



GUVERNUL ROMÂNIEI

ORDONANȚĂ DE URGENȚĂ

privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil

Ținând cont de faptul că evoluția rapidă și adopția tehnologiilor emergente creează noi tipuri de interdependențe și expune infrastructura critică a statului unor riscuri complexe, neprevăzute anterior, susceptibile de a genera efecte semnificative asupra securității cibernetice, efecte care se extind și asupra autorităților și instituțiilor din administrația publică,

Având în vedere faptul că diversificarea și utilizarea serviciilor furnizate în mediul online au cunoscut o accelerare majoră datorată unui ansamblu de factori, incluzând conflictul ruso-ucrainean, pandemia de COVID-19, dezvoltarea și globalizarea mediului de afaceri, precum și reducerea costurilor pentru accesarea de noi piețe, au generat atât beneficii, cât și un nou spectru de amenințări, riscuri și vulnerabilități aferente securității cibernetice, vulnerabilități ce sunt intrinsec asociate tehnologiilor smart, precum rețelele 5G, Internetul Lucrurilor (IoT) și Inteligența Artificială (AI),

Luând în considerare faptul că de la izbucnirea conflictului armat în proximitatea teritoriului României, s-a observat o utilizare intensificată a atacurilor cibernetice ca parte a operațiunilor militare, cu efecte transfrontaliere care afectează și state neimplicate direct în conflict, spre exemplu atacul cibernetic asupra rețelei de comunicații prin satelit KA-SAT, operată de compania VIASAT, ale cărui efecte s-au extins la nivel european, impactul fiind resimțit și în România,

Menționând și faptul că implicarea unor noi actori cibernetici în conflict, printre care grupuri de hackeri ce susțin una dintre tabere implicate în conflicte, precum Gruparea Killnet, au desfășurat atacuri cibernetice îndreptate împotriva infrastructurilor și serviciilor esențiale din state membre ale Uniunii Europene care sprijină Ucraina, inclusiv în România,

Ținând cont și de creșterea nivelului de digitalizare și interconectare a sistemelor informatice, coroborată cu dezvoltarea capacităților actorilor maligni din mediul online a condus la o intensificare a incidentelor care generează un impact semnificativ asupra infrastructurilor din domenii de importanță critică prin compromiterea lanțului de aprovizionare.

Evidențiind incidente majore, precum cel din primul trimestru al anului 2024, care a afectat 26 de spitale, la nivel național, prin intermediul unui furnizor de servicii gestionate, cu impact direct asupra serviciilor

vitale oferite populației, au relevat limitele acoperirii legislației actuale în domeniul securității cibernetice și nevoia de a implementa reglementările europene actualizate în ceea ce privește securitatea lanțului de aprovizionare și impunerea unor obligații, pentru managementul entităților, în vederea creșterii nivelului de reziliență al acestora, în corelare cu nivelul lor de risc în plan societal,

Având în vedere că adoptarea promptă a măsurilor și mecanismelor prevăzute de Directiva NIS2 devine imperativă pentru creșterea rezilienței României în fața amenințărilor cibernetice, dat fiind rolul crucial al acestei directive în consolidarea capacităților naționale de apărare și răspuns la incidente cibernetice și, de asemenea, aplicarea prevederilor Directivei NIS2 contribuie la alinierea României la standardele internaționale, consolidând astfel capacitatea națională de a reacționa în mod eficient în fața evoluțiilor regionale și globale din domeniul securității cibernetice,

Ținând cont de faptul că aspectele prezentate constituie o stare de fapt obiectivă, cuantificabilă, extraordinară, independentă de voința Guvernului, care pune în pericol interesul public și a cărei reglementare nu poate fi amânată,

În temeiul art. 115 alin. (4) din Constituția României, republicată,

Guvernul României adoptă prezenta ordonanță de urgență

Capitolul I – Dispoziții generale

Secțiunea 1 – Obiect și scop

Art. 1 - Prezenta ordonanță de urgență stabilește cadrul juridic și instituțional, măsurile și mecanismele necesare pentru asigurarea unui nivel comun ridicat de securitate cibernetică la nivel național.

Art. 2 - (1) Scopul prezentei ordonanțe de urgență îl constituie:

- a) Stabilirea măsurilor de gestionare a riscurilor de securitate cibernetică și a obligațiilor de raportare a incidentelor pentru entitățile esențiale și importante;
- b) Stabilirea cadrului de cooperare la nivel național și de participare la nivel european și internațional în domeniul asigurării securității cibernetice;
- c) Desemnarea Directoratului Național de Securitate Cibernetică, denumit în continuare "DNSC", ca autoritate competentă responsabilă cu securitatea cibernetică și cu sarcinile de supraveghere și asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică, precum și a altor entități de drept public sau privat cu competențe și responsabilități în aplicarea prevederilor prezentei ordonanțe de urgență;
- d) Desemnarea punctului unic de contact la nivel național și a echipei naționale de răspuns la incidente de securitate cibernetică.

(2) Prezenta ordonanță de urgență nu se aplică instituțiilor din domeniul apărării, ordinii publice și securității naționale, Ministerului Afacerilor Externe, Oficiului Registrului Național al Informațiilor Secrete de Stat, sistemelor informatice și de comunicații care vehiculează informații clasificate.

(3) Entităților cărora li se aplică Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr.

909/2014 și (UE) 2016/1011, denumit în continuare „Regulamentul DORA” le sunt incidente doar dispozițiile art. 5-10 și art. 18.

(4) Prin excepție de la alin. (2), în situația în care entități din cadrul acestora acționează drept prestator de servicii de încredere, instituțiile din domeniul apărării, ordinii publice și securității naționale, Ministerul Afacerilor Externe, precum și Oficiul Registrului Național al Informațiilor Secrete de Stat asigură obținerea unui nivel comun ridicat de securitate cibernetică prin aplicarea Legii nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.

Secțiunea a 2-a – Principii și definiții

Art. 3 - În aplicarea prezentei ordonanțe de urgență, sunt respectate următoarele principii:

- a) principiul responsabilității și conștientizării - constă în efortul continuu derulat de entitățile de drept public și privat în conștientizarea rolului și responsabilității individuale pentru atingerea unui nivel comun ridicat de securitate cibernetică la nivel național;
- b) principiul proporționalității - constă în asigurarea unui echilibru între riscurile la care rețelele și sistemele informatice sunt supuse și măsurile de securitate implementate;
- c) principiul cooperării și coordonării - constă în realizarea în timp oportun a schimbului de informații referitoare la riscurile de securitate la adresa rețelelor și sistemelor informatice și asigurarea într-o manieră sincronizată a reacției la producerea incidentelor;
- d) principiul minimizării efectelor – în cazul unui incident se iau măsuri pentru a evita amplificarea sau extinderea efectelor la alte rețele și sisteme informatice;
- e) principiul satisfacerii interesului public - se urmărește satisfacerea interesului public înaintea celui individual sau de grup.

Art. 4 - În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație:

- a) *amenințare cibernetică* înseamnă o amenințare astfel cum aceasta este definită la art. 2 lit. f) din OUG nr. 104/2021 privind Înființarea Directoratului Național de Securitate Cibernetică;
- b) *amenințare cibernetică semnificativă* înseamnă o amenințare cibernetică despre care se poate presupune, pe baza caracteristicilor sale tehnice, că are potențialul de a afecta grav rețeaua și sistemele informatice ale unei entități sau utilizatorii serviciilor furnizate de entitate, cauzând prejudicii materiale sau morale considerabile;
- c) *audit de securitate cibernetică* astfel cum este definit la art. 2 lit. d) din Legea 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative;
- d) *autoritate competentă sectorial în domeniul securității cibernetice* este acea instituție publică care are fie rol de reglementare sau rol de supraveghere și control, fie rol de reglementare, supraveghere și control în domeniile corespunzătoare sectoarelor prevăzute în anexe și care, potrivit competențelor și atribuțiilor stabilite prin actele normative de organizare și funcționare proprii, are atribuții în domeniul securității cibernetice la nivelul entităților din cadrul sectoarelor prevăzute în anexele 1 și 2;
- e) *criză cibernetică* înseamnă o stare de fapt care reprezintă o amenințare reală sau o deteriorare a unor infrastructuri cibernetice care îndeplinește cumulativ următoarele condiții:
 - 1. amenință interesele vitale ale țării sau nevoile esențiale ale populației;
 - 2. necesită decizii urgente la nivel național;
 - 3. solicită acțiuni coordonate din partea mai multor organizații și persoane.

