurarea inofensivității și calității produselor alimentare comercializate în farmacii, privind siguranța și calitatea materialelor care vin în contact cu produsele alimentare introduse pe piață și privind etichetarea nutrițională și

	farmacii, privind siguranța și calitatea materialelor care vin în contact cu produsele alimentare introduse pe piață și privind etichetarea nutrițională și înscrierea mențiunilor de sănătate pe produsele alimentare se efectuează de către Agenția Națională pentru Sănătate Publică în conformitate cu atribuțiile stabilite de legislația națională. (8) La elaborarea sau adaptarea reglementărilor din domeniul alimentar se iau în considerare normele și recomandările internaționale, inclusiv cele ale Comisiei Codex Alimentarius și ale Uniunii Europene. (9) Operatorii din domeniul alimentar care produc, achiziționează, depozitează, transportă și introduc pe piață produse alimentare sau prestează servicii de alimentație publică trebuie să respecte prevederile Legii nr. 296/2017 privind cerințele generale de igienă a produselor alimentare și să efectueze măsuri de asigurare a siguranței produselor respective.		înscrierea mențiunilor de sănătate pe produsele alimentare se efectuează de către Agenția Națională pentru Sănătate Publică în conformitate cu atribuțiile stabilite de legislația națională. (8) La elaborarea sau adaptarea reglementărilor din domeniul alimentar se iau în considerare normele și recomandările internaționale, inclusiv cele ale Comisiei Codex Alimentarius și ale Uniunii Europene. (9) Operatorii din domeniul alimentar care produc, achiziționează, depozitează, transportă și introduc pe piață produse alimentare sau prestează servicii de alimentație publică trebuie să respecte prevederile Legii nr. 296/2017 privind cerințele generale de igienă a produselor alimentare și să efectueze măsuri de asigurare a siguranței produselor respective. (9)[1] Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la art. 7 alin. (13)1 se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia.
Articolul 22 din Legea nr. 192/2019 privind securitatea aeronautică			
1.	(1) Asigurarea securității cibernetice în domeniul aviației civile reprezintă o atribuție a autorității administrative de implementare și realizare a politicilor în domeniul aviației civile, precum și a instituției publice responsabile de implementarea politicii	Alineatul (1) va avea următorul cuprins: „(1) Pentru asigurarea securității cibernetice în domeniul aviației civile sunt responsabili operatorii aeronautici, entitățile aeronautice, autoritatea administrativă de implementare și	(1) Pentru asigurarea securității cibernetice în domeniul aviației civile sunt responsabili operatorii aeronautici, entitățile aeronautice, autoritatea administrativă de implementare și realizare a politicilor în domeniul aviației civile și autoritatea competentă în domeniul securității

	statului în domeniul securităţii cibernetice la nivel naţional.	realizare a politicilor în domeniul aviației civile și autoritatea competentă în domeniul securității cibernetice în limitele stabilite de cadrul normativ."	cibernetice în limitele stabilite de cadrul normativ.
2.	(1) Asigurarea securităţii cibernetice în domeniul aviaţiei civile reprezintă o atribuţie a autorităţii administrative de implementare şi realizare a politicilor în domeniul aviaţiei civile, precum şi a instituţiei publice responsabile de implementarea politicii statului în domeniul securităţii cibernetice la nivel naţional. (2) Operatorii aeronautici şi entităţile aeronautice evaluează riscurile la adresa securităţii cibernetice, conform procedurii aprobate de către autoritatea administrativă de implementare şi realizare a politicilor în domeniul aviaţiei civile. În baza evaluării respective, operatorii aeronautici şi entităţile aeronautice elaborează şi implementează măsurile corespunzătoare de protecţie în scopul asigurării confidenţialităţii, integrităţii şi accesibilităţii sistemelor informaţionale şi a reţelelor de comunicaţii electronice de importanţă critică, precum şi a datelor utilizate în aviaţia civilă, a căror afectare poate pune în pericol siguranţa şi securitatea aviaţiei civile.	Se completează cu alineatele (3) și (4) cu următorul cuprins: „(3) Operatorii aeronautici și entitățile aeronautice, identificați ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (4) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alineatul (3) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia."	(1) Pentru asigurarea securității cibernetice în domeniul aviației civile sunt responsabili operatorii aeronautici, entitățile aeronautice, autoritatea administrativă de implementare și realizare a politicilor în domeniul aviației civile și autoritatea competentă în domeniul securității cibernetice în limitele stabilite de cadrul normativ. (2) Operatorii aeronautici şi entităţile aeronautice evaluează riscurile la adresa securităţii cibernetice, conform procedurii aprobate de către autoritatea administrativă de implementare şi realizare a politicilor în domeniul aviaţiei civile. În baza evaluării respective, operatorii aeronautici şi entităţile aeronautice elaborează şi implementează măsurile corespunzătoare de protecţie în scopul asigurării confidenţialităţii, integrităţii şi accesibilităţii sistemelor informaţionale şi a reţelelor de comunicaţii electronice de importanţă critică, precum şi a datelor utilizate în aviaţia civilă, a căror afectare poate pune în pericol siguranţa şi securitatea aviaţiei civile. (3) Operatorii aeronautici și entitățile aeronautice, identificați ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de

			punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (4) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alineatul (3) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia.
Codul transportului feroviar nr. 19/2022			
1.	**Articolul 26.** Activitatea de supraveghere a siguranței feroviare (1) Autoritatea Feroviară efectuează supravegherea continuă a respectării condițiilor: a) de desfășurare a activității de transport feroviar de către întreprinderile feroviare; b) de certificare a siguranței feroviare pentru întreprinderile feroviare; c) de autorizare în materie de siguranță a Administratorului infrastructurii; d) de aplicare a sistemului de management al siguranței. (2) Activitatea de supraveghere a siguranței feroviare se realizează prin evaluarea situațiilor economico-financiare semestriale ale entităților din domeniul transportului feroviar, a rapoartelor privind incidentele și accidentele feroviare, a procesului de întreținere a vehiculelor feroviare și a procesului de întreținere a infrastructurii feroviare.	Articolul 26 se completează cu alineatul $(1)^1$ cu următorul cuprins: „$(1)^1$ Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la art. 89 alin. $(3)^1$ se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia.”	**Articolul 26.** Activitatea de supraveghere a siguranței feroviare (1) Autoritatea Feroviară efectuează supravegherea continuă a respectării condițiilor: a) de desfășurare a activității de transport feroviar de către întreprinderile feroviare; b) de certificare a siguranței feroviare pentru întreprinderile feroviare; c) de autorizare în materie de siguranță a Administratorului infrastructurii; d) de aplicare a sistemului de management al siguranței. $(1)^1$ Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la art. 89 alin. $(3)^1$ se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia. (2) Activitatea de supraveghere a siguranței feroviare se realizează prin evaluarea situațiilor

	(3) Întreprinderile feroviare și Administratorul infrastructurii achită plăți pentru supravegherea respectării condițiilor stabilite la alin. (1). Aceste plăți constituie venituri colectate de Autoritatea Feroviară pentru finanțarea cheltuielilor aprobate în bugetul acesteia. (4) Nomenclatorul serviciilor de supraveghere a siguranței feroviare, mărimea plăților, precum și modul de achitare a acestor plăți se stabilesc de Guvern.		economico-financiare semestriale ale entităților din domeniul transportului feroviar, a rapoartelor privind incidentele și accidentele feroviare, a procesului de întreținere a vehiculelor feroviare și a procesului de întreținere a infrastructurii feroviare. (3) Întreprinderile feroviare și Administratorul infrastructurii achită plăți pentru supravegherea respectării condițiilor stabilite la alin. (1). Aceste plăți constituie venituri colectate de Autoritatea Feroviară pentru finanțarea cheltuielilor aprobate în bugetul acesteia. (4) Nomenclatorul serviciilor de supraveghere a siguranței feroviare, mărimea plăților, precum și modul de achitare a acestor plăți se stabilesc de Guvern.
2.	**Articolul 89.** Principii de bază în gestionarea siguranței feroviare (1) Ministerul, Autoritatea Feroviară (în calitate de autoritate națională de siguranță feroviară), Administratorul infrastructurii și întreprinderile feroviare, fiecare în conformitate cu propriile responsabilități, asigură următoarele: a) menținerea și îmbunătățirea în mod continuu a siguranței feroviare, acordând prioritate prevenirii accidentelor atunci când aceasta este judicios și fezabil; b) aplicarea, într-o manieră transparentă și nediscriminatorie, a normelor de siguranță feroviară; c) dezvoltarea unui sistem feroviar uniform;	Articolul 89 se completează cu alineatul $(3)^1$ cu următorul cuprins: „$(3)^1$ Administratorul infrastructurii și întreprinderile feroviare, identificați ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.”	**Articolul 89.** Principii de bază în gestionarea siguranței feroviare (1) Ministerul, Autoritatea Feroviară (în calitate de autoritate națională de siguranță feroviară), Administratorul infrastructurii și întreprinderile feroviare, fiecare în conformitate cu propriile responsabilități, asigură următoarele: a) menținerea și îmbunătățirea în mod continuu a siguranței feroviare, acordând prioritate prevenirii accidentelor atunci când aceasta este judicios și fezabil; b) aplicarea, într-o manieră transparentă și nediscriminatorie, a normelor de siguranță feroviară; c) dezvoltarea unui sistem feroviar uniform; d) abordări bazate pe sistem privind măsurile de dezvoltare și îmbunătățire a siguranței feroviare.

