PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAŢILOR SENATUL

L E G E

privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice

Parlamentul României adoptă prezenta lege.

CAPITOLUL I
Dispoziţii generale

SECŢIUNEA 1
Obiect şi scop

Art. 1. – Prezenta lege stabileşte cadrul juridic şi instituţional, măsurile şi mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice şi a stimulării cooperării în domeniu.

Art. 2. – (1) Scopul prezentei legi îl constituie:

a) stabilirea cadrului de cooperare la nivel naţional şi de participare la nivel european şi internaţional în domeniul asigurării securităţii reţelelor şi sistemelor informatice;

b) desemnarea autorităţii competente la nivel naţional şi a entităţilor de drept public şi privat care deţin competenţe şi responsabilităţi în aplicarea prevederilor prezentei legi, a Punctului unic de contact la nivel naţional şi a echipei naţionale de intervenţie în caz de incidente de securitate informatică;

c) stabilirea cerinţelor de securitate şi notificare pentru operatorii de servicii esenţiale şi pentru furnizorii de servicii digitale şi instituirea mecanismelor de actualizare a acestora în funcţie de evoluţia ameninţărilor la adresa securităţii reţelelor şi sistemelor informatice.

(2) Prezenta lege nu se aplică instituţiilor din domeniul apărării, ordinii publice şi securităţii naţionale, precum şi Oficiului Registrului Naţional al Informaţiilor Secrete de Stat.

SECŢIUNEA a 2-a
Definiţii şi principii

Art. 3. – În sensul prezentei legi, termenii şi expresiile de mai jos au următoarea semnificaţie:

a) *administrarea incidentului* – toate procedurile utilizate pentru detectarea, analiza şi limitarea unui incident şi răspunsul la acesta;

b) *domain name system*, denumit în continuare *DNS* – sistem de atribuire de nume distribuite ierarhic într-o reţea în care se efectuează căutări de nume de domenii;

c) *furnizor de servicii digitale* – orice persoană juridică care furnizează un serviciu digital;

d) *furnizor de servicii DNS* – entitate care furnizează servicii DNS pe internet;

e) *incident* – orice eveniment care are un impact real negativ asupra securităţii reţelelor şi a sistemelor informatice;

f) *internet exchange point*, denumit în continuare *IXP* – facilitate a reţelei care permite interconectarea a mai mult de două sisteme autonome independente, în special în scopul facilitării schimbului de trafic de internet; IXP furnizează interconectare doar pentru sisteme autonome; IXP nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre orice pereche de sisteme autonome participante şi nici nu modifică sau interferează într-un alt mod cu acest trafic;

g) *motor de căutare online* – un serviciu digital care permite utilizatorilor să caute, în principiu, în toate site-urile internet sau site-urile internet într-o anumită limbă pe baza unei interogări privind orice subiect sub forma unui cuvânt, a unei fraze sau a unei alte informaţii-cheie şi care revine cu linkuri în care se pot găsi informaţii legate de conţinutul căutat;

h) *operator de servicii esenţiale* – persoană fizică sau juridică de drept public sau privat de tipul celor prevăzute în anexa care face parte integrantă din prezenta lege, care furnizează un serviciu care îndeplineşte condiţiile prevăzute la art. 6 alin. (1);

i) *piaţă online* – serviciu digital care permite consumatorilor şi/sau comercianţilor, astfel cum sunt definiţi la art. 3 alin. (1) lit. a) şi b) din

Ordonanţa Guvernului nr. 38/2015 privind soluţionarea alternativă a litigiilor dintre consumatori şi comercianţi, cu modificările ulterioare, să încheie cu comercianţii vânzări online sau contracte de servicii, fie pe site-ul internet al pieţei online, fie pe site-ul internet al unui comerciant care utilizează servicii informatice furnizate de piaţa online;

j) *registru de nume de domenii Top-level* – entitate care administrează şi operează înregistrarea de nume de domenii de internet într-un domeniu Top-level (TLD) specific;

k) *reprezentant* – orice persoană fizică sau juridică stabilită în Uniunea Europeană desemnată explicit să acţioneze în numele unui furnizor de servicii digitale nestabilit în Uniunea Europeană, căreia i se poate adresa autoritatea competentă la nivel naţional sau echipa de răspuns la incidente de securitate informatică, denumită în continuare *echipă CSIRT* sau *CSIRT*, în locul furnizorului de servicii digitale în ceea ce priveşte obligaţiile furnizorului de servicii digitale în temeiul prezentei legi;

l) *reţea şi sistem informatic*:

1. reţea de comunicaţii electronice în sensul prevederilor art. 4 alin. (1) pct. 6 din Ordonanţa de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, aprobată cu modificări şi completări prin Legea nr. 140/2012, cu modificările şi completările ulterioare;

2. orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor cu ajutorul unui program informatic;

3. datele digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la pct. 1 şi 2 în vederea funcţionării, utilizării, protejării şi întreţinerii lor;

m) *risc* – orice circumstanţă sau eveniment ce poate fi identificat în mod rezonabil, anterior producerii sale, care are un efect potenţial negativ asupra securităţii reţelelor şi a sistemelor informatice;

n) *securitatea reţelelor şi a sistemelor informatice* – capacitatea unei reţele şi a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acţiuni care compromite disponibilitatea, autenticitatea, integritatea, confidenţialitatea sau nonrepudierea datelor stocate ori transmise sau prelucrate ori a serviciilor conexe oferite de reţeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

o) *serviciu digital* – serviciu, în sensul prevederilor art. 4 alin. (1) pct. 2 din Hotărârea Guvernului nr. 1016/2004 privind măsurile pentru organizarea şi realizarea schimbului de informaţii în domeniul standardelor şi reglementărilor tehnice, precum şi al regulilor referitoare la serviciile societăţii informaţionale între România şi statele membre ale Uniunii Europene, precum şi Comisia Europeană, cu modificările şi completările ulterioare, şi care se încadrează într-una din categoriile:

1. piaţă online;
2. motor de căutare online;
3. serviciu de cloud computing;

p) *specificaţie* – specificaţie tehnică, în sensul prevederilor art. 2 pct. 4 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European şi al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE şi 93/15/CEE ale Consiliului şi a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE şi 2009/105/CE ale Parlamentului European şi ale Consiliului şi de abrogare a Deciziei 87/95/CEE a Consiliului şi a Deciziei nr.1673/2006/CE a Parlamentului European şi a Consiliului;

q) *standard* – standard, în sensul prevederilor art. 2 pct. 1 din Regulamentul (UE) nr. 1025/2012;

r) *strategie naţională privind securitatea reţelelor şi a sistemelor informatice* – cadru care furnizează obiective şi priorităţi strategice privind securitatea reţelelor şi a sistemelor informatice la nivel naţional;

s) *serviciu de cloud computing* – serviciu digital care permite accesul la un sistem configurabil de resurse sau servicii informatice care pot fi puse în comun;

ş) *valoare de prag* – valoare minimă/maximă, cuantificabilă a indicatorilor în baza cărora se determină gradul de îndeplinire a unui criteriu.

Art. 4. – Principiile care stau la baza prezentei legi:

a) *principiul responsabilităţii şi conştientizării* – constă în efortul continuu derulat de entităţile de drept public şi privat în conştientizarea rolului şi responsabilităţii individuale pentru atingerea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice;

b) *principiul proporţionalităţii* – constă în asigurarea unui echilibru între riscurile la care reţelele şi sistemele informatice sunt supuse şi cerinţele de securitate implementate;

c) *principiul cooperării şi coordonării* – constă în realizarea în timp oportun a schimbului de informaţii referitoare la riscurile de securitate la adresa reţelelor şi sistemelor informatice şi asigurarea într-o manieră sincronizată a reacţiei la producerea incidentelor.

CAPITOLUL II
Domeniul de aplicare

SECŢIUNEA 1
Operatorii de servicii esenţiale

Art. 5. – În vederea asigurării unui nivel ridicat de securitate, operatorii de servicii esenţiale se identifică şi se înscriu în Registrul operatorilor de servicii esenţiale.

Art. 6. – (1) Un serviciu este considerat esenţial dacă furnizarea lui îndeplineşte cumulativ următoarele condiţii:

a) serviciul este esenţial în susţinerea unor activităţi societale şi/sau economice de cea mai mare importanţă;

b) furnizarea sa depinde de o reţea sau de un sistem informatic;

c) furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident.

(2) Evaluarea gradului de perturbare a furnizării serviciului esenţial se realizează în funcţie de următoarele criterii intersectoriale, fără a fi cumulative:

a) numărul de utilizatori care se bazează pe serviciul furnizat de entitatea în cauză;

b) dependenţa altor sectoare prevăzute în anexa la prezenta lege de serviciul furnizat de entitatea în cauză;

c) impactul pe care l-ar putea avea incidentele, în ceea ce priveşte intensitatea şi durata, asupra activităţilor economice şi societale sau asupra siguranţei publice;

d) cota de piaţă a entităţii în cauză;

e) distribuţia geografică în ceea ce priveşte zona care ar putea fi afectată de un incident;

f) importanţa entităţii pentru menţinerea unui nivel suficient al serviciului, ţinând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv.

(3) Ministerul Comunicaţiilor şi Societăţii Informaţionale denumit în continuare *MCSI*, la propunerea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică denumit în continuare *CERT-RO*, supune aprobării prin hotărâre a Guvernului în termen de 5 luni de la data intrării în vigoare a prezentei legi:

a) valorile de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale;

b) valorile de prag corespunzătoare criteriilor intersectoriale stabilite potrivit dispoziţiilor alin. (2);

c) criteriile sectoriale specifice şi valorile de prag corespunzătoare fiecărui sector şi subsector de activitate prevăzut în anexă;

d) normele tehnice de stabilire a impactului incidentelor.

(4) La nivelul MCSI, se înfiinţează şi funcţionează Grupul de lucru interinstituţional pentru determinarea valorilor de prag necesare pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale, prevăzute la alin. (3).

(5) MCSI, la propunerea CERT-RO, în termen de 3 luni de la data intrării în vigoare a prezentei legi, supune aprobării prin hotărâre a Guvernului componenţa, atribuţiile şi modul de organizare a Grupului de lucru interinstituţional prevăzute la alin. (4).

(6) Determinarea valorilor de prag necesare pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul operatorilor de servicii esenţiale care furnizează servicii din sectorul prevăzut la pct. 7 din anexă, se realizează cu consultarea Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii.

Art. 7. – (1) Registrul prevăzut la art. 5 se alcătuieşte pentru sectoarele şi subsectoarele prevăzute în anexă şi raportat la criteriile prevăzute la art.6 şi valorile de prag prevăzute la art. 6 alin. (3).

(2) Registrul prevăzut la alin. (1) se înființează, se întreține și se actualizează periodic, cel puțin o dată la doi ani de la data intrării în vigoare a prezentei legi de către CERT-RO în calitate de autoritate competentă la nivel național.

(3) Registrul prevăzut la alin. (1) face parte din categoria documentelor clasificate.

(4) Normele metodologice de organizare şi funcţionare a registrului prevăzut la art. 5 se aprobă, la propunerea directorului general al CERT-RO, prin ordin al ministrului comunicaţiilor şi societăţii informaţionale, care se publică în Monitorul Oficial al României, Partea I.

Art. 8. – (1) Entităţile care îndeplinesc condiţiile şi criteriile prevăzute la art. 6 şi activează într-unul sau mai multe dintre sectoarele sau subsectoarele de activitate prevăzute în anexă, au obligaţia să notifice CERT-RO în vederea înscrierii în Registrul operatorilor de servicii esenţiale.

(2) Prin excepţie de la alin. (1) identificarea în vederea înscrierii în Registrul operatorilor de servicii esenţiale se poate face şi de către CERT-RO din oficiu în vederea îndeplinirii obligaţiilor legale ce îi revin sau în urma unei sesizări privind sustragerea de la obligaţia de notificare şi înscriere în Registrul operatorilor de servicii esenţiale făcută de către orice persoană

interesată, aducând la cunoştinţa entităţii vizate declanşarea procedurii de identificare şi comunicând la final operatorului rezultatul acesteia.

(3) Operatorii de servicii esenţiale pot solicita asistenţa CERT-RO în procesul de identificare.