- f) *entitate* înseamnă o persoană fizică sau juridică constituită și recunoscută ca atare în temeiul dreptului intern al locului său de stabilire care poate, acționând în nume propriu, să exercite drepturi și să fie supusă unor obligații;
- g) *entitate a administrației publice* înseamnă o autoritate sau instituție din administrația publică, potrivit prevederilor art. 5 lit. k), l), w) și kk) din OUG nr. 57/2019 privind Codul administrativ, cu modificările și completările ulterioare, precum și o unitate administrativ-teritorială, un organism de drept public sau o asociație formată din una sau mai multe astfel de autorități sau instituții din sectorul public sau din unul sau mai multe astfel de organisme de drept public;
- h) *entitate care furnizează servicii de înregistrare de nume de domenii* înseamnă un operator de registru sau un agent care acționează în numele operatorilor de registru, cum ar fi un furnizor sau un revânzător de servicii de protecție a confidențialității sau servicii de proxy;
- i) *furnizor de servicii DNS* înseamnă o entitate care furnizează:
1. servicii de rezoluție recursivă a numelor de domenii accesibile publicului pentru utilizatorii finali ai internetului;
 2. servicii de rezoluție a numelor de domenii cu autoritate destinate utilizării de către terți, cu excepția serverelor de nume rădăcină;
- j) *furnizor de servicii gestionate* înseamnă o entitate care furnizează servicii legate de instalarea, gestionarea, funcționarea sau întreținerea produselor, rețelelor, infrastructurilor sau aplicațiilor TIC sau a altor rețele și sisteme informatice, prin asistență sau administrare activă, fie la sediul clientului, fie de la distanță;
- k) *furnizor de servicii de securitate gestionate* înseamnă un furnizor de servicii gestionate care efectuează sau furnizează asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică;
- l) *gestionarea incidentului* înseamnă toate acțiunile și procedurile care vizează prevenirea, detectarea, analizarea și limitarea unui incident, sau vizează răspunsul la acesta și redresarea în urma incidentului;
- m) *incident* înseamnă un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora;
- n) *incident de securitate cibernetică de mare amploare* înseamnă un incident care provoacă perturbări care depășesc capacitățile de răspuns ale unui singur stat membru al Uniunii Europene sau care are un impact semnificativ asupra a cel puțin două state membre ale Uniunii Europene;
- o) *incident evitat la limită* înseamnă un eveniment care ar fi putut compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora, dar care a fost împiedicat cu succes să se materializeze sau care nu s-a materializat;
- p) *internet exchange point* înseamnă o facilitate a rețelei care permite interconectarea a mai mult de două rețele autonome independente, în special în scopul facilitării schimbului de trafic de internet, care furnizează interconectare doar pentru sisteme autonome și care nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre orice pereche de sisteme autonome participante și nici nu modifică sau interacționează într-un alt mod cu acest trafic;
- q) *motor de căutare online* înseamnă un motor de căutare online astfel cum este definit la articolul 2 punctul 5 din Regulamentul (UE) 2019/1150 al Parlamentului European și al Consiliului din 20 iunie 2019 de promovare a echității și a transparenței pentru întreprinderile utilizatoare de servicii de intermediere online;
- r) *organism de cercetare* înseamnă o entitate al cărei obiectiv principal este de a desfășura activități de cercetare aplicată sau de dezvoltare experimentală în vederea exploatării rezultatelor cercetării respective în scopuri comerciale, dar care nu include instituțiile de învățământ;

s) *organism de evaluare a conformității* înseamnă organismul menționat la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93;

t) *organism național de acreditare* înseamnă organismul menționat la articolul 2 punctul 11 din Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 al Consiliului, "Regulamentul (CE) nr. 765/2008";

u) *piață online* înseamnă serviciu digital care permite consumatorilor și/sau comercianților să încheie cu comercianții vânzări online sau contracte de servicii, fie pe site-ul internet al pieței online, fie pe site-ul internet al unui comerciant care utilizează servicii informatice furnizate de piața online;

v) *platformă de servicii de socializare în rețea* înseamnă o platformă care permite utilizatorilor finali să se conecteze, să partajeze, să descopere și să comunice între ei pe mai multe dispozitive, inclusiv prin conversații online, postări, videoclipuri și recomandări;

w) *politica de securitate a sistemelor și rețelelor informatice* înseamnă o politică care stabilește măsurile de securitate pentru rețelele și sistemele informatice care trebuie adoptate de o entitate esențială sau importantă;

x) *prestator de servicii de încredere* înseamnă un prestator de servicii de încredere în sensul articolul 3 alineatul (19) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE;

y) *prestator de servicii de încredere calificat* înseamnă un prestator de servicii de încredere calificat în sensul articolului 3 punctul 20 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE;

z) *proces TIC* înseamnă un proces TIC în sensul articolului 2 punctul 14 din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică);

aa) *produs TIC* înseamnă un produs TIC în sensul articolului 2, pct. 12), din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică);

bb) *registru de nume TLD* înseamnă o entitate căreia i-a fost delegat un anumit domeniu de prim nivel și care răspunde de administrarea domeniului de prim nivel, inclusiv de înregistrarea numelor de domenii sub domeniul de prim nivel și de operarea tehnică a domeniului de prim nivel, inclusiv exploatarea serverelor sale de nume, întreținerea bazelor sale de date și distribuirea fișierelor zonelor de domenii de prim nivel către serverele de nume, indiferent dacă este efectuată de entitatea însăși sau externalizată, dar excluzând situațiile în care numele de domenii de prim nivel sunt utilizate de un registru exclusiv pentru uz propriu;

cc) *reprezentant* înseamnă o persoană fizică sau juridică stabilită în Uniunea Europeană care este desemnată în mod expres să acționeze în numele unui furnizor de servicii DNS, al unui registru TLD, al unei entități care furnizează servicii de înregistrare a numelor de domenii, al unui furnizor de cloud computing, al unui furnizor de servicii de centre de date, un furnizor de rețele de difuzare de conținut, un furnizor de servicii gestionate, un furnizor de servicii de securitate gestionată, o piață online, un motor de

căutare online sau un furnizor de platforme de comunicare socială care nu este stabilit în Uniunea Europeană, care poate fi contactat de autoritatea națională de securitate cibernetică sau CSIRT în locul entității în sine în legătură cu obligațiile entității respective în temeiul dispozițiilor prezentei ordonanțe de urgență;

dd) *rețea de difuzare de conținut* înseamnă o rețea de servere distribuite geografic concepută pentru a asigura disponibilitatea ridicată, accesibilitatea sau furnizarea rapidă de conținut și servicii digitale utilizatorilor de internet în numele furnizorilor de conținut și servicii;

ee) *rețea publică de comunicații electronice* înseamnă o rețea publică de comunicații electronice în sensul articolului 4 alin. (1) punctul 10 din OUG nr. 111/2011 privind comunicațiile electronice;

ff) *rețea și sistem informatic* înseamnă:

1. rețea de comunicații electronice în sensul prevederilor art. 4 alin. (1) pct. 6 din OUG nr. 111/2011 privind comunicațiile electronice;

2. orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, 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 și 2 în vederea funcționării, utilizării, protejării și întreținerii lor.

