Cuprins

Proiect

Lege privind securitatea cibernetică

Capitolul I. Dispoziții generale

Articolul 1. Obiectul de reglementare al legii

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

Articolul 2. Principalele noțiuni și definițiile lor

În sensul prezentei legi, următoarele noțiuni înseamnă:

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

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

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

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

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

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

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

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

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

10) ***rețea și sistem informatic*** :

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

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

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

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

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

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

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

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

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

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

Articolul 3. Domeniul de aplicare

(1) Prezenta lege se aplică persoanelor juridice care se califică drept întreprinderi mijlocii sau care depășesc plafoanele pentru întreprinderile mijlocii, potrivit clasificării prevăzute de legislația cu privire la întreprinderile mici și mijlocii, care furnizează servicii în unul sau mai multe dintre sectoarele sau subsectoarele stabilite de către Guvern, instituită conform articolului 7, și care sunt identificate de către autoritatea competentă în conformitate cu prevederile prezentei legi și a actelor normative de punere a acesteia în aplicare.

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

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

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

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

d) furnizează servicii de înregistrare a numelor de domenii;

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

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

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

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

(3) Prevederile prezentei legi se aplică și persoanelor juridice de drept public.

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

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

(6) În cazul în care tratatele internaționale la care Republica Moldova este parte stabilesc măsuri de securitate ale rețelelor și sistemelor informatice, prevederile respective se aplică în coroborare cu cerințele prevăzute de prevederile prezentei legi.

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

(8) În cazul în care obligațiile, prevăzute la alineatul (7), stabilite de legile sectoriale specifice, sunt aplicabile unui cerc mai restrâns de persoane juridice decât cel prevăzut de prezenta lege și de actele normative de pune în aplicare a acesteia, prevederile prezentei legi se aplică persoanelor juridice care nu cad sub incidența obligațiilor impuse de legile sectoriale specifice.

(9) Prevederile alineatelor (7) și (8) se aplică de către autoritatea competentă pentru fiecare caz în parte în procesul de identificare a furnizorilor de servicii.

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

Articolul 4. Identificarea furnizorilor de servicii

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

(2) În scopul întocmirii listei menționate la alineatul (1), persoanele juridice, la solicitarea autorității competente, sunt obligați să prezinte următoarele date: denumirea persoanei juridice, adresa și datele de contact actualizate, inclusiv adresele de e-mail, gama de IP-uri și numerele de telefon, sectorul și subsectorul relevant în care își desfășoară activitatea.

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

Articolul 5. Principiile de asigurare a securității cibernetice

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

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

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

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

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

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

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

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

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

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

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

Articolul 7. Autoritatea competentă

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

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

(3) Autoritatea competentă exercită următoarele atribuții principale:

a) identifică furnizorii de servicii pe teritoriul Republicii Moldova;

b) elaborează și promovează practici comune pentru gestionarea incidentelor cibernetice și a riscurilor și pentru sistemele de clasificare a incidentelor cibernetice, a riscurilor și a informațiilor;

c) asigură interacțiunea strategică la nivel internațional și schimbul de experiență cu alte state, organizații internaționale sau entități create de acestea privind aspecte legate de securitatea rețelelor și a sistemelor informatice, studiază exemple de bune practici privind riscurile și incidente cibernetice;

d) asigură interacțiunea cu autoritățile și instituțiile publice naționale;

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

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

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

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

i) alte atribuții care decurg din prevederile prezentei legi.

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

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

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

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

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

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

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

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

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

i) asigură coordonarea procesului de divulgare a vulnerabilităților în conformitate cu cadrul normativ aprobat de Guvern, la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

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

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

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

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

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

(1) Pentru asigurarea securității cibernetice la nivel guvernamental, Guvernul instituie centrul de răspuns la incidentele cibernetice la nivelul rețelelor și sistemelor informatice ale căror proprietar este statul, desemnează autoritatea sau instituția publică responsabilă de exercitarea funcțiilor respective și stabilește modul de organizare și funcționare al acestuia.

(2) Centrul de răspuns la incidentele de securitate cibernetică la nivel guvernamental constituie punctul unic de contact şi de raportare a incidentelor cibernetice pentru persoanele juridice de drept public. Guvernul este responsabil de asigurarea capacității necesare a centrului de răspuns la incidentele de securitate cibernetică la nivel guvernamental pentru prevenirea, analiza, identificarea şi răspunsul la incidentele cibernetice la nivel guvernamental.

(3) Autoritatea sau instituția publică desemnată de Guvern să exercite funcția de centru de răspuns la incidentele cibernetice la nivel guvernamental, este responsabilă de asigurarea

cooperării cu autoritatea competentă și echipa de răspuns la incidentele cibernetice la nivel național.