(4) Înscrierea operatorilor de servicii esenţiale în Registrul operatorilor de servicii esenţiale se realizează prin decizia directorului general al CERT-RO care se comunică operatorului de servicii esenţiale în urma depunerii unui raport de audit care atestă îndeplinirea cerinţelor minime de securitate şi notificare, întocmit de un auditor atestat în conformitate cu prevederile art. 32 şi a evaluării informaţiilor şi documentaţiilor furnizate de operator în cadrul procesului de identificare.

(5) Atunci când o entitate furnizează un serviciu dintre cele reglementate la art. 6 alin. (1) lit. a) şi în cadrul altor state membre ale Uniunii Europene, CERT-RO se consultă cu autorităţile omologe din statele respective în procesul de identificare înainte de adoptarea unei decizii privind identificarea operatorului.

(6) Notificarea prevăzută la alin. (1) se realizează în termen de 30 de zile de la data îndeplinirii condiţiilor prevăzute la art. 6 alin. (1) prin raportare la criteriile intersectoriale de stabilire a impactului unui incident prevăzute la art. 6 alin. (2), respectiv la criteriile sectoriale, precum şi la valorile de prag prevăzute la art. 6 alin. (3) prin depunerea unei declaraţii pe propria răspundere.

(7) Operatorii economici şi celelalte entităţi care operează ori furnizează servicii în cadrul sectoarelor şi subsectoarelor definite în anexă au obligaţia de a pune la dispoziţia CERT-RO, la cererea acesteia în calitate de autoritate competentă la nivel naţional, în termen de 60 de zile de la data primirii solicitării, documentaţiile necesare, inclusiv rapoarte de audit, pentru:

a) stabilirea calităţii de operator de servicii esenţiale în conformitate cu prevederile art. 6 şi 7;

b) stabilirea măsurilor necesare pentru conformarea cu cerinţele prezentei legi;

c) stabilirea interdependenţei şi interconectării reţelelor şi sistemelor informatice cu cele ale altor operatori de servicii esenţiale ori furnizori de servicii digitale, inclusiv a celor pe care se bazează furnizarea serviciilor entităţii în cauză;

d) stabilirea listei de autorităţi ale statului pentru care furnizează serviciile definite la art. 6 alin. (1).

(8) Prin excepţie de la termenul general de furnizare a documentaţiilor stabilit la alin. (7), termenul de realizare a auditurilor şi de depunere a rapoartelor de audit prevăzute la alin. (4) şi (7), precum şi tematica şi obiectivele acestora se stabilesc de către CERT-RO în urma

evaluării celorlalte informaţii furnizate în conformitate cu prevederile alin. (7) şi curge de la data primirii comunicării termenului de către entitatea vizată.

(9) Documentaţia prevăzută la alin. (7) şi (8) va fi stabilită prin normele metodologice de identificare a operatorilor de servicii esenţiale şi furnizorilor de servicii digitale, aprobate la propunerea directorului general al CERT-RO, prin ordin al ministrului comunicaţiilor şi societăţii informaţionale, care se publică în Monitorul Oficial al României, Partea I.

Art. 9. – (1) Entităţile care nu mai îndeplinesc condiţiile şi criteriile prevăzute la art. 6 notifică CERT-RO în vederea radierii din Registrul operatorilor de servicii esenţiale şi furnizează documentaţiile relevante în conformitate cu art. 8 alin. (7) lit. a).

(2) CERT-RO dispune prin decizia directorului general radierea din Registrul operatorilor de servicii esenţiale la cerere sau din oficiu, în urma evaluării documentaţiilor prevăzute la alin. (1) şi comunică operatorului decizia.

(3) Operatorii de servicii esenţiale pot solicita asistenţa CERT-RO cu privire la documentaţiile prevăzute la alin. (1) necesare în procesul de radiere.

(4) Atunci când o entitate furnizează un serviciu esenţial şi în cadrul altor state membre ale Uniunii Europene, CERT-RO se consultă cu autorităţile omologe din statele respective înainte de adoptarea unei decizii privind radierea.

(5) Notificarea prevăzută la alin. (1) se realizează în termen de 30 de zile de la data la care entitatea nu mai îndeplineşte condiţiile prevăzute la art. 6.

Art. 10. – (1) În scopul asigurării securităţii reţelelor şi sistemelor informatice, operatorii de servicii esenţiale au următoarele obligaţii:

a) implementează măsurile tehnice şi organizatorice adecvate şi proporţionale pentru îndeplinirea cerinţelor minime de securitate stabilite în temeiul prevederilor art. 25 alin. (3);

b) implementează măsuri adecvate pentru a preveni şi minimiza impactul incidentelor care afectează securitatea reţelelor şi a sistemelor informatice utilizate pentru furnizarea acestor servicii esenţiale, cu scopul de a asigura continuitatea serviciilor respective, stabilite în temeiul prevederilor art. 25 alin. (3);

c) notifică de îndată CERT-RO în calitate de CSIRT naţional incidentele care au un impact semnificativ asupra continuităţii serviciilor esenţiale furnizând cel puţin informaţiile prevăzute la art. 26 alin. (3);

d) pun la dispoziţia CERT-RO informaţii care să permită stabilirea impactului transfrontalier al incidentului în conformitate cu prevederile art. 26 alin. (3);

e) se supun controlului desfăşurat de către CERT-RO în vederea stabilirii gradului de respectare a obligaţiilor ce le revin în temeiul prezentei legi;

f) stabilesc mijloacele permanente de contact, desemnează responsabilii cu securitatea reţelelor şi sistemelor informatice însărcinaţi cu monitorizarea mijloacelor de contact şi comunică CERT-RO în termen de 60 de zile de la înscrierea în Registrul operatorilor de servicii esenţiale lista acestora, precum şi orice modificări ulterioare de îndată ce au survenit;

g) comunică în termen de maximum 30 de zile către CERT-RO, în calitate de autoritate competentă la nivel naţional, orice schimbare survenită în datele furnizate în cadrul procesului de identificare ca operator de servicii esenţiale;

h) se interconectează în termen de 60 de zile de la înscrierea în Registrul operatorilor de servicii esenţiale la serviciul de alertare şi cooperare al CERT-RO, asigură monitorizarea permanentă a alertelor şi solicitărilor primite prin acest serviciu ori prin celelalte modalităţi de contact şi ia în cel mai scurt timp măsurile adecvate de răspuns la nivelul reţelelor şi sistemelor informatice proprii;

i) asigură de îndată răspunsul la incidentele survenite, restabilesc în cel mai scurt timp funcţionarea serviciului la parametrii dinaintea incidentului şi realizează auditul de securitate, conform prezentei legi.

(2) Operatorii de servicii esenţiale pun la dispoziţia CERT-RO în calitate de autoritate competentă la nivel naţional, la solicitarea acesteia făcută cu menţionarea scopului şi precizând informaţiile necesare şi termenul de furnizare a acestora:

a) informaţiile necesare pentru evaluarea securităţii reţelelor şi a sistemelor informatice vizate de prezenta lege, inclusiv politicile de securitate documentate;

b) rezultatele auditului de securitate realizat la solicitarea CERT-RO, inclusiv informaţiile şi documentaţiile pe care se bazează acesta, precum şi alte elemente care atestă punerea efectivă în aplicare a cerinţelor minime de securitate.

(3) Notificarea de îndată a afectării serviciilor esenţiale prevăzută la alin. (1) lit. c) se face şi în situaţia în care afectarea se datorează unor incidente care afectează un furnizor de servicii digitale de care depinde furnizarea serviciilor esenţiale.

(4) Termenul de conformare pentru îndeplinirea obligaţiilor prevăzute la alin. (1) lit. a) şi b) este de 6 luni de la data intrării în vigoare a normelor tehnice privind cerinţele de securitate şi notificare ori, după caz, de la data înscrierii în Registrul operatorilor de servicii esenţiale.

Art. 11. – Operatorii de servicii esenţiale au obligaţia să implementeze în termenul de conformare stabilit în conformitate cu dispoziţiile art.37, măsurile dispuse de CERT-RO pentru îndeplinirea cerinţelor minime de securitate, în vederea remedierii deficienţelor constatate cu ocazia controlului exercitat în temeiul art. 35.

SECŢIUNEA a 2-a
Furnizorii de servicii digitale

Art. 12. – (1) Furnizorii de servicii digitale au următoarele obligaţii:

a) implementează măsurile tehnice şi organizatorice adecvate şi proporţionale pentru îndeplinirea cerinţelor minime de securitate a reţelelor şi sistemelor informatice stabilite în temeiul prevederilor prezentei legi cu privire la serviciile prevăzute la art. 3 lit. o) pe care le oferă pe teritoriul Uniunii Europene ţinând cont de normele tehnice prevăzute la art.25 alin. (1), în termen de 6 luni de la data intrării în vigoare a acestora;

b) implementează, în termen de 6 luni de la data intrării în vigoare a normelor tehnice prevăzute la art. 25 alin. (1) măsuri adecvate pentru a preveni şi minimiza impactul incidentelor care afectează securitatea reţelelor şi a sistemelor informatice utilizate pentru furnizarea serviciilor prevăzute la lit.a), asigură răspunsul la incidente şi continuitatea serviciilor acestora;

c) notifică de îndată CERT-RO în calitate de CSIRT naţional incidentele care au un impact semnificativ asupra furnizării serviciilor prevăzute la art. 3 lit. o) furnizând cel puţin informaţiile prevăzute la art. 26 alin. (3);

d) pun la dispoziţia CERT-RO informaţii care să permită stabilirea impactului transfrontalier al incidentului în conformitate cu prevederile art. 26 alin. (3);

e) stabilesc mijloace permanente de contact, desemnează responsabilii cu securitatea reţelelor şi sistemelor informatice însărcinaţi cu monitorizarea canalelor de contact şi comunică CERT-RO în termen de 60 de zile de la data intrării în vigoare a prezentei legi, lista acestora precum şi orice modificări ulterioare de îndată ce au survenit;

f) se interconectează în termen de 60 de zile de la data intrării în vigoare a prezentei legi la serviciul de alertare şi cooperare al CERT-RO, asigură monitorizarea permanentă a alertelor şi solicitărilor primite prin acest serviciu ori prin celelalte modalităţi de contact şi ia în cel mai scurt timp măsurile adecvate de răspuns la nivelul reţelelor şi sistemelor informatice proprii.

(2) Furnizorii de servicii digitale pun la dispoziţia CERT-RO în calitate de autoritate competentă la nivel naţional, la solicitarea acesteia făcută cu menţionarea scopului şi precizând informaţiile necesare şi termenul de furnizare a acestora:

a) informaţiile necesare pentru evaluarea securităţii reţelelor şi a sistemelor informatice vizate de prezenta lege, inclusiv politicile de securitate documentate;

b) rezultatele auditului de securitate realizat, inclusiv informațiile și documentațiile pe care se bazează acesta, precum și alte elemente care atestă punerea efectivă în aplicare a cerințelor minime de securitate.

(3) Obligaţia de notificare prevăzută la alin. (1) lit. c) se aplică doar în cazul în care furnizorul de servicii digitale are acces la informaţiile necesare pentru evaluarea impactului incidentului prevăzute la art. 26 şi care să permită evaluarea prevăzută la art. 28.

(4) Prevederile prezentei legi se aplică furnizorilor de servicii digitale care au stabilit sediul social pe teritoriul României, precum şi celor din afara Uniunii Europene care stabilesc sediul reprezentanţei din Uniune pe teritoriul României.

(5) Prevederile alin. (1) – (4), art. 25 alin. (4), art. 26 alin. (2) din prezenta lege nu se aplică furnizorilor de servicii digitale care se încadrează în categoria întreprinderilor mici şi mijlocii, aşa cum sunt definite în Legea nr. 346/2004 privind stimularea înfiinţării şi dezvoltării întreprinderilor mici şi mijlocii, cu modificările şi completările ulterioare.

(6) Operatorii economici, precum şi celelalte entităţi care furnizează servicii digitale, au obligaţia de a furniza către CERT-RO, în termen de 60 de zile de la data primirii solicitării făcută cu menţionarea scopului şi precizând informaţiile necesare următoarele categorii de documente:

a) documentaţiile necesare stabilirii calităţii de furnizor de servicii digitale în sensul prezentei legi;

b) documentaţiile necesare stabilirii interdependenţei şi interconectării reţelelor şi sistemelor informatice cu cele ale altor operatori de servicii esenţiale ori furnizori de servicii digitale;

c) stabilirea listei de autorităţi ale statului pentru care furnizează serviciile definite la art. 3 lit. o).