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

hh) *securitate cibernetică* înseamnă securitate cibernetică astfel cum aceasta este definită la art. 2 lit. y) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative;

ii) *securitatea rețelelor și a sistemelor informatice* înseamnă capacitatea rețelelor și a sistemelor informatice de a rezista, la un anumit nivel de încredere, oricărui eveniment care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate sau a serviciilor furnizate de aceste rețele și sisteme informatice puse la dispoziție;

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

1. piață online;

2. motor de căutare online;

3. serviciu de cloud computing.

kk) *serviciu de centre de date* înseamnă un serviciu care include structuri sau grupuri de structuri, dedicat găzduirii, interconectării și exploatarea centralizată a echipamentelor informatice și de rețea care furnizează servicii de stocare, prelucrare și transport al datelor, precum și a tuturor instalațiilor și infrastructurii de distribuție a energiei electrice și de control al mediului;

ll) *serviciu de cloud computing* înseamnă un serviciu digital care permite administrarea la cerere și accesul larg de la distanță la un set scalabil și variabil de resurse informatice care pot fi partajate, inclusiv în cazul în care resursele respective sunt repartizate în diferite locații;

mm) *serviciu de comunicații electronice* înseamnă un serviciu de comunicații electronice în sensul articolului 4 alin. (1) punctul 9 din OUG nr. 111/2011 privind comunicațiile electronice;

nn) *serviciu de încredere* înseamnă un serviciu de încredere în sensul articolului 3 punctul 16 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE ("Regulamentul eIDAS");

oo) *serviciu de încredere calificat* înseamnă un serviciu de încredere calificat în sensul articolului 3 punctul 17 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE ("Regulamentul eIDAS");

pp) *serviciu TIC* înseamnă un serviciu TIC în sensul articolului 2, pct.13) din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică);

qq) *sistem de nume de domenii sau DNS* înseamnă un sistem de denumire ierarhic și distribuit care permite identificarea serviciilor și resurselor de internet, care permite dispozitivelor utilizatorilor finali să utilizeze servicii de rutare și conectivitate a internetului pentru a accesa aceste servicii și resurse;

rr) *specificație tehnică* înseamnă o specificație tehnică astfel cum este definită la art. 2 punctul 4 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și 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 și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului;

ss) *standard* înseamnă un standard în sensul art. 2 alin. (1) din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și 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 și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului;

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

Capitolul II - Domeniul de aplicare

Secțiunea 1 - Entități esențiale

Art. 5 – (1) Următoarele entități sunt considerate esențiale, indiferent de dimensiunea pe care o au:

- a) entitățile administrației publice centrale;
- b) entitățile din anexele 1 și 2 identificate în conformitate cu art. 9;
- c) entitățile identificate drept entități critice conform dispozițiilor Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului;
- d) furnizorii de servicii DNS;
- e) furnizorii de servicii de încredere calificați;
- f) registrele de nume TLD.

(2) Sunt considerate esențiale, entitățile din categoria întreprinderilor mari conform art. 8 și care se încadrează în sectoarele prevăzute în anexa 1.

(3) Sunt considerate esențiale, entitățile din categoria întreprinderilor mijlocii conform art. 8 și care sunt furnizori de rețele publice de comunicații electronice sau furnizori de servicii de comunicații electronice accesibile publicului.

(4) Sunt considerate esențiale, entitățile din categoria întreprinderilor mijlocii conform art. 8 și care sunt furnizori de servicii de securitate gestionate.

Secțiunea a 2-a - Entități importante

Art. 6 – (1) Sunt considerate entități importante, entitățile din categoriile întreprinderilor mari și mijlocii conform art. 8, care se încadrează în anexele 1 și 2 și care nu sunt identificate drept entități esențiale conform art. 5.

(2) Următoarele entități sunt considerate importante dacă nu au fost identificate drept entități esențiale conform art. 5 și indiferent de dimensiunea pe care o au:

- a) entitățile din anexele 1 și 2 identificate în conformitate cu art. 9;
- b) furnizorii de rețele publice de comunicații electronice și furnizorii de servicii de comunicații accesibile publicului;
- c) furnizorii de servicii de încredere.

Secțiunea a 3-a - Dispoziții speciale

Art. 7 – (1) Entitățile care intră în domeniul de aplicare al prezentei ordonanțe de urgență sunt entitățile din sectoarele prevăzute în anexele 1 și 2, înființate și înregistrate pe teritoriul României conform prevederilor legale.

(2) Furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului intră în domeniul de aplicare al prezentei ordonanțe de urgență atunci când prestează servicii pe teritoriul României.

(3) Furnizorii de servicii DNS, registrele de nume TLD, entitățile care furnizează servicii de înregistrare a numelor de domenii, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, precum și furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea intră în domeniul de aplicare al prezentei ordonanțe de urgență atunci când sediul principal al acestora din Uniunea Europeană este situat pe teritoriul României.

(4) Entitățile administrației publice străine sunt în jurisdicția statului care le-a instituit.

(5) În înțelesul prezentei ordonanțe de urgență, sediul principal astfel cum este menționat la alin. (3), se determină astfel:

- a) este sediul în care se iau deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică în mod predominant;
- b) atunci când nu se poate stabili sediul principal conform lit. a), se consideră a fi sediul în care își desfășoară operațiunile de securitate cibernetică;
- c) atunci când nu se poate stabili sediul principal conform lit. b), acesta este considerat a fi în statul în care entitatea în cauză își are sediul cu cel mai mare număr de angajați.

(6) Atunci când, în situația descrisă la alin. (3), entitatea nu este stabilită în Uniunea Europeană, dar oferă servicii pe teritoriul acesteia, entitatea este obligată să desemneze un reprezentant în Uniunea Europeană, în cadrul unuia dintre statele membre în care își prestează serviciile.

(7) Atunci când entitatea nu a desemnat un reprezentant conform alin. (6) și prestează servicii pe teritoriul României, DNSC poate introduce acțiuni în justiție conform prevederilor legale împotriva entității în cauză pentru nerespectarea prevederilor prezentei ordonanțe de urgență.

Art. 8 – (1) O entitate este considerată întreprindere mare dacă depășește criteriile stabilite pentru întreprinderile mijlocii astfel cum sunt prevăzute la art. 4 alin. (1) lit. c) din Legea nr. 346/2004 privind stimularea înființării și dezvoltării întreprinderilor mici și mijlocii, cu modificările și completările ulterioare.

(2) O entitate este considerată întreprindere mijlocie dacă îndeplinește criteriile prevăzute la art. 4 alin. (1) lit. c) din Legea nr. 346/2004 privind stimularea înființării și dezvoltării întreprinderilor mici și mijlocii, cu modificările și completările ulterioare.

Art. 9 – O entitate este considerată esențială sau importantă, dacă:

- a) entitatea este singurul furnizor al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice;
- b) perturbarea serviciului furnizat de entitate ar putea avea un impact semnificativ asupra siguranței publice, a securității publice sau a sănătății publice;
- c) perturbarea serviciului furnizat de entitate ar putea genera un risc sistemic semnificativ, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier;
- d) entitatea este critică datorită importanței sale specifice la nivel național sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente.

Art. 10 – (1) Determinarea impactului generat de perturbarea serviciului furnizat de entitate, prevăzut de art. 9, se realizează în funcție de:

- a) impactul asupra drepturilor și libertăților fundamentale;
- b) impactul asupra economiei naționale;
- c) impactul asupra sănătății și vieții persoanelor;
- d) impactul financiar;
- e) impactul asupra apărării, ordinii publice și securității naționale;
- f) impactul trans-sectorial sau transfrontalier.

(2) Criteriile prevăzute la alin. (1), pragurile corespunzătoare acestora și metodologia de evaluare a nivelului de risc al entităților se stabilesc prin ordin al Directorului DNSC.