	d) abordări bazate pe sistem privind măsurile de dezvoltare și îmbunătățire a siguranței feroviare. (2) Administratorul infrastructurii și întreprinderile feroviare sunt responsabile de funcționarea în siguranță a sistemului feroviar și de controlul riscurilor asociate, pun în aplicare măsurile necesare de control al riscurilor, cooperează în vederea aplicării normelor și a standardelor naționale și internaționale de siguranță feroviară și stabilesc sisteme de management al siguranței. (3) Administratorul infrastructurii și întreprinderile feroviare răspund de părțile componente ale sistemului feroviar și de funcționarea în siguranță a acestora, inclusiv de furnizarea de materiale și contractarea de servicii, față de utilizatori, clienți și angajați. (4) Răspunderea Administratorului infrastructurii și a întreprinderilor feroviare prevăzută la alin. (3) nu-i scutește de răspundere pe producătorii de piese integrale și de elemente constitutive de interoperabilitate ale subsistemelor individuale, pe entitățile responsabile cu întreținerea vehiculelor feroviare, pe deținătorii de vehicule feroviare și pe furnizorii de alte servicii necesare vehiculelor feroviare, de structuri, instalații, echipamente, materiale. Toate acestea trebuie să fie conforme cu cerințele și condițiile stipulate privind utilizarea lor, astfel încât Administratorul infrastructurii sau		(2) Administratorul infrastructurii și întreprinderile feroviare sunt responsabile de funcționarea în siguranță a sistemului feroviar și de controlul riscurilor asociate, pun în aplicare măsurile necesare de control al riscurilor, cooperează în vederea aplicării normelor și a standardelor naționale și internaționale de siguranță feroviară și stabilesc sisteme de management al siguranței. (3) Administratorul infrastructurii și întreprinderile feroviare răspund de părțile componente ale sistemului feroviar și de funcționarea în siguranță a acestora, inclusiv de furnizarea de materiale și contractarea de servicii, față de utilizatori, clienți și angajați. (3)[1] Administratorul infrastructurii și întreprinderile feroviare, identificați ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (4) Răspunderea Administratorului infrastructurii și a întreprinderilor feroviare prevăzută la alin. (3) nu-i scutește de răspundere pe producătorii de piese integrale și de elemente constitutive de interoperabilitate ale subsistemelor individuale, pe entitățile responsabile cu întreținerea vehiculelor feroviare, pe deținătorii de vehicule feroviare și pe furnizorii de alte servicii necesare vehiculelor feroviare, de structuri, instalații, echipamente,

	întreprinderile feroviare să le poată folosi în siguranță în sistemul feroviar.		materiale. Toate acestea trebuie să fie conforme cu cerințele și condițiile stipulate privind utilizarea lor, astfel încât Administratorul infrastructurii sau întreprinderile feroviare să le poată folosi în siguranță în sistemul feroviar.
Articolul 39 din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere			
1.	**Articolul 39.** Cerințe de Securitate aplicabile prestatorilor de servicii de încredere (1) Prestatorii de servicii de încredere calificați și necalificați aplică măsurile tehnice și organizaționale corespunzătoare pentru gestionarea riscurilor la adresa securității serviciilor de încredere pe care le prestează. (2) Prestatorii de servicii de încredere calificați și necalificați notifică organului de supraveghere și control, nu mai târziu de 24 de ore din momentul constatării, încălcarea securității sau pierderea integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de aceștia. În cazul în care încălcarea securității sau pierderea integrității este de natură să afecteze în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de încredere, prestatorul de servicii de încredere notifică și persoanei fizice sau juridice respective încălcarea securității sau pierderea integrității, fără întârzieri nejustificate. (3) Organul de supraveghere și control notificat informează publicul sau solicită prestatorului de servicii de încredere să facă acest lucru în cazul în care consideră că	Articolul 39 va avea următorul cuprins: „**Articolul 39.** Asigurarea securității cibernetice de către prestatorii de servicii de încredere (1) În scopul asigurării securității rețelelor și a sistemelor informatice utilizate la prestarea serviciilor de încredere, prestatorii de servicii de încredere sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia. (3) În exercitarea supravegherii și controlului respectării prevederilor Legii nr. 48/2023 privind securitatea cibernetică, autoritatea competentă în temeiul acestei legi informează, în termen de 5 zile, organul de supraveghere și control despre	**Articolul 39.** Asigurarea securității cibernetice de către prestatorii de servicii de încredere (1) În scopul asigurării securității rețelelor și a sistemelor informatice utilizate la prestarea serviciilor de încredere, prestatorii de servicii de încredere sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia. (3) În exercitarea supravegherii și controlului respectării prevederilor Legii nr. 48/2023 privind securitatea cibernetică, autoritatea competentă în temeiul acestei legi informează, în termen de 5 zile, organul de supraveghere și control despre încălcările depistate și eventualele sancțiuni aplicate.

	dezvăluirea încălcării securității sau pierderea integrității servește interesului public.	încălcările depistate și eventualele sancțiuni aplicate.”	