(7) Documentaţia prevăzută la alin. (6) va fi stabilită prin normele metodologice prevăzute la art. 8 alin. (9).

CAPITOLUL III
Roluri și responsabilităţi

SECŢIUNEA 1
Coordonarea strategică la nivel naţional

Art. 13. – Coordonarea strategică, la nivel naţional a activităţilor de asigurare a unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice se realizează de către Guvern prin Ministerul Comunicaţiilor şi

Societăţii Informaţionale sub aspectul politicilor publice şi al iniţiativei legislative în domeniu.

Art. 14. – Strategia naţională privind securitatea reţelelor şi a sistemelor informatice se aprobă prin hotărâre a Guvernului, la propunerea MCSI în termen de 6 luni de la data intrării în vigoare a prezentei legi.

SECŢIUNEA a 2-a
Autorităţi competente şi responsabilităţi

Art. 15. – (1) CERT-RO este autoritate competentă la nivel naţional pentru securitatea reţelelor şi a sistemelor informatice care asigură furnizarea serviciilor esenţiale ori furnizează serviciile digitale identificate în temeiul prezentei legi.

(2) Pentru asigurarea unui nivel ridicat de securitate a reţelelor şi sistemelor informatice, CERT-RO se consultă şi cooperează cu:

a) Serviciul Român de Informaţii, pentru securitatea reţelelor şi a sistemelor informatice care asigură servicii esenţiale a căror afectare aduce atingere securităţii naţionale;

b) Ministerul Apărării Naţionale, pentru securitatea reţelelor şi a sistemelor informatice care asigură servicii esenţiale în sprijinul activităţilor privind apărarea naţională;

c) Ministerul Afacerilor Interne, Oficiul Registrului Naţional al Informaţiilor Secrete de Stat, Serviciul de Informaţii Externe, Serviciul de Telecomunicaţii Speciale şi Serviciul de Protecţie şi Pază, pentru securitatea reţelelor şi a sistemelor informatice care asigură servicii esenţiale în domeniul lor de activitate şi responsabilitate.

Art. 16. – CERT-RO se consultă şi cooperează, după caz, cu:

a) organele de urmărire penală;

b) Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, atunci când incidentele au ca rezultat afectarea securităţii ori funcţionării reţelelor publice de comunicaţii electronice, ori când pentru administrarea unui incident sunt necesare măsuri ce intră în aria de activitate şi responsabilitate a acesteia;

c) Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal în cazul incidentelor care au ca rezultat încălcarea securităţii datelor cu caracter personal, în condiţiile legii.

SECȚIUNEA a 3-a

Echipele de intervenție în caz de incidente de securitate informatică

Art. 17. – (1) Echipa *CSIRT* definită la art. 19 lit. b) respectă cerințele de la art. 24 și acoperă sectoarele din anexa și serviciile prevăzute la art. 3 lit. o).

(2) Persoanele juridice care activează în cadrul aceluiași sector sau subsector de activitate din anexa la prezenta lege pot constitui echipe CSIRT proprii sau sectoriale ori pot achiziționa servicii de specialitate de tip CSIRT.

(3) Entitățile prevăzute la art. 15 alin. (2) și art. 16 lit. b) pot constitui echipe CSIRT pentru asigurarea securității rețelelor și sistemelor informatice conform domeniului de activitate și responsabilitate.

(4) Echipele CSIRT sectoriale se autorizează și se desemnează de către CERT-RO în urma evaluării îndeplinirii condițiilor specifice de autorizare a acestui tip de echipe elaborate în conformitate cu prevederile art. 20 lit e).

Art. 18. – (1) Echipele CSIRT proprii, sectoriale sau serviciile de specialitate prevăzute la art.17 alin. (2) care deservesc operatori de servicii esențiale și furnizori de servicii digitale au următoarele obligații:

a) să fie autorizate de către CERT-RO în temeiul prezentei legi;

b) să asigure compatibilitatea și interoperabilitatea sistemelor, procedurilor și metodelor utilizate cu cele ale echipei CSIRT naționale din cadrul CERT-RO;

c) să furnizeze cel puțin setul minim de servicii de tip CSIRT necesar asigurării la nivel național a unei protecții unitare a operatorilor și furnizorilor ce fac obiectul prezentei legi;

d) să utilizeze în cadrul echipelor un număr corespunzător de persoane calificate în conformitate cu prezenta lege;

e) să se interconecteze la serviciul de alertă, monitorizare și cooperare al CERT-RO și să asigure un răspuns prompt la alertele și solicitările transmise de echipa CSIRT națională.

(2) Normele tehnice privind compatibilitatea și interoperabilitatea prevăzute la alin.(1) lit.b), setul minim de servicii menționat la alin. (1) lit. c) și criteriile de stabilire a numărului de persoane calificate prevăzute la alin. (1) lit. d) se aprobă, la propunerea directorului general al CERT-RO, prin ordin al ministrului comunicațiilor și societății informaționale, care se publică în Monitorul Oficial al României, Partea I.

SECŢIUNEA a 4-a
Autoritatea competentă la nivel naţional – CERT-RO

Art. 19. – În cadrul CERT-RO se organizează şi funcţionează şi:

a) Punctul unic de contact la nivel naţional;

b) Echipa de răspuns la incidente de securitate informatică la nivel naţional, denumită în continuare *echipa CSIRT naţională* sau *CSIRT naţional.*

Art. 20. – CERT-RO în calitate de autoritate competentă la nivel naţional are următoarele atribuţii generale:

a) identifică, cu consultarea autorităţilor şi entităţilor de reglementare şi administrare a sectoarelor şi subsectoarelor prevăzute în anexă, operatorii de servicii esenţiale care au sediul social, filială, sucursală sau punct de lucru pe teritoriul României;

b) elaborează şi actualizează normele tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice;

c) elaborează şi actualizează normele tehnice privind îndeplinirea obligaţiilor de notificare a incidentelor de securitate de către operatorii şi furnizorii prevăzuţi de prezenta lege;

d) coordonează activitatea Grupului de lucru interinstituţional menţionat la art. 6 alin. (4);

e) elaborează și actualizează, după consultarea celorlalte instituții cu responsabilități în domeniul apărării, ordinii publice și securității naționale, precum și a altor instituții și autorități, după caz, normele metodologice, tehnice, precum și regulamentele privind cerințele referitoare la înființarea, autorizarea și funcționarea echipelor CSIRT, desemnarea echipelor CSIRT sectoriale, cele referitoare la atestarea auditorilor calificați cu competențe în domeniul securității serviciilor esențiale și a serviciilor digitale, precum și normele referitoare la autorizarea formatorilor și furnizorilor de servicii de formare pentru activitățile prevăzute la literele o) și p);

f) elaborează şi promovează practici comune pentru administrarea incidentelor şi a riscurilor şi pentru sistemele de clasificare a incidentelor, riscurilor şi informaţiilor;

g) participă, prin reprezentanți, la Grupul de cooperare la nivelul Uniunii Europene constituit pentru a facilita cooperarea strategică și schimbul de informații între statele membre, pentru a consolida încrederea și în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană și compus din reprezentanți ai statelor membre, ai Comisiei Europene și ai Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor – ENISA, în vederea adoptării

soluțiilor optime pentru atingerea obiectivului de securitate și a schimbului de informații între statele membre respectiv:

i. după caz, participă la schimbul de experienţă privind aspecte legate de securitatea reţelelor şi a sistemelor informatice cu instituţii, organe, oficii şi agenţii relevante ale Uniunii Europene;

ii. participă la dezbateri privind standardele şi specificaţiile prevăzute la art.25 alin.(6) cu reprezentanţi ai organizaţiilor de standardizare europene relevante;

iii. colectează exemple de bune practici privind riscurile și incidentele;

h) permite echipelor CSIRT, acces la datele privind incidentele notificate de operatorii de servicii esenţiale sau de furnizorii de servicii digitale, în măsura necesară pentru a-şi îndeplini atribuţiile, cu respectarea legii;

i) verifică în condiţiile art. 35 – 42 respectarea de către operatorii de servicii esenţiale şi furnizorii de servicii digitale a obligaţiilor ce le revin conform prezentei legi;

j) emite în temeiul art. 37 dispoziţii cu caracter obligatoriu pentru operatorii de servicii esenţiale în vederea conformării și remedierii deficiențelor constatate și stabileşte termenul până la care aceştia trebuie să se conformeze;

k) instituie măsuri de supraveghere ex post pentru furnizorii de servicii digitale cu privire la neîndeplinirea obligaţiilor ce le revin conform prevederilor prezentei legi;

l) primeşte sesizări cu privire la neîndeplinirea obligaţiilor operatorilor şi furnizorilor prevăzuţi de prezenta lege;

m) cooperează cu autorităţile competente din celelalte state şi oferă asistenţă acestora, prin schimbul de informaţii, transmiterea de solicitări şi sesizări, efectuarea controlului ori luarea de măsuri de supraveghere şi remediere a deficienţelor constatate, în cazul operatorilor şi furnizorilor prevăzuţi de prezenta lege care îşi au sediul principal în România ori care, deşi au sediul principal stabilit în alt stat membru, reţelele sau sistemele informatice acestora sunt situate şi pe teritoriul României;

n) monitorizează aplicarea prevederilor prezentei legi;

o) autorizează, revocă sau reînnoieşte autorizarea echipelor CSIRT ce deservesc operatori de servicii esenţiale ori furnizori de servicii digitale;

p) eliberează, revocă sau reînnoieşte atestatele auditorilor de securitate informatică care pot efectua audit în cadrul reţelelor şi sistemelor informatice ce susţin servicii esenţiale ori furnizează servicii digitale în condiţiile prezentei legi;

q) autorizează, revocă sau reînnoieşte autorizarea formatorilor şi furnizorilor de servicii de formare pentru activităţile prevăzute la lit.o) şi p);

r) alcătuiește și actualizează periodic, cel puțin o dată la doi ani, începând cu data intrării în vigoare a prezentei legi, lista serviciilor esențiale care îndeplinesc condițiile de la art. 6 alin. (1) cu consultarea autorităților și entităților prevăzute la lit. a), precum și a celor prevăzute la art. 15 alin. (2) și o înaintează MCSI spre a fi supusă aprobării, prin hotărâre a Guvernului. Prima listă se supune aprobării Guvernului în termen de 6 luni de la data intrării în vigoare a prezentei legi;

s) propune spre aprobare MCSI normele tehnice, metodologice și regulamentele prevăzute de prezenta lege, în termen de 6 luni de la data intrării în vigoare a acesteia.

Art. 21. – În calitate de Punct național unic de contact, CERT-RO are următoarele atribuții:

a) exercită o funcție de legătură între autoritățile statului și autoritățile similare din alte state, Grupul de cooperare și rețeaua echipelor de răspuns la incidentele de securitate informatică, denumită în continuare *rețeaua CSIRT*;

b) elaborează și transmite Grupului de cooperare rapoarte de sinteză privind notificările primite și acțiunile întreprinse;

c) transmite la cererea autorităților sau a echipelor CSIRT, către punctele unice de contact din celelalte state membre, notificările și solicitările privind incidentele ce afectează funcționarea serviciilor esențiale și a celor digitale de pe teritoriul respectivelor state;

d) transmite autorităților prevăzute la art. 15 alin. (2) și art. 16 notificările și cererile primite din alte state membre, potrivit ariei de responsabilitate.