Capitolul III - Măsuri de gestionare a riscurilor de securitate cibernetică și obligații de raportare

Art. 11 – (1) Entitățile esențiale și entitățile importante iau măsuri tehnice, operaționale și organizatorice proporționale și adecvate pentru a identifica, evalua și gestiona riscurile aferente securității rețelelor și a sistemelor informatice pe care acestea le utilizează în desfășurarea activităților lor sau furnizarea serviciilor lor, precum și pentru a elimina sau, după caz, a reduce efectele incidentelor asupra destinatarilor serviciilor lor și asupra altor servicii.

(2) Măsurile prevăzute la alin. (1) trebuie să asigure un nivel de securitate cibernetică adecvat nivelului de risc al entității, ținând seama de stadiul actual al tehnologiei și, după caz, de cele mai relevante standarde și bune practici naționale, europene și internaționale, cât și de costurile de punere în aplicare a acestor măsuri.

(3) Nivelul de risc al entității se evaluează conform metodologiei de evaluare a nivelului de risc cuprinse în ordinul Directorului DNSC prevăzut la art. 10 alin. (2).

(4) Măsurile prevăzute la alin. (1) trebuie să cuprindă o abordare cuprinzătoare a amenințărilor cibernetice în vederea asigurării protecției rețelelor și a sistemelor informatice, atât la nivel logic, cât și fizic, împotriva incidentelor, inclusiv prin jurnalizarea și asigurarea trasabilității tuturor activităților în cadrul rețelelor și sistemelor informatice.

(5) Entitățile esențiale și entitățile importante sunt obligate să se supună efectuării unui audit de securitate cibernetică în condițiile și cu periodicitatea stabilite prin ordinul Directorului DNSC prevăzut la art. 12 alin. (1), în funcție de nivelul de risc prevăzut la alin. (3).

(6) Atunci când există autoritatea cu competențe sectoriale, condițiile și periodicitatea auditului de securitate prevăzute la alin. (5) vor fi stabilite prin ordin comun în condițiile art. 37 alin. (8) lit. b), în funcție de nivelul de risc prevăzut la alin. (3).

(7) Entitățile esențiale și importante pun la dispoziția DNSC, la cerere, lista activelor relevante și lista riscurilor identificate în urma analizei riscurilor, prevăzută la alin. (1).

(8) Cu privire la securitatea lanțului de aprovizionare, măsurile prevăzute la alin. (1) trebuie să țină seama de:

a) vulnerabilitățile specifice ale fiecărui furnizor direct și ale fiecărui furnizor de servicii, de calitatea generală a produselor și de calitatea practicilor de securitate cibernetică ale furnizorilor direcți și ale furnizorilor de servicii, inclusiv de securitatea proceselor de dezvoltare ale acestora;

b) rezultatele evaluărilor coordonate ale riscurilor efectuate care au în vedere rezultatele evaluărilor coordonate ale riscurilor de securitate a lanțurilor critice de aprovizionare elaborate la nivelul Uniunii Europene în cadrul Grupului de cooperare.

(9) În vederea asigurării securității lanțului de aprovizionare, entitățile esențiale și entitățile importante au obligația să transmită către DNSC, la cerere, date cu privire la furnizorii de servicii de încredere, furnizorii de servicii de încredere calificați, furnizorii de servicii DNS, registrele de nume TLD sau entitățile care oferă servicii de înregistrare nume de domenii, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate și care le asigură aceste tipuri de servicii.

(10) Atunci când este evaluată proporționalitatea măsurilor de gestionare a riscurilor în conformitate cu alin. (1), se ține seama în mod corespunzător de amploarea expunerii la riscuri a entității și a serviciilor pe care le furnizează, de dimensiunea entității, de probabilitatea producerii unor incidente și de gravitatea acestora, inclusiv de impactul lor social și economic.

Art. 12 - (1) Directorul DNSC emite un ordin privind măsurile de gestionare a riscurilor prevăzute la art. 11 alin. (1) în ceea ce privește cerințele tehnice, operaționale și organizatorice, conform art. 13.

(2) Ordinul emis conform alin. (1) poate include și cerințe sectoriale specifice pentru aceste măsuri de gestionare a riscurilor ca urmare a consultării autorităților competente la nivel sectorial cu atribuții de reglementare.

(3) În cazul în care organele de conducere ale entităților esențiale și ale entităților importante constată că nu respectă măsurile prevăzute în ordinul de la alin. (1), acestea aplică, fără întârzieri nejustificate, măsurile corective necesare.

(4) Entitățile esențiale și entitățile importante realizează și transmit către DNSC, anual, o autoevaluare a nivelului de maturitate a măsurilor de gestionare a riscurilor de securitate cibernetică conform ordinului prevăzut la alin. (1), asumată de managementul entității.

(5) Entitățile esențiale întocmesc și transmit către DNSC, în termen de 30 de zile de la realizarea autoevaluării, un plan de măsuri pentru remedierea deficiențelor identificate, asumat de managementul entității, în conformitate cu măsurile de gestionare a riscurilor aplicabile acestora.

Art. 13 – Măsurile prevăzute la art. 11 alin. (1) cuprind cel puțin următoarele:

a) politicile și procedurile referitoare la analiza riscurilor și la securitatea sistemelor informatice și revizuirea periodică a acestora;

b) politicile și procedurile de evaluare a eficacității măsurilor de gestionare a riscurilor de securitate cibernetică;

c) politicile și procedurile referitoare la utilizarea criptografiei și, după caz, a criptării;

d) securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitatea relației dintre entitate și prestatorii și furnizorii săi direcți;

- e) securitatea achiziției, dezvoltării, întreținerii și casării rețelelor și sistemelor informatice, inclusiv gestionarea și divulgarea vulnerabilităților;
- f) securitatea resurselor umane, politicile de control al accesului și gestionarea activelor;
- g) gestionarea incidentelor;
- h) continuitatea activității, inclusiv gestionarea copiilor de rezervă, redresarea în caz de dezastru și managementul crizelor;
- i) practicile de bază în materie de igienă cibernetică și formarea în domeniul securității cibernetice;
- j) utilizarea soluțiilor de autentificare multi-factor sau de autentificare continuă a comunicațiilor vocale, video și text, a sistemelor de comunicații de urgență securizate și securizate în interiorul entității, după caz.

Art. 14 – (1) Organele de conducere ale entităților esențiale și ale entităților importante aprobă măsurile de gestionare a riscurilor de securitate cibernetică pe care le iau în vederea respectării art. 11-13, supraveghează punerea acestora în aplicare și sunt responsabile de încălcările acestor dispoziții, fără a aduce atingere dispozițiilor legale privind răspunderea instituțiilor publice, a funcționarilor publici și a celor aleși sau numiți.

(2) Membrii organelor de conducere ale entităților esențiale și ale entităților importante urmează cursuri de formare profesională în vederea asigurării unui nivel suficient de cunoștințe și competențe pentru a identifica riscurile și a evalua practicile de gestionare a riscurilor de securitate cibernetică, precum și impactul acestora asupra serviciilor furnizate de entitate.

(3) Organele de conducere ale entităților esențiale și ale entităților importante stabilesc mijloacele permanente de contact, asigură alocarea resurselor necesare pentru punerea în aplicare a măsurilor de gestionare a riscurilor de securitate cibernetică și, după caz, desemnează responsabilii cu securitatea rețelelor și sistemelor informatice care au rolul de a implementa și supraveghea măsurile de gestionare a riscurilor de securitate cibernetică la nivelul entității.

(4) Persoana responsabilă cu securitatea rețelelor și sistemelor informatice, prevăzută la alin. (3), desemnată în cadrul entităților esențiale, cu excepția entităților administrației publice, precum și a microîntreprinderilor și întreprinderilor mici, astfel cum sunt stabilite conform dispozițiilor art. 4 alin. (1) lit. a) din Legea nr. 346/2004 privind stimularea înființării și dezvoltării întreprinderilor mici și mijlocii, cu modificările și completările ulterioare, trebuie să îndeplinească cumulativ cel puțin următoarele:

- a) are autoritate managerială;
- b) este subordonată direct organelor de conducere ale entității;
- c) funcționează independent de structurile IT și de tehnologie operațională din cadrul entității;
- d) are acces la resursele necesare pentru supravegherea și implementarea eficientă a măsurilor de gestionare a riscurilor de securitate cibernetică.