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

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

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

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

a) obiectivele măsurilor și ale activităților naționale de pregătire;
b) sarcinile și responsabilitățile autorităților naționale competente;
c) procedurile de gestionare a crizelor și canalele de schimb de informații;
d) măsurile de pregătire, inclusiv exerciții și activități de formare;
e) părțile interesate relevante din sectorul public și privat și infrastructura implicată;
f) procedurile și mecanismele de interacțiune dintre autoritățile și instituțiile publice responsabile la nivel național, precum și de interacțiune coordonată a acestora în gestionarea incidentelor și a crizelor de securitate cibernetică de mare amploare, inclusiv a celor la nivel european și internațional.

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

Articolul 10. Registrul de stat al incidentelor cibernetice

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

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

Capitolul III. Obligații privind asigurarea securității cibernetice

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

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

a) prevenirii incidentelor cibernetice;
b) soluționării incidentelor cibernetice;

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

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

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

a) să evalueze vulnerabilitățile și riscurile rețelei și sistemului informatic, să determine severitatea impactului unui eventual incident cibernetic survenit urmare a materializării riscurilor, precum și să descrie măsurile pentru soluționarea unui incident cibernetic.

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

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

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

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

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

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

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

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

b) la propunerea autorității competente, aprobă cerințele specifice privind măsurile de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(7) În cazul soluționării unui incident cibernetic cu impact semnificativ, furnizorul de servicii este obligat, în termen de 30 zile, să transmită autorității competente un raport care să includă cel puțin informații despre cauzele producerii incidentului cibernetic, timpul de soluționare a acestuia, măsurile aplicate și impactul incidentului cibernetic.

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

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

Articolul 13. Notificarea voluntară

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

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

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

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

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

(1) Furnizorii de servicii care sunt persoane juridice de drept public, în procesul de administrare a rețelelor și sistemelor informatice sunt obligate să aplice măsurile stabilite la articolului 11 alineatele (1)-(3) și cerințele de notificare obligatorie a unui incident cibernetic prevăzute la articolul 12.

(2) Cerințele minime de securitate a rețelelor și sistemelor informatice prevăzute în alineatul (1) sunt stabilite de Guvern la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

Articolul 15. Gestionarea incidentelor cibernetice

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

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

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

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

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

Articolul 16. Schimbul de informații

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

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

b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de limitare și prevenire a amenințărilor, strategiile de

atenuare sau etapele proceselor de răspuns și de recuperare sau promovarea colaborării dintre persoanele juridice de drept public și cel de drept privat în domeniul cercetării amenințărilor cibernetice.

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

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

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

Capitolul IV. Supraveghere și control de stat

Articolul 17. Supravegherea de stat în domeniul securității cibernetice

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

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

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

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

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

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

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

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

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

Articolul 18. Controlul

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

a) legalitatea și respectarea competenței stabilite de lege;

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

c) tratarea dubiilor în favoarea furnizorului de servicii;

d) efectuarea controlului pe cheltuiala statului;

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

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

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

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

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

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

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

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

Articolul 19. Protecția datelor cu caracter personal

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

Capitolul V. Răspunderea

Articolul. 20 Răspunderea pentru încălcarea dispozițiilor prezentei legi

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

(2) Personalul autorităților/instituțiilor publice, furnizorilor de servicii care interacționează cu autoritatea competentă în condițiile prezentei legi, poartă răspundere, în conformitate cu legislația, pentru neîndeplinirea atribuțiilor funcționale stabilite de actele normative.

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

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

Capitolul VI. Dispoziții finale și tranzitorii

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

(1) Prezenta lege intră în vigoare în termen de 1 an din data publicării.

(2) Guvernul:

a) în termen de 6 luni din data publicării prezentei legi, va întreprinde măsurile necesare pentru instituirea/desemnarea autorității competente, reglementarea modului de organizare și funcționare a acesteia și dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite prin prezenta lege;

b) în termen de 6 luni din data publicării prezentei legi va prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege;

c) în termen de 9 luni din data publicării prezentei legi va aduce actele sale normative în concordanță cu prezenta lege, va asigura elaborarea și va adopta actele normative necesare punerii în aplicare a prevederilor prezentei legi, inclusiv va determina autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice;

d) în termen de 6 luni din data intrării în vigoare a prezentei legi va elabora și va aproba Strategia națională în domeniul securității cibernetice.

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

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

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

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

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

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

f) să asigure confidențialitatea și credibilitatea operațiunilor lor;

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

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

(4) Autoritatea competentă:

în termen de 3 luni de la data publicării actului de desemnare în conformitate cu prevederile articolul 7 alineatul (1) din prezenta lege, în cooperare cu autoritățile și instituțiile publice responsabile de realizarea politicii statutului în sectoarele sau subsectoarele stabilite de Guvern în temeiul prevederilor articolului 4 alineatul (3), precum și, dacă e cazul, cu cele de reglementare a acestor domenii, va identifica furnizorii de servicii, îi va notifica în modul stabilit și îi va include în Lista furnizorilor de servicii, întocmită în condițiile prezentei legi;

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

(5) Autoritățile și instituțiile publice vor acorda suportul necesar autorității competente în procesul de identificare a furnizorilor de servicii.