Art. 22. – (1) În calitate de CSIRT național, CERT-RO are următoarele atribuții:

a) monitorizează incidentele de securitate a rețelelor și sistemelor informatice la nivel național;

b) emite avertizări timpurii, alerte și anunțuri și diseminează informațiile privind riscurile și incidentele către autoritățile prevăzute la art. 15 alin. (2), precum și orice entitate de drept public sau privat căreia îi poate fi afectată securitatea rețelelor și sistemelor informatice;

c) primește notificări privind incidentele care afectează rețelele și sistemele operatorilor de servicii esențiale ori ale furnizorilor de servicii digitale;

d) furnizează operatorului de servicii esențiale care a făcut notificarea, în măsura posibilităților, informații relevante în ceea ce privește acțiunile ulterioare notificării;

e) stabileşte, în baza notificărilor primite, impactul la nivel naţional şi transfrontalier al incidentelor şi informează autorităţile relevante la nivel naţional precum şi autorităţile similare din alte state potenţial afectate;

f) aduce la cunoştinţa publicului periodic şi ori de câte ori este necesar avertizări, alerte şi informări privind riscuri şi ameninţări, posibile măsuri de prevenire şi contracarare în scopul cunoaşterii de către public a acestora şi al luării măsurilor adecvate şi publică statistici privitoare la incidentele identificate la nivel naţional, cu respectarea condiţiilor prezentei legi;

g) asigură răspunsul la incidente în limitele prezentei legi;

h) elaborează analize dinamice de risc şi de incident;

i) cooperează, la nivel naţional, cu echipele CSIRT în cadrul unei platforme de management al incidentelor şi pentru schimbul de informaţii;

j) participă la acţiunile comune în cadrul reţelei CSIRT la nivel european, precum şi, după necesităţi, la acţiunile solicitate în cadrul reţelelor internaţionale de cooperare;

k) poate solicita asistenţa ENISA pentru aducerea la îndeplinire a atribuţiilor sale;

l) înfiinţează, întreţine şi operează serviciul de alertare şi cooperare cu operatorii de servicii esenţiale şi furnizorii de servicii digitale menţionat la art. 10 alin. (1) lit. h) şi art. 12 alin. (1) lit. f).

(2) Echipele CSIRT se conectează şi realizează schimbul de informaţii cu echipa CSIRT naţională aflată în cadrul CERT-RO prin intermediul platformei de management al incidentelor, menţionată la alin. (1) lit. i).

(3) În vederea administrării adecvate a incidentelor majore la nivel naţional ori pentru administrarea unor incidente care necesită înaltă specializare şi pregătire tehnică de specialitate, CERT-RO poate dezvolta parteneriate şi alcătui echipe mixte compuse din specialiştii proprii şi specialişti proveniţi de la alte instituţii ori entităţi din mediul privat, cu respectarea legii şi asigurarea condiţiilor privind confidenţialitatea şi accesul la informaţii în limitele legii şi cu acordul părţilor implicate în incident.

Art. 23. – (1) În scopul cooperării operaţionale, Echipa CSIRT naţională care funcţionează în cadrul CERT-RO participă la Reţeaua CSIRT compusă din reprezentanţi ai echipelor CSIRT naţionale ale statelor membre din Uniunea Europeană şi cea a CERT-UE.

(2) Cooperarea prevăzută la alin. (1) se realizează prin:

a) schimbul de informaţii privind serviciile, operaţiunile şi posibilităţile de cooperare;

b) schimbul şi analiza informaţiilor fără caracter comercial referitoare la incidentele ce afectează un stat membru;

c) schimbul de informaţii fără caracter confidenţial privind incidente individuale;

d) participarea la elaborarea unui răspuns coordonat al Rețelei CSIRT, pentru managementul unui incident identificat pe teritoriul unui alt stat membru;

e) acordarea de sprijin voluntar în abordarea incidentelor transfrontaliere;

f) analiza şi identificarea de noi forme de cooperare operaţională în cadrul Reţelei CSIRT;

g) participarea la elaborarea de orientări şi practici unitare în domeniul cooperării operaţionale;

h) solicitarea Reţelei CSIRT de a asigura un răspuns coordonat la un incident identificat la nivel naţional.

(3) Fac excepţie de la schimbul de informaţii prevăzut la alin. (2) lit. c) situaţiile în care schimbul ar periclita investigarea incidentului.

(4) Echipa CSIRT participă şi la alte reţele internaţionale de cooperare, după necesităţi.

Art. 24. – (1) În vederea îndeplinirii atribuţiilor ce îi revin în calitate de autoritate competentă la nivel naţional în temeiul art. 20, din bugetul CERT-RO se asigură resursele materiale, financiare şi umane suficiente pentru:

a) desfăşurarea activităţilor de normare prevăzute la art. 20 lit. a) – f) şi r);

b) primirea sesizărilor, efectuarea controlului, verificărilor şi supravegherilor prevăzute la art. 20 lit. i) – l), precum şi pentru asigurarea punerii în aplicare a deciziilor şi sancţiunilor, rezolvării contestaţiilor şi reprezentarea în contencios administrativ;

c) desfășurarea activităților de cooperare prevăzute la art. 20 lit. g), h) și m), înființarea, administrarea și funcționarea registrelor și evidențelor prevăzute de art. 20 lit. o) – r), precum și a registrului operatorilor de servicii esențiale prevăzut la art. 5;

d) desfășurarea activităților de autorizare și acreditare prevăzute la art. 20 lit. o) – q);

e) luarea măsurilor cu caracter excepţional prevăzute la art. 41.

(2) În vederea îndeplinirii atribuţiilor ce îi revin în calitate de Punct unic de contact la nivel naţional, din bugetul CERT-RO se asigură resursele materiale, financiare şi umane suficiente pentru asigurarea în regim permanent a funcţiei de legătură, primire şi retransmitere a cererilor şi solicitărilor prevăzute la art. 21 lit. a), c) şi d).

(3) În vederea îndeplinirii atribuţiilor ce îi revin în calitate de echipă CSIRT naţională conform prevederilor art. 22 şi 23, din bugetul CERT-RO se asigură resursele materiale, financiare şi umane suficiente pentru:

a) alertele prevăzute la art. 22 alin. (1) lit. a) şi c);

b) emiterea avertizărilor, contactarea şi alertarea altor entităţi şi diseminarea de informaţii relevante în temeiul art. 22 alin. (1) lit. b), d) – f) şi l);

c) asigurarea răspunsului, intervenţiei şi cooperării în temeiul art. 22 alin. (1) lit. g), i) – l);

d) stabilirea impactului incidentelor şi analiza acestora în temeiul art. 22 alin. (1) lit. e) şi h).

(4) Resursele financiare, materiale şi umane alocate CERT-RO vor asigura:

a) continuitatea activităţilor şi disponibilitatea permanentă a serviciilor;

b) participarea la Grupul de cooperare prevăzut de art. 20 lit. g);

c) un sistem adecvat de gestionare şi transmitere a cererilor;

d) o infrastructură adecvată prevăzută cu sisteme redundante;

e) spaţiu de lucru de rezervă în amplasamente securizate;

f) disponibilitatea ridicată a serviciilor de comunicaţii prin mijloace multiple de contact, capacitatea de a contacta alte entităţi în orice moment şi evitarea punctelor unice de defecţiune;

g) amplasamente securizate a sediilor echipei CSIRT naţionale din cadrul CERT-RO şi a sistemelor informatice de suport;

h) mijloacele necesare asigurării controlului punerii în aplicare a dispoziţiilor prezentei legi şi aplicării de sancţiuni, precum şi pentru îndeplinirea celorlalte obligaţii ce îi revin conform legii;

i) personalul adecvat, inclusiv din punct de vedere al competenţelor.

(5) Începând cu 1 ianuarie 2019 resursele financiare necesare pentru funcţionarea CERT-RO se asigură din venituri proprii prevăzute la alin.(6) şi în completare din subvenţii de la bugetul de stat prin bugetul MCSI.

(6) Începând cu 1 ianuarie 2019 CERT-RO poate reţine şi utiliza următoarele categorii de venituri proprii:

a) sumele provenite din activităţile prevăzute la art. 32 alin. (2) lit. c) şi e), respectiv activităţile prevăzute la art. 33 alin. (2) lit. c) şi e);

b) sumele provenite din furnizarea serviciului prevăzut la art. 22 alin. (1) lit. l).

(7) Cuantumul tarifului pentru serviciile prevăzute la alin. (6) se stabileşte prin ordin al ministrului comunicaţiilor şi societăţii informaţionale, la propunerea directorului general al CERT-RO şi se publică în Monitorul Oficial al României, Partea I.

(8) Din bugetul CERT-RO se asigură cu respectarea prevederilor legale în vigoare şi următoarele categorii de cheltuieli:

a) achiziţionarea de servicii de specialitate;

b) închirierea, achiziţionarea sau construcţia de imobile în vederea desfăşurării activităţii;

c) achiziţia de echipamente şi software, inclusiv software dezvoltat la comandă;

d) afilierea la reţele şi organizaţii internaţionale de profil şi participarea prin reprezentanţi la lucrările acestora, precum şi la alte evenimente de profil;

e) cursuri de formare şi perfecţionare, precum şi certificări ale personalului propriu;

f) editarea de publicaţii, ghiduri de specialitate, clipuri video de conştientizare;

g) organizarea de conferinţe, seminarii şi alte evenimente de profil;

h) efectuarea de studii statistice şi activităţi de cercetare;

i) renovări şi îmbunătăţiri ale sediilor şi locaţiilor de desfăşurare a activităţii.

(9) CERT-RO poate folosi pentru desfăşurarea activităţii bunuri materiale şi fonduri băneşti primite de la persoanele juridice şi fizice, sub formă de donaţii şi sponsorizări, cu respectarea dispoziţiilor legale și asigurarea transparenței privind donațiile, sponsorizările și sursa acestora.

(10) CERT-RO poate înfiinţa birouri şi sedii la nivel local în vederea asigurării activităţilor şi reprezentării adecvate pentru îndeplinirea obligaţiilor ce îi revin în temeiul prezentei legi.

CAPITOLUL IV
Asigurarea securității rețelelor și sistemelor informatice

SECŢIUNEA 1
Cerinţele minime de securitate

Art. 25. – (1) În vederea asigurării unui nivel comun de securitate a reţelelor şi sistemelor informatice, operatorii de servicii esenţiale şi furnizorii de servicii digitale au obligaţia de a respecta normele tehnice elaborate de CERT-RO în temeiul prevederilor art. 20 lit. b).

(2) CERT-RO elaborează cu consultarea autorităţilor care reglementează sectoarele şi subsectoarele prevăzute în anexă ghiduri în sprijinul implementării măsurilor minime de securitate pentru operatorii şi furnizorii prevăzuţi în prezenta lege.

(3) Normele tehnice prevăzute la alin. (1) aplicabile operatorilor de servicii esenţiale se stabilesc în baza cel puţin a următoarelor categorii de activităţi de asigurare a securităţii reţelelor şi sistemelor informatice:

a) managementul drepturilor de acces;

b) conştientizarea şi instruirea utilizatorilor;

c) jurnalizarea şi asigurarea trasabilităţii activităţilor în cadrul reţelelor şi sistemelor informatice;

d) testarea şi evaluarea securităţii reţelelor şi sistemelor informatice;

e) managementul configuraţiilor reţelelor şi sistemelor informatice;

f) asigurarea disponibilităţii serviciului esenţial şi a funcţionării reţelelor şi sistemelor informatice;

g) managementul continuităţii funcţionării serviciului esenţial;

h) managementul identificării şi autentificării utilizatorilor;

i) răspunsul la incidente;

j) mentenanţa reţelelor şi sistemelor informatice;

k) managementul suporturilor de memorie externă;

l) asigurarea protecţiei fizice a reţelelor şi sistemelor informatice;

m) realizarea planurilor de securitate;

n) asigurarea securităţii personalului;

o) analizarea şi evaluarea riscurilor;

p) asigurarea protecţiei produselor şi serviciilor aferente reţelelor şi sistemelor informatice;

q) managementul vulnerabilităţilor şi alertelor de securitate.

(4) Normele tehnice prevăzute la alin. (1) aplicabile furnizorilor de servicii digitale se stabilesc în baza următoarelor categorii de activităţi de asigurare a securităţii reţelelor şi sistemelor informatice:

a) securitatea sistemelor şi a instalaţiilor;

b) gestionarea incidentelor;

c) gestionarea continuităţii activităţii;

d) monitorizarea, auditarea şi testarea;

e) conformitatea cu standardele europene şi internaţionale.

(5) În implementarea măsurilor de la alin. (1) operatorii de servicii esenţiale:

a) identifică reţelele şi sistemele informatice care susţin furnizarea de servicii esenţiale;

b) elaborează şi implementează politici şi planuri proprii de securitate a reţelelor şi sistemelor informatice;

c) asigură managementul incidentelor care afectează securitatea reţelelor şi sistemelor informatice;

d) previn accesul neautorizat la reţelele şi sistemele informatice;

e) previn diseminarea datelor deţinute la nivelul reţelelor şi sistemelor informatice către alte persoane decât cele autorizate să cunoască conţinutul acestora;

f) implementează un sistem de management al riscului;

g) implementează planuri de acţiune pe niveluri de alertă de securitate a reţelelor şi sistemelor informatice;

h) asigură continuitatea serviciilor.