Art. 15 – (1) Entitățile esențiale și entitățile importante raportează, fără întârzieri nejustificate, echipei de răspuns la incidente de securitate cibernetică naționale orice incident care are un impact semnificativ asupra prestării serviciilor lor și, dacă este cazul, entitățile în cauză notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor, incidentele semnificative care ar putea afecta prestarea serviciilor respective.

(2) Raportarea se face prin intermediul Platformei naționale pentru raportarea incidentelor de securitate cibernetică, denumită în continuare PNRISC, astfel cum este prevăzută la art. 20 din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.

(3) Entitățile esențiale și entitățile importante raportează orice informație care îi permite echipei de răspuns la incidente de securitate cibernetică naționale să constate un impact transfrontalier al incidentului. Simpla raportare nu expune entitatea unei răspunderi sporite.

(4) În cazul unui incident semnificativ transfrontalier, punctul unic de contact național se asigură că autoritățile omoloage din statele respective primesc în timp util informațiile relevante raportate conform alin. (7).

(5) Dacă este cazul, entitățile esențiale și entitățile importante comunică, fără întârzieri nejustificate, destinatarilor serviciilor lor care ar putea fi afectați de o amenințare cibernetică semnificativă orice măsuri sau măsuri corective pe care destinatarii respectivi le pot lua ca răspuns la amenințarea respectivă și, după caz, entitățile informează, de asemenea, destinatarii în cauză despre amenințarea semnificativă propriu-zisă.

(6) Un incident este considerat semnificativ dacă:

a) a provocat sau poate provoca perturbări operaționale grave ale serviciilor sau pierderi financiare pentru entitatea în cauză;

b) a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau non-materiale considerabile.

(7) În scopul notificării în temeiul alin. (1), entitățile în cauză transmit echipei de răspuns la incidente de securitate cibernetică naționale:

a) în termen de 24 de ore de la data la care au luat cunoștință de incidentul semnificativ, o avertizare timpurie care, după caz, indică dacă există suspiciuni că incidentul este cauzat de acțiuni ilicite sau răuvoitoare sau că ar putea avea un impact transfrontalier;

b) în termen de 72 de ore din momentul în care au luat cunoștință de incidentul semnificativ, o raportare a incidentului, care, după caz, actualizează informațiile menționate la lit. a) și prezintă o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili;

c) un raport intermediar privind actualizarea relevantă a situației, la cererea echipei de răspuns la incidente de securitate cibernetică naționale;

d) un raport final, în termen de cel mult 30 de zile de la transmiterea notificării incidentului în temeiul lit.

b), care să includă cel puțin următoarele elemente:

1. o descriere detaliată a incidentului, inclusiv a gravității și a impactului acestuia;

2. tipul de amenințare sau de cauză principală care probabil că a declanșat incidentul;

3. măsurile de atenuare aplicate și în curs;

4. dacă este cazul, impactul transfrontalier al incidentului.

e) în cazul unui incident în desfășurare la momentul prezentării raportului menționat la lit. d), entitățile în cauză prezintă un raport privind progresele înregistrate și un raport final în termen de 30 de zile de la gestionarea incidentului.

(8) Prin excepție de la alin. (7) lit. b), un prestator de servicii de încredere notifică, în ceea ce privește incidentele semnificative care afectează prestarea serviciilor sale de încredere, echipei de răspuns la incidente de securitate cibernetică naționale, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care a luat cunoștință de incidentul semnificativ.

(9) Echipa de răspuns la incidente de securitate cibernetică națională furnizează, fără întârzieri nejustificate și, atunci când este posibil, în termen de 24 de ore de la primirea avertizării timpurii conform alin. (7) lit. a), un răspuns entității raportoare, inclusiv un răspuns inițial cu privire la incidentul semnificativ și, la cererea entității, orientări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de atenuare.

(10) Echipa de răspuns la incidente de securitate cibernetică națională poate să furnizeze sprijin tehnic suplimentar în cazul în care entitatea în cauză solicită acest lucru. În cazul în care se apreciază că incidentul este de natură penală, echipa de răspuns la incidente de securitate cibernetică națională furnizează, de asemenea, orientări privind sesizarea incidentului către organele de urmărire penală.

(11) După caz, și în special dacă incidentul semnificativ implică două sau mai multe state, DNSC informează celelalte state afectate și Agenția Uniunii Europene pentru Securitate Cibernetică, denumită în continuare „ENISA”, cu privire la incidentul semnificativ. Aceste informații includ tipul de informații primite conform alin. (7).

(12) În cazul alin. (11), DNSC, în conformitate cu legislația națională și normele Uniunii Europene, protejează interesele de securitate și pe cele comerciale ale entității, precum informațiile privilegiate, datele legate de afacere sau cele corporative și asigură confidențialitatea informațiilor furnizate.

(13) În cazul în care informarea publicului este necesară pentru a preveni un incident semnificativ sau pentru a gestiona un incident semnificativ în curs sau în cazul în care divulgarea incidentului semnificativ este în alt mod în interesul public, DNSC sau, după caz, DNSC împreună cu autoritățile omoloage din alte state în cauză pot, după consultarea entității respective, să informeze publicul cu privire la incidentul semnificativ sau să solicite entității să facă acest lucru.

(14) Punctul unic de contact național, înaintează, după caz, raportările primite conform alin. (1) punctelor unice de contact din celelalte state membre afectate.

(15) Punctul unic de contact național transmite către ENISA, o dată la 90 de zile, un raport de sinteză care include date anonimizate agregate privind incidentele semnificative, incidentele, amenințările cibernetice și incidentele evitate la limită raportate conform alin. (1) și cu cele privind raportarea voluntară.

(16) DNSC furnizează Centrului Național de Coordonare a Protecției Infrastructurilor Critice, denumit în continuare „CNCPIC”, informații cu privire la incidentele semnificative, incidentele, amenințările cibernetice și incidentele evitate la limită raportate conform alin. (1) și cu prevederile privitoare la raportarea voluntară de către entitățile identificate ca fiind entități critice în temeiul Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului.

(17) Prin ordin al Directorului DNSC se stabilesc norme metodologice privind raportarea incidentelor.

Art. 16 - (1) Pot raporta către echipa de răspuns la incidente de securitate cibernetică națională:

a) entitățile esențiale și entitățile importante, cu privire la incidente, amenințări cibernetice și incidente evitate la limită;

b) alte entități decât cele menționate la lit. a), indiferent dacă intră în domeniul de aplicare al prezentei ordonanțe de urgență, cu privire la incidente semnificative, amenințări cibernetice și incidente evitate la limită.

(2) Raportarea voluntară menționată la alin. (1) se realizează în conformitate cu art. 15.

(3) Echipa de răspuns la incidente de securitate cibernetică națională prelucrează cu prioritate notificările obligatorii atunci când consideră necesar.

(4) Raportarea voluntară nu impune entității notificatoare nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis raportarea.

Art. 17 - Prin excepție de la dispozițiile art. 21 alin. (1) și (2) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, persoanele prevăzute la art. 3 alin. (1) lit. b) și c) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative care sunt identificate ca fiind entități esențiale și entități importante, aplică art. 15 și 16 privind raportarea incidentelor.

Capitolul IV – Înregistrare

Secțiunea 1 - Registrul entităților

Art. 18 - (1) DNSC păstrează un registru al entităților esențiale și al entităților importante identificate.

(2) Entitățile care desfășoară activitate în sectoarele din anexele 1 și 2, notifică DNSC în vederea înregistrării în cel mult 30 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență sau în termen de cel mult 30 zile de la data la care prevederile prezentei ordonanțe de urgență le sunt aplicabile, atunci când, conform art. 5 și art. 6, se încadrează ca entități esențiale sau entități importante.