(6) Normele tehnice prevăzute la alin. (1) se emit cu luarea în considerare a cerinţelor şi standardelor europene şi internaţionale fără a impune sau a discrimina în favoarea utilizării unui anumit tip de tehnologie.

SECŢIUNEA a 2-a
Notificarea incidentelor de securitate

Art. 26. – (1) Notificările efectuate de operatorii de servicii esenţiale în temeiul art. 10 alin. (1) lit. c) trebuie să îndeplinească condiţiile şi să conţină informaţiile prevăzute în normele tehnice prevăzute la art. 20 lit. c).

(2) Notificările efectuate de furnizorii de servicii digitale în temeiul prevederilor art. 12 alin. (1) lit. c) trebuie să îndeplinească condiţiile şi să conţină informaţiile prevăzute în normele tehnice prevăzute la art. 20 lit. c).

(3) Notificarea incidentelor conţine, în mod obligatoriu, următoarele informaţii:

a) elementele de identificare ale infrastructurii şi operatorului sau furnizorului în cauză;

b) descrierea incidentului;

c) perioada de desfăşurare a incidentului;

d) impactul estimat al incidentului;

e) măsuri preliminare adoptate;

f) lista de autorităţi ale statului afectate de incident;

g) întinderea geografică potenţială a incidentului;

h) date despre efecte potenţial transfrontaliere ale incidentului.

(4) Notificarea prevăzută la alin. (1) şi (2) nu va conţine:

a) informaţii clasificate;

b) date care pot aduce atingere drepturilor şi libertăţilor cetăţeneşti ori intereselor legitime ale unor terţe entităţi implicate în incident, în condiţiile legii.

(5) CERT-RO în calitate de autoritate competentă la nivel naţional elaborează şi actualizează prin decizia directorului general publicată în Monitorul Oficial al României, Partea I, formularele necesare notificărilor de incident efectuate în temeiul prezentului articol, detaliind informaţiile şi documentaţiile necesare a fi furnizate.

(6) CERT-RO în calitate de CSIRT naţional va stabili şi va aduce la cunoştinţa publicului, precum şi operatorilor şi furnizorilor menţionaţi în prezenta lege, mijloacele de comunicare pentru efectuarea notificărilor cerute prin prezenta lege.

(7) Notificările privind incidentele ce fac obiectul prezentei legi pot fi făcute şi de către echipele CSIRT ale entităţilor de drept public sau privat ori care deservesc un anumit sector de activitate, ori de către furnizorii de servicii

de securitate aflaţi în relaţie contractuală, conform atribuţiilor ce le revin în baza actului de înfiinţare ori a contractului de prestări servicii, după caz.

(8) Notificarea făcută de o echipă CSIRT în temeiul alin. (7) echivalează cu notificarea făcută de operatorul sau furnizorul afectat, acesta purtând întreaga răspundere pentru conţinutul notificării şi îndeplinirea celorlalte obligaţii ce îi revin conform prezentei legi.

(9) Obligaţia de a notifica un incident de către furnizorii de servicii digitale se aplică doar în cazul în care aceştia au acces la informaţiile necesare pentru a evalua impactul unui incident asupra parametrilor menţionaţi la art. 28 alin. (2).

(10) Entităţile care nu au fost identificate drept operatori de servicii esenţiale şi nu sunt furnizori de servicii digitale pot notifica voluntar CERT-RO în calitate de CSIRT naţional furnizând cel puţin informaţiile prevăzute la alin. (3), incidentele care au un impact semnificativ asupra continuităţii serviciilor pe care le furnizează.

(11) CERT-RO tratează notificările obligatorii cu prioritate faţă de notificările voluntare.

(12) Notificările voluntare se tratează doar atunci când această prelucrare nu împiedică îndeplinirea celorlalte obligaţii ce îi revin autorităţii competente la nivel naţional şi în limita resurselor existente.

(13) Notificarea voluntară nu impune entităţii notificatoare nicio obligaţie care nu i-ar fi revenit dacă nu ar fi făcut notificarea.

(14) Notificările prevăzute la alin. (1) şi (2) nu atrag răspunderea pentru entităţile care notifică, în condiţiile respectării obligaţiilor prevăzute de prezenta lege.

SECŢIUNEA a 3-a
Managementul incidentelor

Art. 27. – După primirea notificării, CERT-RO în calitate de CSIRT naţional:

a) evaluează preliminar impactul incidentului la nivel naţional şi alertează, sesizează ori notifică, sau după caz, poate solicita operatorului sau furnizorului să alerteze alte entităţi afectate, precum şi autorităţile cu responsabilităţi în prevenirea, limitarea şi combaterea efectelor incidentului, precum şi autorităţile prevăzute la art. 16, potrivit legii;

b) poate solicita informaţii suplimentare operatorului sau furnizorului care a făcut notificarea în vederea îndeplinirii obligaţiilor ce îi revin menţionând termenul de furnizare a acestora;

c) oferă operatorului sau furnizorului care a făcut notificarea, atunci când circumstanţele o permit, informaţii care ar putea sprijini administrarea incidentului;

d) în calitate de Punct unic de contact informează celelalte state membre sau partenere afectate dacă incidentul are un impact semnificativ asupra continuităţii serviciilor esenţiale ori a serviciilor digitale în statele respective;

e) în urma analizei incidentelor, poate, după caz, declanşa acţiune de control pentru verificarea respectării cerinţelor prezentei legi;

f) poate lua măsurile prevăzute la art. 41;

g) coordonează la nivel naţional răspunsul la incident în colaborare cu celelalte autorităţi şi entităţi publice sau private, conform domeniului de activitate şi responsabilitate.

Art. 28. – (1) Impactul unui incident se determină ţinând cont cel puţin de următorii parametri:

i. în cazul operatorilor de servicii esenţiale:

a) numărul de utilizatori afectaţi de perturbarea serviciului esenţial;

b) durata incidentului;

c) distribuţia geografică în ceea ce priveşte zona afectată de incident.

ii. în cazul furnizorilor de servicii digitale:

a) numărul de utilizatori afectaţi de incident, în special utilizatori care se bazează pe serviciul pentru furnizarea propriilor servicii;

b) durata incidentului;

c) distribuţia geografică în ceea ce priveşte zona afectată de incident;

d) amploarea perturbării funcţionării serviciului;

e) amploarea impactului asupra activităţilor economice şi societale.

(2) Grupul de lucru interinstituţional prevăzut la art. 6 alin. (4) elaborează şi actualizează normele tehnice de stabilire a impactului pentru categoriile de operatori şi furnizori prevăzuţi de prezenta lege.

(3) Criteriile prevăzute la pct. 2 se aplică şi notificărilor voluntare efectuate în temeiul prevederilor art. 26 alin. (10).

Art. 29. – (1) CERT-RO poate înştiinţa publicul, atunci când informarea este necesară pentru a preveni un incident sau pentru a se administra un incident în curs.

(2) Pentru incidentele care afectează un operator de servicii esenţiale sau un furnizor de servicii digitale informarea menţionată la alin. (1) se realizează după consultarea prealabilă a acestuia asupra conţinutului înştiinţării.

(3) În cazul furnizorilor de servicii digitale, informarea publicului specificată la alin. (1) poate fi făcută şi direct de către aceştia la solicitarea CERT-RO ori a autorităţilor sau echipelor CSIRT ale altor state membre afectate.

Art. 30. – (1) În activităţile de identificare a operatorilor de servicii esenţiale şi furnizorilor de servicii digitale, de control, de primire a notificărilor privitoare la incidente şi de management al acestora desfăşurate în baza prezentei legi, precum şi în procesele interne, CERT-RO protejează interesele de securitate şi comerciale ale operatorului de servicii esenţiale şi ale furnizorului de servicii digitale, precum şi confidenţialitatea informaţiilor furnizate.

(2) Cu excepţia informaţiilor necesare înştiinţării de la art. 29 alin. (1), informaţiile prelucrate în sensul îndeplinirii obligaţiilor de la alin. (1) nu fac parte din categoria informaţiilor de interes public aşa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare.

(3) Informaţiile confidenţiale conform legislaţiei naţionale şi normelor Uniunii Europene, precum cele privind secretul comercial, fac obiectul schimbului de informaţii cu Comisia Europeană şi cu alte autorităţi numai dacă acest lucru este necesar pentru aplicarea prezentei legi.

(4) Informaţiile care fac obiectul schimbului menţionat la alin. (3) se limitează la informaţii relevante şi proporţionale cu scopul urmărit.

(5) Schimbul de informaţii menţionat la alin. (3) se va face cu garantarea păstrării confidenţialităţii informaţiilor şi protejarea securităţii şi intereselor comerciale ale operatorilor de servicii esenţiale şi ale furnizorilor de servicii digitale.

(6) Prelucrările de date cu caracter personal ce intră sub incidenţa prezentei legi se efectuează cu respectarea reglementărilor legale privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.

(7) Notificările realizate în temeiul prezentei legi nu afectează obligaţiile operatorilor de date cu caracter personal stabilite potrivit art. 33 şi 34 din Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE.

(8) În scopul îndeplinirii atribuţiilor ori furnizării serviciilor prevăzute de prezenta lege, precum şi în scopul prevenirii şi răspunsului la incidentele de securitate informatică, ori al cooperării la nivel naţional, comunitar şi internaţional în prevenirea şi răspunsul la incidentele de securitate informatică, CERT-RO colectează, primeşte, prelucrează şi

transmite date și informații ce pot constitui sau pot conține date cu caracter personal, în limitele legislației aplicabile, cu asigurarea respectării prevederilor alin. (6).

CAPITOLUL V
Audit și autorizare

SECȚIUNEA 1
Auditul de securitate a rețelelor și sistemelor informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale

Art. 31. – Poate fi auditor de securitate a rețelelor și sistemelor informatice – persoana fizică sau persoana juridică ce realizează, audit de securitate a rețelelor și sistemelor informatice, adică desfășoară acea activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul rețelelor și sistemelor informatice, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora.

Art. 32. – (1) Auditul de securitate specificat la art. 8 alin. (4), respectiv art. 10 alin. (2) lit. b) și art. 12 alin. (2) lit. b) se realizează de către auditorii de securitate informatică ce dețin atestat valabil eliberat de către CERT-RO pentru a audita rețele și sisteme informatice ce deservesc servicii esențiale sau servicii digitale în sensul prezentei legi.

(2) În acest sens CERT-RO:

a) întreține și actualizează Registrul auditorilor menționați la alin. (1);

b) elaborează și transmite spre aprobare MCSI în conformitate cu prevederile art. 20 lit. e) și s), regulamentul pentru atestarea și verificarea auditorilor de securitate informatică pentru rețelele și sistemele informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale și stabilește condițiile de valabilitate pentru atestatele acordate;

c) acordă, prelungește, suspendă sau retrage atestarea pentru auditorii de securitate informatică pentru rețelele și sistemele informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale, în conformitate cu prevederile regulamentului prevăzut la lit. b);

d) verifică în urma sesizărilor sau din oficiu în conformitate cu prevederile art. 35 – 42 îndeplinirea de către auditorii atestați în temeiul prezentei legi a obligațiilor legale ce le revin;

e) elaborează și aprobă prin decizia directorului general publicată în Monitorul Oficial al României, Partea I, tematicile pentru specializarea auditorilor în vederea atestării prevăzute la lit. c) și autorizează, verifică, suspendă sau retrage autorizarea formatorilor din domeniul auditului de

securitate informatică pentru reţelele şi sistemele informatice ale operatorilor de servicii esenţiale şi furnizorilor de servicii digitale.

(3) Nu pot realiza auditul solicitat la art. 10 alin. (2) lit. b), respectiv art. 12 alin. (2) lit. b):

a) auditorii atestaţi care asigură în mod curent servicii de securitate informatică ori servicii de tip CSRIT operatorului de servicii esenţiale sau furnizorul de servicii digitale, ori sunt angajaţi ai acestora;

b) auditorul care are un contract de prestări servicii pentru reţeaua şi sistemul supus auditului aflat în desfăşurare la momentul la care se efectuează auditul sau într-un termen mai mic de un an;

c) auditorul care a mai efectuat 3 audituri consecutive la acelaşi operator de servicii esenţiale sau furnizor de servicii digitale.

(4) Activitatea de audit se efectuează potrivit standardelor şi specificaţiilor europene şi internaţionale aplicabile în domeniu.

(5) Tematicile de audit vor ţine seama de normele tehnice în vigoare privind securitatea reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale elaborate în temeiul prezentei legi.

(6) Atestatele au o valabilitate de 3 ani.

(7) Constituie excepţie de la prevederile alin. (1) auditul de securitate realizat la nivelul instituţiilor cu responsabilităţi în domeniul apărării, ordinii publice şi securităţii naţionale cât şi pentru serviciile puse la dispoziţie de către aceştia.

(8) Lista standardelor şi specificaţiilor europene şi internaţionale prevăzute la alin. (4) se elaborează şi se aprobă prin decizia directorului general al CERT-RO, se actualizează periodic şi se publică în Monitorul Oficial al României, Partea I.

SECŢIUNEA a 2-a

Autorizarea echipelor CSIRT ce deservesc reţele şi sisteme informatice din categoria serviciilor esenţiale şi serviciilor digitale

Art. 33. – (1) Echipele CSIRT care deservesc operatori de servicii esenţiale ori furnizori de servicii digitale se autorizează de către CERT-RO în calitate de autoritate competentă la nivel naţional.

(2) În acest sens CERT-RO:

a) întreţine şi actualizează Registrul echipelor CSIRT prevăzute la alin. (1);

b) elaborează şi transmite spre aprobare MCSI în conformitate cu prevederile art. 20 lit. e) şi s), regulamentul pentru autorizarea şi verificarea echipelor CSIRT care deservesc operatorii de servicii esenţiale sau furnizorii

de servicii digitale şi stabileşte condiţiile de valabilitate pentru autorizaţiile acordate;

c) acordă, prelungeşte, suspendă sau retrage autorizarea pentru echipele CSIRT, în conformitate cu prevederile regulamentului prevăzut la lit. b);

d) verifică în urma sesizărilor sau din oficiu în conformitate cu prevederile art. 35 – 42 îndeplinirea de către echipele CSIRT autorizate în temeiul prezentei legi a obligaţiilor legale ce le revin;

e) elaborează tematicile pentru formarea membrilor echipelor CSIRT în vederea autorizării prevăzute la lit. c) şi autorizează, verifică, suspendă sau retrage autorizarea formatorilor din domeniul asigurării de servicii de tip CSIRT pentru reţelele şi sistemele informatice ale operatorilor de servicii esenţiale şi furnizorilor de servicii digitale.

(3) În vederea autorizării, echipa CSIRT trebuie să îndeplinească condiţiile prevăzute în normele tehnice elaborate în temeiul prevederilor art. 20 lit. e).

(4) Autorizaţiile au o valabilitate de 3 ani.

CAPITOLUL VI
Cooperare

Art. 34. – (1) Autorităţile şi entităţile care reglementează sectoarele şi subsectoarele de activitate prevăzute în anexă au obligaţia de a coopera şi sprijini CERT-RO în calitate de autoritate competentă la nivel naţional şi de a răspunde solicitărilor acesteia, potrivit domeniilor de activitate şi responsabilitate pentru:

a) identificarea serviciilor esenţiale din sectoarele de activitate reglementate de acestea;

b) identificarea operatorilor de servicii esenţiale în sensul prezentei legi şi actualizarea listei acestora;

c) identificarea cerinţelor de securitate şi notificare existente în cadrul sectorului sau subsectorului respectiv, în vederea determinării nivelului de securitate asigurat de acestea;

d) stabilirea cerinţelor specifice de asigurare a securităţii reţelelor şi sistemelor informatice şi de notificare a incidentelor survenite pentru sectoarele şi subsectoarele prevăzute în anexă;

e) armonizarea cerinţelor specifice prevăzute la punctele anterioare cu cerinţele de securitate şi notificare prevăzute de prezenta lege;

f) luarea măsurilor cu caracter excepţional prevăzute la art. 41;

g) stabilirea criteriilor şi valorilor de prag specifice, necesare pentru determinarea impactului unui incident la nivelul sectorului sau subsectorului respectiv;

h) armonizarea reglementărilor emise de acestea la nivel de sector cu cerinţele prezentei legi.

(2) Cerinţele specifice de securitate impuse operatorilor de servicii esenţiale sau furnizorilor de servicii digitale prin acte juridice ale Uniunii Europene de directă aplicare sau prin acte juridice ale Uniunii Europene transpuse la nivel naţional care reglementează respectivul sector de activitate se aplică doar în măsura în care nivelul de securitate asigurat este cel puţin echivalent cu obligaţiile prevăzute în prezenta lege.

(3) Aplicarea actelor juridice ale Uniunii Europene prevăzute la alin. (2) nu derogă de la celelalte obligaţii care revin operatorilor de servicii esenţiale şi furnizorilor de servicii digitale conform prezentei legi.

CAPITOLUL VII
Supraveghere, control, sancţionare

SECŢIUNEA 1
Activitatea de control

Art. 35. – (1) CERT-RO exercită controlul respectării prevederilor prezentei legi, a obligaţiilor impuse prin actele emise de CERT-RO în aplicarea prezentei legi, în limitele competenţelor legale de monitorizare sau de verificare.

(2) În vederea efectuării controlului prevăzut la alin.(1), directorul general al CERT-RO, prin decizie, desemnează personalul de specialitate împuternicit să efectueze controlul şi stabileşte atribuţiile acestuia.

(3) Normelor de aplicare a dispoziţiilor privind controlul îndeplinirii obligaţiilor de securitate şi notificare de către operatorii de servicii esenţiale şi furnizorii de servicii digitale şi controlul îndeplinirii obligaţiilor de către auditorii de securitate informatică atestaţi ori de către echipele CSIRT autorizate să deservească operatori de servicii esenţiale şi furnizori de servicii digitale se aprobă, la propunerea CERT-RO, prin ordin al ministrului comunicaţiilor şi societăţii informaţionale care se publică în Monitorul Oficial al României, Partea I.

Art. 36. – (1) În urma sesizărilor primite, din oficiu, sau în urma autosesizării în temeiul art. 27 lit. e), precum şi în situaţia existenţei unor indicii temeinice privind sustragerea unui operator sau furnizor de la obligaţiile ce îi revin în temeiul prezentei legi, ori încălcarea de către un auditor, echipă CSIRT sau furnizor de formare autorizat, a obligaţiilor ce le revin în temeiul prezentei legi, personalul de control poate să efectueze acţiuni de control, în cadrul cărora poate să solicite, menţionând temeiul legal şi scopul solicitării, documentele necesare pentru efectuarea controlului, să

ridice copii de pe registre ori alte acte sau documente, în condiţiile legii, inclusiv a prevederilor referitoare la păstrarea confidenţialităţii tuturor documentelor şi informaţiilor primite.

(2) În cadrul acţiunilor de control, personalul de control poate să solicite şi să primească, la faţa locului sau la termenul solicitat, informaţiile necesare pentru efectuarea controlului şi poate stabili termene până la care aceste informaţii să îi fie furnizate, în condiţiile legii, inclusiv a prevederilor referitoare la păstrarea confidenţialităţii tuturor documentelor şi informaţiilor primite.

(3) Rezultatul acţiunilor de control va fi consemnat într-o notă de control.

Art. 37. – (1) Înainte de aplicarea unei sancţiuni, în cazul descoperirii nerespectării de către un furnizor de servicii digitale sau operator de servicii esenţiale a unei obligaţii prevăzută de prezenta lege sau de un act emis de CERT-RO în baza prezentei legi, CERT-RO va transmite entităţii în cauză o notificare prin care îi va aduce la cunoştinţă încălcarea constatată, măsurile cu caracter obligatoriu ce trebuie luate în vederea remedierii deficienţelor constatate şi stabileşte termenul de conformare, precum şi sancţiunea aplicabilă.

(2) Termenul de conformare se calculează începând cu data comunicării notificării prevăzute la alin. (1).

Art. 38. – Următoarele fapte constituie contravenţii dacă nu au fost săvârşite în astfel de condiţii încât să fie considerate potrivit legii infracţiuni:

1. neîndeplinirea obligaţiei de notificare în vederea înscrierii în registrul operatorilor de servicii esenţiale, prevăzută la art. 8 alin. (1) în termenul prevăzut la art. 8 alin. (6);

2. neîndeplinirea în termenul prevăzut a obligaţiei de furnizare a informaţiilor solicitate de către CERT-RO în temeiul art. 8 alin. (7) lit. a);

3. neîndeplinirea în termenul prevăzut a obligaţiei de furnizare a informaţiilor solicitate de către CERT-RO în temeiul art. 8 alin. (7) lit. b);

4. neîndeplinirea în termenul prevăzut a obligaţiei de furnizare a informaţiilor solicitate de către CERT-RO în temeiul art. 8 alin. (7) lit. c);

5. neîndeplinirea în termenul prevăzut a obligaţiei de furnizare a informaţiilor solicitate de către CERT-RO în temeiul art. 8 alin. (7) lit. d);

6. nedepunerea raportului de audit specificat la art. 8 alin. (4) şi (7) în termenul comunicat de către CERT-RO persoanei juridice în temeiul art. 8 alin. (8);

7. neîndeplinirea obligaţiei prevăzută la art. 9 alin. (1) în termenul prevăzut la art. 9 alin. (5);

8. neducerea la îndeplinire a măsurilor dispuse de CERT-RO prin notificarea transmisă în urma controlului, pentru remedierea deficiențelor constatate, în termenul de conformare stabilit în conformitate cu prevederile art.37;

9. neîndeplinirea de către operatorii de servicii esenţiale a obligaţiei de implementare a măsurilor pentru îndeplinirea cerinţelor minime de securitate în conformitate cu art. 10 alin. (1) lit. a) în termenul stabilit la art. 10 alin. (4);

10. neîndeplinirea de către operatorii de servicii esenţiale a obligaţiei de implementare a măsurilor adecvate pentru a preveni şi minimiza impactul incidentelor în conformitate cu art. 10 alin. (1) lit. b) în termenul stabilit la art. 10 alin. (4);

11. încălcarea de către operatorii de servicii esenţiale a obligaţiei stabilită la art. 10 alin. (1) lit. c) de a notifica incidentul de securitate ori notificarea acestuia cu o întârziere mai mare de 12 ore de la data constatării acestuia;

12. încălcarea obligaţiei stabilită la art. 10 alin. (1) lit. d) prin nefurnizarea în cadrul notificării privitoare la incidentul de securitate a informaţiilor care să permită stabilirea impactului transfrontalier a acestuia;

13. nerespectarea prevederilor art. 10 alin. (1) lit. e) în termen de 48 de ore de la data comunicării de către CERT-RO a ordinului de începere a controlului;

14. necomunicarea către CERT-RO a informaţiilor şi mijloacelor permanente de contact ori a actualizărilor acestora în termenele stabilite la art. 10 alin. (1) lit. f);

15. neîndeplinirea obligaţiei de comunicare prevăzută la art. 10 alin. (1) lit. g) în termen de 30 de zile;

16. neîndeplinirea obligaţiei de interconectare prevăzută la art. 10 alin. (1) lit. h) în termen de 60 de zile;

17. neluarea de către operatorul de servicii esenţiale a măsurilor adecvate de răspuns în termen de 12 ore de la primirea prin serviciul de alertare şi cooperare al CERT-RO menţionat la art. 10 alin. (1) lit. h) ori prin celelalte mijloace de contact a alertelor şi solicitărilor privitoare la incidente;

18. neîndeplinirea de îndată a obligaţiei de a asigura răspunsul la incidentele survenite stabilită la art. 10 alin. (1) lit. i) ori îndeplinirea acesteia cu o întârziere mai mare de 12 ore de la data constatării incidentului;

19. neîndeplinirea obligaţiei stabilită la art. 10 alin. (1) lit. i) de a restabili funcţionarea serviciului esenţial afectat de incident la parametrii dinaintea incidentului ori întârzierea nejustificată a restabilirii funcţionării acestuia;

20. neîndeplinirea în urma răspunsului la incident a obligaţiei stabilită la art. 10 alin. (1) lit. i) de a efectua auditul de securitate a reţelelor şi sistemelor informatice afectate;

21. nefurnizarea în termenul stabilit de CERT-RO a informaţiilor si documentaţiilor solicitate în temeiul art. 10 alin. (2) lit. a);