(3) Notificarea de la alin. (2), constă în furnizarea către DNSC a următoarelor tipuri de informații:

a) denumirea;

b) adresa sediului social principal și datele de contact actualizate, inclusiv adresele de e-mail și numerele de telefon;

c) adresele celorlalte sedii sociale din Uniunea Europeană, după caz;

d) mijloacele permanente de contact și persoana din cadrul entității însărcinată cu monitorizarea mijloacelor de contact;

e) persoana desemnată în calitate de reprezentant al entității, adresa și datele de contact ale acesteia, dacă entitatea nu este stabilită în Uniunea Europeană;

f) sectorul, subsectorul și tipul de entitate, astfel cum acestea se încadrează în anexa 1 sau în anexa 2;

g) statele membre în care prestează servicii, după caz;

h) intervalele de adrese IP publice ale entității, în cazul furnizorilor de servicii DNS, registrelor de nume TLD, entităților care furnizează servicii de înregistrare a numelor de domenii, furnizorilor de servicii de cloud computing, operatorilor de rețele de livrare de conținut, furnizorilor de servicii de centre de date, furnizorilor de servicii gestionate, furnizorilor de servicii de securitate gestionate și furnizorilor de servicii digitale;

i) intervalele de adrese IP publice ale entității, pentru alte entități decât cele prevăzute la lit. h), după caz;

j) informații necesare și suficiente din care să rezulte îndeplinirea condițiilor pentru identificarea drept entitate esențială sau entitate importantă conform art. 5 și respectiv art. 6.

(4) În termen de 60 de zile de la primirea notificării prevăzute la alin. (2), conducerea DNSC emite o decizie pentru identificarea și înscrierea în registru a entităților esențiale.

(5) În termen de 150 de zile de la primirea notificării, conducerea DNSC emite o decizie pentru identificarea și înscrierea în registru a entităților importante.

(6) În termen 60 de zile de la data comunicării deciziei Directorului DNSC prevăzute la alin. (4), respectiv alin. (5), entitățile esențiale și entitățile importante transmit către DNSC evaluarea nivelului de risc a entității în conformitate cu art. 10 alin. (2).

(7) În termen de 60 de zile de la transmiterea evaluării nivelului de risc prevăzute la alin. (6), entitățile realizează o autoevaluare a nivelului de maturitate prevăzută la art. 12 alin. (4).

(8) Entitățile prevăzute la alin. (2) comunică DNSC modificările aduse informațiilor prevăzute la alin. (3), astfel:

a) pentru informațiile prevăzute la alin. (3) lit. a)-d), lit. f) și lit. j), fără întârzieri nejustificate și în orice caz în termen de cel mult 15 zile de la data modificării;

b) pentru informațiile prevăzute la alin. (3) lit. e) și lit. g)-i), fără întârzieri nejustificate și în orice caz în termen de cel mult 90 zile de la data modificării.

(9) Prin ordin al Directorului DNSC, se stabilesc cerințele privind alin. (3), inclusiv metoda de transmitere a informațiilor și utilizarea unor formulare.

(10) Punctul unic de contact național transmite în legătură cu furnizorii de servicii DNS, registrele de nume TLD, entitățile care furnizează servicii de înregistrare a numelor de domenii, furnizorii de servicii

de cloud computing, operatorii de rețele de livrare de conținut, furnizorii de servicii de centre de date, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate și furnizorii de servicii digitale, informațiile prevăzute la alin. (3) către ENISA după primirea acestora, cu excepția informațiilor cuprinse în alin. (3) lit. i) și lit. j) până cel târziu la 17 ianuarie 2025 și ori de câte ori intervin modificări în legătură cu acestea.

(11) Entitatea se asigură că poate fi contactată prin intermediul datelor de contact transmise în conformitate cu alin. (3).

(12) După expirarea termenului prevăzut la alin. (12), DNSC, din oficiu sau în urma unei sesizări privind sustragerea de la o obligație de notificare și înscriere în registru făcută de orice persoană interesată, notifică entitatea în cauză cu privire la respectarea obligației de a se supune procesului de identificare în vederea înscrierii în registrul entităților esențiale sau importante conform alin. (2).

(13) Entitățile care nu mai îndeplinesc condițiile și criteriile prevăzute de dispozițiile prezentei ordonanțe de urgență, notifică DNSC în vederea radierei din registru și furnizează acte doveditoare pentru aceasta în termen de 30 de zile de la data la care se constată schimbările.

(14) DNSC dispune, prin decizie a conducerii, radierea din registru, în urma evaluării documentațiilor prevăzute la alin. (13) și comunică entității decizia.

(15) Entitățile pot solicita asistența DNSC cu privire la procesul de identificare, modificare sau radiere.

(16) Atunci când o entitate furnizează un serviciu esențial și în cadrul altor state membre ale Uniunii Europene, DNSC se consultă cu autoritățile omoloage din statele respective înainte de adoptarea unei decizii privind radierea.

(17) Se pot înregistra la DNSC și alte entități decât cele menționate la alin. (2), indiferent de dimensiunea acestora, în conformitate cu alin. (2)-(16).

Art. 19 - (1) Pentru a contribui la securitatea, stabilitatea și reziliența sistemelor de nume de domenii, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii depun diligențele necesare pentru a colecta date exacte și complete de înregistrare a numelor de domenii într-o bază de date dedicată, în conformitate cu dreptul Uniunii privind protecția datelor.

(2) O bază de date conform alin. (1) conține informațiile necesare pentru identificarea și contactarea titularilor de nume de domenii și a punctelor de contact care administrează numele de domenii în TLD și trebuie să includă următoarele:

a) numele de domeniu;

b) data înregistrării;

c) numele, adresa de e-mail și numărul de telefon ale solicitantului înregistrării;

d) adresa de e-mail de contact și numărul de telefon ale punctului de contact care administrează numele de domeniu, dacă sunt diferite de cele ale solicitantului înregistrării.

(3) Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii stabilesc politici și proceduri, inclusiv proceduri de verificare, pentru a se asigura că bazele de date menționate la alin. (1) conțin informații exacte și complete și pun la dispoziția publicului aceste politici și proceduri.

(4) Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pun la dispoziția publicului datele de înregistrare a numelor de domenii fără caracter personal imediat după înregistrarea unui nume de domeniu.

(5) În măsura în care datele furnizate de titularul numelui de domeniu sunt incorecte, inexacte sau incomplete, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domeniu notifică aceasta titularului dreptului de utilizare a numelui de domeniu pentru a pune la dispoziție datele corecte, exacte și complete în termenul comunicat.

(6) Dacă termenul acordat conform alin. (5) nu este respectat, numele de domeniu este blocat.

- (7) Transferul unui nume de domeniu blocat este interzis, iar atunci când datele solicitate nu au fost corectate corespunzător, numele de domeniu este anulat.
- (8) Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii oferă acces la datele solicitate de înregistrare a numelor de domenii, în baza unor cereri legal întemeiate și motivate corespunzător, persoanelor care justifică un interes legitim conform dispozițiilor legale.
- (9) Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pun la dispoziția publicului politicile și procedurile privind divulgarea datelor conform alin. (5) și răspund la toate cererile de acces cu celeritate și, în orice caz, în termen de 72 de ore de la primirea unei cereri.
- (10) Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii cooperează între ele.
- (11) DNSC poate solicita motivat accesul la datele de înregistrare a numelor de domenii și poate încheia protocoale corespunzătoare cu operatorii de registru TLD și cu furnizorii de servicii de înregistrare a numelor de domenii.

Secțiunea a 2-a - Schimbul de informații în materie de securitate cibernetică

Art. 20 – (1) Entitățile esențiale, entitățile importante și, după caz, alte entități pot face schimb reciproc de informații relevante în materie de securitate cibernetică, în mod voluntar, inclusiv de informații referitoare la amenințări ciberneticе, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor ciberneticе.