22. neefectuarea auditului de securitate şi netransmiterea rezultatelor acestuia şi a datelor necesare în termenul stabilit de CERT-RO în urma solicitării făcute în temeiul prevederilor art. 10 alin. (2) lit. b);

23. încălcarea cumulativă a obligaţiilor prevăzute la art. 10 alin. (3) şi art. 26 alin. (1) – (3) într-un termen de 12 ore de la data constatării incidentului de către operatorul de servicii esenţiale;

24. neîndeplinirea de către operatorii de servicii esenţiale a obligaţiei prevăzute la art. 11 în termenele stabilite de CERT-RO prin actul de control comunicat operatorului de servicii esenţiale;

25. neducerea la îndeplinire de către furnizorul de servicii digitale a măsurilor dispuse de CERT-RO prin notificarea transmisă în urma controlului, pentru remedierea deficienţelor constatate în aplicarea prevederilor art. 12 alin. (1) lit. a) şi b) în termenul de conformare stabilit în conformitate cu prevederile art. 37;

26. neîndeplinirea de către furnizorii de servicii digitale, în termenul stabilit, a obligaţiei de implementare a măsurilor pentru respectarea cerinţelor minime de securitate în conformitate cu prevederile art. 12 alin. (1) lit. a);

27. neîndeplinirea de către furnizorii de servicii digitale a obligaţiei de implementare, în termenul stabilit, a măsurilor adecvate pentru a preveni şi minimiza impactul incidentelor în conformitate cu prevederile art. 12 alin. (1) lit. b);

28. încălcarea de către furnizorii de servicii digitale a obligaţiei stabilită la art. 12 alin. (1) lit. c) de a notifica incidentul de securitate ori notificarea acestuia cu o întârziere mai mare de 12 ore de la data constatării acestuia;

29. încălcarea obligaţiei stabilită la art. 12 alin. (1) lit. d) prin nefurnizarea în cadrul notificării privitoare la incidentul de securitate a informaţiilor care să permită stabilirea impactului transfrontalier a acestuia;

30. necomunicarea către CERT-RO a informaţiilor şi mijloacelor permanente de contact în termenul stabilit la art. 12 alin. (1) lit. e);

31. neîndeplinirea obligaţiei de comunicare a modificărilor survenite în datele de contact prevăzută la art. 12 alin. (1) lit. e) în termen de 30 de zile;

32. neîndeplinirea obligaţiei de interconectare prevăzută la art. 12 alin. (1) lit. f) în termen de 60 de zile;

33. neluarea de către furnizorul de servicii digitale a măsurilor adecvate de răspuns în termen de 12 ore de la primirea prin serviciul de

alertare şi cooperare al CERT-RO menţionat la art. 12 alin. (1) lit. f) ori prin celelalte mijloace de contact a alertelor şi solicitărilor privitoare la incidente;

34. neîndeplinirea obligaţiei de a asigura răspunsul la incidentele de securitate şi de a asigura continuitatea serviciilor stabilite la art. 12 alin. (1) lit. b) ori îndeplinirea acestora cu o întârziere mai mare de 12 ore de la data constatării incidentului;

35. nefurnizarea în termenul stabilit de CERT-RO a informaţiilor şi documentaţiilor solicitate în temeiul art. 12 alin. (2) lit. a);

36. neefectuarea auditului de securitate şi netransmiterea rezultatelor acestuia şi a datelor necesare în termenul stabilit de CERT-RO în urma solicitării făcute în temeiul art. 12 alin. (2) lit. b);

37. neîndeplinirea în termenul prevăzut a obligaţiei de furnizare a informaţiilor solicitate de către CERT-RO în temeiul art. 12 alin. (6) lit. a);

38. neîndeplinirea în termenul prevăzut a obligaţiei de furnizare a informaţiilor solicitate de către CERT-RO în temeiul art. 12 alin. (6) lit. b);

39. neîndeplinirea în termenul prevăzut a obligaţiei de furnizare a informaţiilor solicitate de către CERT-RO în temeiul art. 12 alin. (6) lit. c);

40. neducerea la îndeplinire a măsurilor instituite de CERT-RO în temeiul art.20 lit.k), în termen de 60 de zile de la data comunicării;

41. neconformarea cu normele tehnice prevăzute la art. 25 alin. (1);

42. neconformarea operatorilor de servicii esenţiale cu normele tehnice privitoare la notificarea incidentelor de securitate prevăzute la art. 26 alin. (1);

43. neconformarea furnizorilor de servicii digitale cu normele tehnice privitoare la notificarea incidentelor de securitate prevăzute la art. 26 alin. (2);

44. nefurnizarea de către operatorul de servicii esenţiale ori furnizorul de servicii digitale în termenul stabilit de CERT-RO a informaţiilor suplimentare solicitate de CERT-RO în temeiul art. 27 lit. b);

45. încălcarea de către auditorii specificaţi la art. 32 alin. (1) a normelor privind incompatibilitatea, prevăzute la art. 32 alin. (3);

46. furnizarea de rapoarte de audit de securitate dintre cele prevăzute la art. 8 alin. (4), respectiv art. 10 alin. (2) lit. b) şi art. 12 alin. (2) lit. b) realizate de către auditori fără atestat valabil eliberat de CERT-RO în temeiul art. 32 alin. (1) şi (2) lit. c) ori aflaţi într-una din stările de incompatibilitate prevăzute la art. 32 alin. (3);

47. asigurarea de servicii de tip echipă CSIRT către operatorii de servicii esenţiale ori furnizorii de servicii digitale de către entităţi care nu deţin autorizaţie valabil, eliberată în temeiul art. 33 alin. (1) de către CERT-RO în calitate de autoritate competentă la nivel naţional;

48. neîndeplinirea de către autorităţile şi entităţile de reglementare pentru sectoarele şi subsectoarele de activitate prevăzute în anexă a

obligaţiilor prevăzute la art. 34 alin. (1), precum şi neparticiparea în procesul de stabilire a nivelului de securitate menţionat la art. 34 alin.(2);

49. refuzul de a se supune controlului declanşat de CERT-RO în temeiul prevederile art. 36 ori întârzierea în furnizarea informaţiilor şi documentelor solicitate în cadrul activităţilor de control în temeiul prevederile art. 37.

Art. 39. – (1) Contravenţiile prevăzute la art. 38 se sancţionează astfel:

a) cu amendă de la 3.000 lei la 50.000 lei, iar în cazul constatării unor încălcări repetate limita maximă a amenzii este de 100.000 lei;

b) prin derogare de la dispoziţiile art. 8 alin. (2) lit. a) din Ordonanţa Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, pentru persoanele cu o cifră de afaceri de peste 2.000.000 lei, cu amendă în cuantum de la 0,5% la 2% din cifra de afaceri, iar, în cazul unor încălcări repetate, limita maximă a amenzii este de 5% din cifra de afaceri.

(2) În vederea individualizării sancţiunii, CERT-RO va lua în considerare gradul de pericol social concret al faptei, perioada de timp în care obligaţia legală a fost încălcată, precum şi, dacă este cazul, consecinţele încălcării.

(3) Cifra de afaceri este cea prevăzută în ultima situaţie financiară anuală raportată de operatorul economic.

(4) Pentru persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale, cifrei de afaceri prevăzute la alin. (1) lit. b) îi corespunde totalitatea veniturilor brute, astfel cum sunt definite de Legea nr. 227/2015 privind Codul fiscal, cu modificările şi completările ulterioare, realizate de respectivele entităţi.

(5) Prin excepţie de la prevederile alin. (3) şi (4), în cazul în care, în anul financiar anterior sancţionării, întreprinderea nu a înregistrat cifra de afaceri sau cifra de afaceri nu poate fi determinată, va fi luată în considerare cea aferentă anului financiar în care entitatea a înregistrat cifra de afaceri, an imediat anterior anului de referinţă pentru calcularea cifrei de afaceri în vederea aplicării sancţiunii. În ipoteza în care nici în anul anterior anului de referinţă pentru calcularea cifrei de afaceri în vederea aplicării sancţiunii entitatea nu a realizat cifra de afaceri, va fi luată în calcul ultima cifră de afaceri înregistrată de entitate.

(6) Pentru entităţile nou înfiinţate şi care nu au înregistrat cifra de afaceri în anul anterior sancţionării, amenda prevăzută la alin. (1) se stabileşte în cuantum de minimum unu şi maximum 25 de salarii minime brute pe economie.

(7) În măsura în care prezenta lege nu prevede altfel, contravenţiilor prevăzute la art. 38 li se aplică dispoziţiile Ordonanţei Guvernului nr. 2/2001, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare.

Art. 40. – (1) Contravenţiile prevăzute la art. 38 se constată de către personalul de control din cadrul CERT-RO prin procesul-verbal de constatare a contravenţiei şi de aplicare a sancţiunii semnat de către personalul care efectuează controlul şi de către reprezentantul operatorului sau furnizorului prezent la momentul încheierii procesului-verbal căruia i se va înmâna o copie a procesului-verbal.

(2) Sancţiunea pentru contravenţiile prevăzute la alin. (1) se aplică de către personalul de control care a făcut constatarea.

Art. 41. – (1) În cazul constatării unei contravenţii în conformitate cu prevederile art. 38, CERT-RO dispune încetarea încălcării dispoziţiilor respective fie imediat, fie într-un termen rezonabil, precum şi orice măsuri necesare pentru a asigura încetarea încălcării şi remedierea situaţiei produse. Măsurile vor fi adecvate şi proporţionale cu încălcarea săvârşită şi vor prevedea un termen în care operatorul de servicii esenţiale ori furnizorul de servicii digitale trebuie să se conformeze acestora.

(2) În cazul în care nerespectarea de către operatori sau furnizori a obligaţiilor din prezenta lege poate crea probleme grave de natură economică sau operaţională altor operatori sau furnizori, CERT-RO poate lua măsuri urgente cu caracter provizoriu pentru remedierea situaţiei.

(3) În cazul în care nerespectarea de către operatori sau furnizori a obligaţiilor prevăzute de prezenta lege prezintă un pericol grav şi iminent la adresa apărării naţionale, ordinii publice, securităţii naţionale sau sănătăţii publice, CERT-RO va informa organele judiciare şi va notifica instituţiile competente din domeniul apărării şi securităţii naţionale, ordinii publice sau sănătăţii publice.

(4) Atunci când apreciază că este necesar, CERT-RO poate menţine măsurile dispuse conform prevederilor alin. (2) pentru o perioadă de cel mult 90 de zile. În cazul în care punerea în executare a acestora necesită o durată mai mare de timp, CERT-RO poate dispune prelungirea aplicabilităţii pentru o perioadă suplimentară de cel mult 90 de zile. Operatorului sau furnizorului în cauză i se va acorda posibilitatea de a-şi prezenta punctul de vedere şi de a propune soluţii pentru remedierea definitivă a situaţiei create.

(5) Măsurile prevăzute la alin. (2) se dispun prin decizie a directorului general al CERT-RO ce poate fi atacată cu plângere în termen de 30 zile de la comunicare.

(6) Măsurile prevăzute la alin. (2) se pot dispune de către CERT-RO cu titlu excepţional şi în situaţia administrării unor incidente de natură să prezinte pericolele ori să aibă urmările prevăzute la alin. (3) cu consultarea, precum şi la solicitarea motivată a instituţiilor prevăzute la alineatul respectiv.

Art. 42. – (1) În exercitarea atribuţiilor ce îi revin potrivit actelor normative în vigoare, CERT-RO va fi sprijinită operativ, la cerere, de către autorităţile publice, precum şi de către organele de poliţie în cazuri temeinic justificate, în vederea identificării şi localizării persoanelor fizice sau juridice care săvârşesc fapte de natură contravenţională.

(2) Orice decizie a CERT-RO prin care se vatămă drepturile unei persoane fizice sau juridice, ori refuzul nejustificat al CERT-RO de a-i procesa cererea referitoare la un drept recunoscut de prezenta lege pot fi atacate în contencios administrativ.

CAPITOLUL VIII
Dispoziţii tranzitorii

Art. 43. – Înscrierea în Registrul prevăzut la art. 8, în primii 2 ani de la data intrării în vigoare a prezentei legi, se face prin depunerea unei declaraţii pe propria răspundere însoţită de o documentaţie de autoevaluare a îndeplinirii cerinţelor minime de securitate şi notificare.

CAPITOLUL IX
Dispoziţii finale

Art. 44. – Până la 9 august 2018 şi, ulterior, în fiecare an, CERT-RO în calitate de Punct unic de contact transmite grupului de cooperare un raport de sinteză privind notificările primite, care include numărul de notificări şi natura incidentelor notificate, precum şi acţiunile întreprinse în conformitate cu prevederile art. 10 alin. (1) lit. c), art. 12 alin. (1) lit. c) coroborate cu art. 27 lit. d).

Art. 45. – (1) Strategia naţională prevăzută la art. 14 va acoperi cel puţin următoarele elemente:

a) obiectivele şi priorităţile strategiei naţionale privind securitatea reţelelor şi a sistemelor informatice;

b) un cadru de guvernanţă pentru realizarea obiectivelor şi a priorităţilor strategiei naţionale privind securitatea reţelelor şi a sistemelor informatice, care să includă rolurile şi responsabilităţile organismelor guvernamentale şi ale altor actori relevanţi;

c) identificarea măsurilor referitoare la gradul de pregătire, răspuns şi redresare, inclusiv cooperarea dintre sectorul public şi cel privat;

d) indicarea programelor de instruire, sensibilizare şi formare legate de strategia naţională privind securitatea reţelelor şi a sistemelor informatice;

e) indicarea planurilor de cercetare şi dezvoltare legate de strategia naţională privind securitatea reţelelor şi a sistemelor informatice;

f) un plan de evaluare a riscurilor pentru identificarea riscurilor;

g) o listă a diferiţilor actori implicaţi în punerea în aplicare a strategiei naţionale privind securitatea reţelelor şi a sistemelor informatice.

(2) În elaborarea strategiei, MCSI poate solicita asistenţa ENISA.

(3) În termen de 3 luni de la data intrării în vigoare a prezentei legi, MCSI transmite Comisiei Europene strategia adoptată în temeiul art. 14.

(4) Comunicarea de la alin. (3) nu va conţine elementele care au legătură cu securitatea naţională.

Art. 46. – CERT-RO identifică şi stabileşte documentele şi detaliile tehnice necesare pentru evaluarea iniţială a securităţii entităţilor care urmează să se declare operator de servicii esenţiale.

Art. 47. – Cerinţele de securitate şi notificare prevăzute la cap. IV nu se aplică:

a) furnizorilor de reţele publice de comunicaţii electronice şi furnizorilor de servicii de comunicaţii electronice destinate publicului;

b) prestatorilor de servicii de încredere calificaţi şi necalificaţi care fac obiectul art. 19 din Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE.

Art. 48. – (1) Până la 9 noiembrie 2018, pentru fiecare sector şi subsector menţionat în anexă, pe lângă primirea de notificări în vederea înscrierii în Registrul operatorilor de servicii esenţiale conform art. 8 alin. (1), CERT-RO identifică operatorii de servicii esenţiale care au sediul social, filială, sucursală, punct de lucru sau altă formă de reprezentare legal stabilită pe teritoriul României.

(2) În termen de 30 zile de la data intrării în vigoare a prezentei legi, MCSI notifică Comisiei Europene regimul sancţionator aplicabil în temeiul prezentei legi, precum şi orice modificare ulterioară a acestuia.

(3) În termenul prevăzut la alin. (1) şi ulterior la fiecare doi ani, CERT-RO transmite Comisiei Europene următoarele informaţii în vederea evaluării aplicării prezentei legi:

a) lista măsurilor care permit identificarea operatorilor de servicii esenţiale;

b) lista serviciilor prevăzute la art. 6 alin. (1) lit. a);

c) numărul operatorilor de servicii esenţiale identificaţi pentru fiecare sector menţionat în anexă şi o indicaţie a importanţei lor în legătură cu sectorul respectiv;

d) limite, atunci când acestea există, pentru determinarea nivelului relevant de furnizare, în raport cu numărul de utilizatori care se bazează pe serviciul respectiv sau cu importanţa operatorului de servicii esenţiale.

Art. 49. – (1) MCSI va notifica Comisia Europeană în termen de 30 zile de la publicarea în Monitorul Oficial al României, Partea I, a prezentei legi cu privire la desemnarea autorității competente, a Punctului unic de contact și atribuțiilor acestora.

(2) MCSI va notifica Comisia Europeană în termen de 30 zile de la publicarea în Monitorul Oficial al României, Partea I, orice modificare a actelor normative în baza cărora a fost făcută desemnarea de la alin. (1).

(3) MCSI va notifica Comisia Europeană în termen de 30 zile de la publicarea în Monitorul Oficial al României, Partea I, a prezentei legi cu privire la misiunea, precum și la principalele elemente ale procedurilor de administrare a incidentelor folosite de echipa CSIRT națională.

Art. 50. – CERT-RO își desfășoară activitatea în baza prevederilor prezentei legi și a Hotărârii Guvernului nr. 494 din 11 mai 2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, care va fi modificată și completată corespunzător prevederilor prezentei legi.

* *
*

Prezenta lege transpune în totalitate Directiva (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune, publicată în Jurnalul Oficial al Uniunii Europene seria L nr. 194 din 19 iulie 2016.

Această lege a fost adoptată de Parlamentul României, în condiţiile art. 147 alin. (2), cu respectarea prevederilor art. 75 şi ale art. 76 alin. (2) din Constituţia României, republicată.

p. PREŞEDINTELE
CAMEREI DEPUTAŢILOR

FLORIN IORDACHE

PREŞEDINTELE
SENATULUI

CĂLIN POPESCU-TĂRICEANU

Bucureşti,
Nr.

Anexă

Sectoare de activitate și tipuri de entități

Sectorul	Subsectorul	Tipul de entitate
1. Energie	a) Electricitate	- Operatori economici din domeniul energiei electrice astfel cum sunt definiţi la art. 3 pct. 42 din Legea energiei electrice şi a gazelor naturale nr. 123/2012, cu modificările şi completările ulterioare;
		- Operatori de distribuţie, astfel cum sunt definiţi la art. 3 pct. 39 din Legea nr. 123/2012, cu modificările şi completările ulterioare;
		- Operatori de transport şi de sistem, astfel cum sunt definiţi la art. 3 pct. 40 din Legea nr. 123/2012, cu modificările şi completările ulterioare;
	b) Petrol	- Operatori de conducte de transport al petrolului;
		- Operatori ai instalaţiilor de producţie, de rafinare şi de tratare a petrolului, de depozitare şi de transport;
	c) Gaze naturale	- Furnizori persoană fizică sau juridică, astfel cum sunt definiţi la art. 100 pct. 44 din Legea nr. 123/2012, cu modificările şi completările ulterioare;
		- Operatori de distribuţie, astfel cum sunt definiţi la art. 100 pct. 63 din Legea nr. 123/2012, cu modificările şi completările ulterioare;
		- Operatori de transport şi de sistem, astfel cum sunt definiţi la art. 100 pct. 65 din Legea nr. 123/2012, cu modificările şi completările ulterioare;
		- Operatori de înmagazinare, astfel cum sunt definiţi la art. 100 pct. 64 din Legea nr. 123/2012, cu modificările şi completările ulterioare;

		- Operatori ai terminalelor GNL, astfel cum sunt definiţi la art. 100 pct. 60 din Legea nr. 123/2012, cu modificările şi completările ulterioare;
		- Operatori economici din sectorul gazelor naturale, astfel cum sunt definiţi la art. 100 pct. 67 din Legea nr. 123/2012, cu modificările şi completările ulterioare;
		- Operatori de instalaţie de rafinare şi de tratare a gazelor naturale;
2. Transport	a) Transport aerian	- Transportatori aerieni, astfel cum sunt definiţi la art. 3 punctul 4 din Regulamentul (CE) nr. 300/2008 al Parlamentului European şi al Consiliului din 11 martie 2008 privind norme comune în domeniul securităţii aviaţiei civile şi de abrogare a Regulamentului (CE) nr. 2320/2002;
		- Organe de administrare a aeroportului, astfel cum sunt definite la art. 4 din Hotărârea Guvernului nr. 455/2011 privind tarifele de aeroport, inclusiv aeroporturile principale enumerate în Secţiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 al Parlamentului European şi al Consiliului din 11 decembrie 2013 privind orientările Uniunii pentru dezvoltarea reţelei transeuropene de transport şi de abrogare a Deciziei nr. 661/2010/UE, precum şi entităţi care operează instalaţii auxiliare în cadrul aeroporturilor;
		- Operatori de control al gestionării traficului care prestează servicii de control al traficului aerian (ATC), astfel cum sunt definite la art. 2 punctul 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European şi al Consiliului din 10 martie 2004 de stabilire a cadrului pentru crearea

		cerului unic European (regulament-cadru);
	b) Transport feroviar	- Administratori de infrastructuri, astfel cum sunt definiţi la art. 3 pct. 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spaţiul feroviar unic european;
		- Întreprinderi feroviare, astfel cum sunt definite la art. 3 pct. 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spaţiul feroviar unic european;
	c)Transport pe apă	- Companii de transport de mărfuri şi pasageri pe ape interioare, maritime şi de coastă, astfel cum sunt definite pentru transportul maritim în anexa I la Regulamentul (CE) nr. 725/2004 al Parlamentului European şi al Consiliului din 31 martie 2004 privind consolidarea securităţii navelor şi a instalaţiilor portuare, fără a include navele individuale operate de companiile respective;
		- Organe de gestionare a porturilor, astfel cum sunt definite la art. 3 din Ordinul ministrului transporturilor nr. 290/2007 pentru introducerea măsurilor de întărire a securităţii portuare, inclusiv instalaţiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004 şi entităţile care operează lucrări şi echipamente în cadrul porturilor;
		- Operatori de servicii de trafic naval, astfel cum sunt definiţi la art. 3 din Hotărârea Guvernului nr. 1016/2010 pentru stabilirea Sistemului de informare şi monitorizare a traficului navelor maritime care intră/ies în/din apele naţionale navigabile ale României, cu modificările şi completările ulterioare;

	d) Transport rutier	- Autorităţi rutiere, astfel cum sunt definite la art. 2 punctul 12 din Regulamentul delegat (UE) 2015/962 al Comisiei din 18 decembrie 2014 de completare a Directivei 2010/40/UE a Parlamentului European şi a Consiliului în ceea ce priveşte prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic, responsabile pentru controlul gestionării traficului;
		- Operatori de sisteme de transport inteligente, astfel cum sunt definiţi la art. 4 din Ordonanţa Guvernului nr. 7/2012 privind implementarea sistemelor de transport inteligente în domeniul transportului rutier şi pentru realizarea interfeţelor cu alte moduri de transport, aprobată prin Legea nr. 221/2012;
3. Sectorul bancar		- Instituţii de credit, astfel cum sunt definite la art. 4 punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European şi al Consiliului din 26 iunie 2013 privind cerinţele prudenţiale pentru instituţiile de credit şi societăţile de investiţii şi de modificare a Regulamentului (UE) nr. 648/2012;
4. Infrastructuri ale pieţei financiare		- Operatori de locuri de tranzacţionare, astfel cum sunt definite la art. 4 punctul 24 din Directiva 2014/65/UE a Parlamentului European şi a Consiliului din 15 mai 2014 privind pieţele instrumentelor financiare şi de modificare a Directivei 2002/92/CE şi a Directivei 2011/61/UE;
		- Contrapartide centrale, astfel cum sunt definite la art. 2 punctul 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European şi al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate

		extrabursiere, contrapărțile centrale și registrele centrale de tranzacții;
5. Sectorul sănătății	Instituții de asistență medicală (inclusiv spitale și clinici private)	- Furnizori de servicii medicale, astfel cum sunt definiți în Hotărârea Guvernului nr. 304 din 16 aprilie 2014 pentru aprobarea Normelor metodologice privind asistența medicală transfrontalieră;
6. Furnizarea și distribuirea de apă potabilă		- Furnizori și distribuitori de *apă destinată consumului uman*, astfel cum sunt definiți la art. 2 din Legea nr. 458/2002 privind calitatea apei potabile, republicată, cu modificările și completările ulterioare, excluzând distribuitorii pentru care distribuția de apă destinată consumului uman reprezintă doar o parte din activitatea lor generală de distribuire a altor produse de bază și produs care nu sunt considerate servicii esențiale;
7. Infrastructură digitală		- IXP
		- DNS
		- TLD