(2) Schimbul de informații prevăzut la alin. (1) se realizează în cadrul unor comunități ale entităților esențiale și ale entităților importante și, după caz, ale prestatorilor sau furnizorilor lor de servicii, prin intermediul unor acorduri privind schimbul de informații în materie de securitate cibernetică.

(3) Schimbul de informații se realizează în următoarele scopuri:

- a) prevenirea și detectarea incidentelor, răspunsul la incidente sau redresarea în urma acestora sau atenuarea impactului lor;
- b) sporirea nivelului de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările ciberneticе, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de limitare și prevenire a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare sau promovarea colaborării dintre entitățile publice și private în domeniul cercetării amenințărilor ciberneticе.

(4) Acordurile privind schimbul de informații în materie de securitate cibernetică cuprind și informații cu privire la elemente operaționale, inclusiv utilizarea platformelor TIC dedicate și a instrumentelor de automatizare, conținutul și condițiile acordurilor privind schimbul de informații și se notifică DNSC atât încheierea, cât și retragerea din cadrul acestora.

(5) DNSC poate sprijini entitățile interesate în încheierea unui acord privind schimbul de informații în materie de securitate cibernetică și poate solicita limitarea schimbului de informații atunci când acestea fac referire la informațiile puse la dispoziție de autorități competente sau de echipele de răspuns la incidente de securitate cibernetică.

Capitolul III - Roluri și responsabilități

Secțiunea 1 - Coordonare la nivel național

Art. 21 - (1) Viziunea, principalele linii directoare și abordările generale privind domeniul securității cibernetice la nivel național sunt definite și asumate în Strategia de Securitate Cibernetică a României, aprobată prin Hotărârea de Guvern nr. 1.321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, denumită în continuare „Strategia” și în Planul de acțiune pentru implementarea acesteia.

(2) Cadrul general de cooperare în domeniul securității cibernetice la nivel național este Sistemul Național de Securitate Cibernetică, denumit în continuare „SNSC”, în conformitate cu dispozițiile Legii nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.

Art. 22 - (1) Strategia națională de securitate cibernetică este elaborată de către DNSC, cu avizul COSC și este adoptată prin hotărâre a Guvernului, împreună cu planul de acțiune pentru implementarea strategiei, care este anexă la aceasta.

(2) În elaborarea strategiei naționale de securitate cibernetică, DNSC poate solicita asistența ENISA.

(3) Strategia națională de securitate cibernetică prevede obiectivele strategice, resursele necesare pentru atingerea obiectivelor respective și măsurile de politică și de reglementare adecvate în vederea atingerii și menținerii unui nivel ridicat de securitate cibernetică.

(4) Strategia națională de securitate cibernetică este evaluată periodic și cel puțin o dată la cinci ani, pe baza indicatorilor-cheie de performanță și, dacă este necesar, este actualizată și adoptată, urmând același mecanism.

(5) În termen de 90 de zile de la data adoptării strategiei naționale de securitate cibernetică, DNSC transmite Comisiei Europene aceasta.

Art. 23 - (1) Strategia națională de securitate cibernetică elaborată conform art. 22 cuprinde cel puțin următoarele:

a) obiectivele și prioritățile strategiei naționale de securitate cibernetică, care acoperă în special sectoarele menționate în anexele 1 și 2;

b) un cadru de guvernanță pentru realizarea obiectivelor și priorităților menționate la lit. a), inclusiv politicile publice;

c) un cadru de guvernanță care clarifică rolurile și responsabilitățile părților interesate relevante la nivel național, care sprijină cooperarea și coordonarea la nivel național între autoritățile competente, punctele unice de contact și echipele de răspuns la incidente de securitate cibernetică în temeiul prezentei ordonanțe de urgență, precum și coordonarea și cooperarea dintre aceste organisme și autoritățile competente în temeiul actelor juridice sectoriale ale Uniunii Europene;

d) un mecanism care să identifice activele relevante și o evaluare a riscurilor la nivel național;

e) o identificare a măsurilor de asigurare a pregătirii pentru incidente la nivel național, a capacității de răspuns la acestea și a redresării în urma acestora, inclusiv cooperarea dintre sectorul public și cel privat;

f) o listă a diferitelor autorități și părți interesate care participă la punerea în aplicare a strategiei naționale de securitate cibernetică;

g) un cadru de politică menit să asigure o mai bună coordonare între autoritățile competente în temeiul prezentei ordonanțe de urgență și al Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a

Consiliului în scopul schimbului de informații privind riscurile, amenințările cibernetice și incidentele, precum și privind riscurile, amenințările și incidentele fără caracter cibernetic și al exercitării sarcinilor de supraveghere, după caz;

h) un plan care să cuprindă inclusiv măsurile necesare pentru a spori nivelul general de sensibilizare a cetățenilor cu privire la securitatea cibernetică.

(2) În cadrul strategiei naționale de securitate cibernetică se prevăd cel puțin următoarele politici publice:

a) care abordează securitatea cibernetică a lanțului de aprovizionare pentru produsele TIC și serviciile TIC utilizate de entități pentru furnizarea serviciilor lor;

b) care privesc includerea și specificarea cerințelor legate de securitatea cibernetică pentru produsele TIC și serviciile TIC în cadrul achizițiilor publice, inclusiv în legătură cu certificarea de securitate cibernetică, criptarea și utilizarea produselor de securitate cibernetică cu sursă deschisă;

c) de gestionare a vulnerabilităților, inclusiv promovarea și facilitarea divulgării coordonate a vulnerabilităților;

d) legate de menținerea disponibilității, integrității și confidențialității generale a nucleului public al internetului deschis, inclusiv securitatea cibernetică a cablurilor de comunicații submarine, după caz;

e) de promovare a dezvoltării și integrării tehnologiilor avansate relevante care vizează implementarea unor măsuri de ultimă generație de gestionare a riscurilor în materie de securitate cibernetică;

f) de promovare și dezvoltare a educației și a formării privind securitatea cibernetică, competențele, sensibilizarea și inițiativele de cercetare și dezvoltare în materie de securitate cibernetică, precum și orientări privind bunele practici și controale în materie de igienă cibernetică, destinate cetățenilor, părților interesate și entităților;

g) de sprijinire a instituțiilor academice și de cercetare în vederea dezvoltării, consolidării și promovării implementării unor instrumente de securitate cibernetică și a unei infrastructuri de rețele securizate;

h) care să includă proceduri relevante și instrumente adecvate de schimb de informații care să sprijine schimbul voluntar de informații în materie de securitate cibernetică între entități, în conformitate cu dreptul Uniunii;

i) de consolidare a rezilienței cibernetice și a nivelului de referință în materie de igienă cibernetică pentru întreprinderile mici și mijlocii, în special pentru cele excluse din domeniul de aplicare al prezentei ordonanțe de urgență, prin furnizarea de orientări și asistență ușor accesibile pentru nevoile lor specifice;

j) de promovare a unei protecții cibernetice active.

Secțiunea a 2-a - Autoritatea competentă la nivel național

Art. 24 - (1) DNSC este autoritatea competentă responsabilă cu securitatea cibernetică și cu sarcinile de supraveghere și asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică.

(2) DNSC îndeplinește funcția de echipă de răspuns la incidente de securitate cibernetică națională, denumită în continuare „CSIRT național”, în temeiul dispozițiilor OUG nr. 104/2021 privind Înființarea Directoratului Național de Securitate Cibernetică.

(3) În vederea îndeplinirii atribuțiilor ce îi revin în calitate de autoritate competentă responsabilă cu securitatea cibernetică și cu sarcinile de supraveghere și asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică și ale funcției îndeplinite conform alin. (2), DNSC se asigură că deține personal suficient și competent și că dispune de resurse adecvate pentru a-și îndeplini în mod eficace și eficient atribuțiile.

(4) Pentru aplicarea alin. (3), din bugetul DNSC se asigură, cu respectarea prevederilor legale, următoarele categorii de cheltuieli:

a) achiziționarea de servicii de specialitate;

b) achiziția de echipamente și software, inclusiv software dezvoltat la comandă;

- c) afilierea la rețele și organizații internaționale de profil și participarea prin reprezentanți la lucrările acestora precum și la alte evenimente de profil;
- d) cursuri de formare și perfecționare precum și certificări ale personalului propriu;
- e) editarea de publicații, ghiduri de specialitate, clipuri video de conștientizare;
- f) organizarea de conferințe, seminare și alte evenimente de profil;
- g) efectuarea de studii statistice și activități de cercetare.

Art. 25 - (1) DNSC, în exercitarea calității de autoritate competentă responsabilă cu securitatea cibernetică și cu sarcinile de supraveghere și asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică, are următoarele atribuții:

- a) elaborează și asigură punerea în aplicare a strategiei naționale de securitate cibernetică alături de celelalte autorități competente în domeniul securității cibernetică;
- b) emite norme și cerințe în domeniul de aplicare al prezentei ordonanțe de urgență prin ordine și decizii ale Directorului DNSC;
- c) elaborează și actualizează ghiduri, recomandări și bune practici în domeniul de aplicare al prezentei ordonanțe de urgență;
- d) administrează și gestionează resursele pentru punerea în aplicare a prezentei ordonanțe de urgență;
- e) participă, prin reprezentanți, la formatele de cooperare la nivel european;
- f) supraveghează, verifică și controlează respectarea prevederilor prezentei ordonanțe de urgență;
- g) primește sesizări cu privire la neîndeplinirea obligațiilor de către entitățile esențiale și importante;
- h) cooperează cu autoritățile competente din celelalte state și oferă asistență acestora, prin schimbul de informații, transmiterea de solicitări și sesizări, efectuarea controlului ori luarea de măsuri de supraveghere și remediere a deficiențelor constatate, în cazul entităților care fac obiectul prezentei ordonanțe de urgență;
- i) autorizează, revocă sau reînnoiește autorizarea echipelor de răspuns la incidente de securitate cibernetică ce deservește entitățile esențiale și importante;
- j) eliberează, revocă sau reînnoiește atestatele auditorilor de securitate cibernetică care pot efectua audit în cadrul rețelelor și sistemelor informatice ce susțin servicii esențiale ori servicii importante, în condițiile prezentei ordonanțe de urgență;
- k) autorizează, revocă sau reînnoiește autorizarea furnizorilor de servicii de formare pentru securitate cibernetică pentru formarea auditorilor de securitate cibernetică și a echipelor de răspuns la incidente de securitate cibernetică;
- l) asigură ducerea la îndeplinire a obligațiilor de raportare a incidentelor de către entitățile esențiale și importante în condițiile prezentei ordonanțe de urgență;
- m) încurajează utilizarea de către entitățile esențiale și importante a produselor ce corespund cerințelor de standardizare și certificare în domeniul securității cibernetică și a serviciilor de încredere calificate;
- n) reglementează și gestionează procesul de divulgare coordonată a vulnerabilităților.

(2) DNSC este responsabil de gestionarea procesului de identificare a entităților esențiale și a entităților importante și păstrează un registru al acestora conform art. 18.

(3) DNSC este responsabil de gestionarea procesului de identificare a furnizorilor de servicii DNS, registrelor de nume TLD, furnizorilor de servicii de cloud computing, furnizorilor de servicii de centre de date, furnizorilor de rețele de furnizare de conținut, furnizorilor de servicii gestionate, furnizorilor de servicii de securitate gestionate, precum și furnizorilor de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea și transmite către ENISA datele privind identificarea acestora până la 17 ianuarie 2025.

(4) DNSC identifică serviciile, sistemele și produsele TIC care pot face obiectul evaluării de risc naționale din perspectiva lanțului de aprovizionare pe care o elaborează și o transmite către ENISA, rezultatele evaluării fiind transmise și către entitățile esențiale și entitățile importante.

(5) DNSC păstrează evidența datelor prevăzute la alin. (3), le actualizează periodic și transmite modificările către ENISA.

(6) DNSC realizează, ori de câte ori este nevoie și cel puțin o dată pe an, o evaluare a securității cibernetice a spațiului cibernetic național civil.

Art. 26 - (1) DNSC, în exercitarea atribuțiilor de supraveghere și control, în cazul neîndeplinirii de către entitățile esențiale și entitățile importante a obligațiilor ce le revin conform dispozițiilor prezentei ordonanțe de urgență, verifică respectarea dispozițiilor prezentei ordonanțe de urgență și realizează controale, emite dispoziții cu caracter obligatoriu pentru entitățile esențiale și entitățile importante în vederea conformării și remedierii deficiențelor constatate și stabilește termene pentru aceasta, instituie măsuri de supraveghere pentru entitățile esențiale și pentru entitățile importante și aplică sancțiuni.

(2) DNSC asigură evaluarea procesului de pregătire și specializare a auditorilor în vederea atestării ca auditori de securitate cibernetică, a membrilor echipelor de răspuns la incidente de securitate cibernetică, a responsabililor de securitate cibernetică și a furnizorilor de servicii de formare pentru securitate cibernetică.

Art. 27 - (1) DNSC cooperează cu instituțiile din COSC și poate solicita efectuarea de verificări ale riscurilor de securitate, inclusiv din perspectiva securității naționale, cu privire la solicitantul de atestat de auditor, membrii echipelor de răspuns la incidente de securitate cibernetică și furnizorilor de servicii specifice echipelor de răspuns la incidente de securitate cibernetică.

(2) În urma aplicării alin. (1), DNSC evaluează riscurile de securitate și în funcție de situație dispune continuarea sau întreruperea procedurii de evaluare și atestare.

Secțiunea a 3-a - Cadrul național de gestionare a crizelor cibernetice

Art. 28 - (1) DNSC este autoritatea națională de gestionare a crizelor cibernetice și este responsabilă la nivel național cu gestionarea incidentelor de securitate cibernetică de mare amploare și crize de securitate cibernetică, calitate pe care o îndeplinește prin Centrul Național de Gestionare a Crizelor de Securitate Cibernetică, denumit în continuare „CNGCSC”, conform dispozițiilor art. 5 lit. o) din OUG nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică.

(2) În îndeplinirea calității prevăzute la alin. (1), DNSC are următoarele atribuții:

a) identifică capacitățile, mijloacele și procedurile care pot fi utilizate în caz de criză, în funcție de care elaborează, actualizează și coordonează aplicarea Planului de management al crizelor de securitate cibernetică la nivel național pe timp de pace, adoptat prin ordin al Directorului DNSC.

b) adoptă măsurile tehnice și organizatorice necesare pentru instituirea nivelului critic de alertă cibernetică și pentru gestionarea acestuia, conform prevederilor Legii nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative;

c) asigură și coordonează schimbul de informații referitoare la crizele de securitate cibernetică cu toate părțile interesate relevante din sectorul public și privat;

d) participă, prin intermediul CNGCSC, la gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare și a crizelor de securitate cibernetică la nivelul Uniunii Europene și acordă sprijin autorităților statelor membre;

e) organizează și participă, prin intermediul CNGCSC, la exerciții, activități de formare și alte măsuri naționale de pregătire în domeniul crizelor de securitate cibernetică.

Art. 29 - (1) Gestionarea la nivel național a incidentelor și a crizelor de securitate cibernetică se realizează în conformitate cu Planul de management al crizelor de securitate cibernetică la nivel național pe timp de pace.

(2) Planul de management al crizelor de securitate cibernetică la nivel național pe timp de pace are ca scop gestionarea incidentelor de securitate cibernetică de mare amploare și al crizelor cibernetică și prevede cel puțin:

- a) obiectivele măsurilor și ale activităților de pregătire;
 - b) sarcinile și responsabilitățile autorităților de gestionare a crizelor cibernetică;
 - c) procedurile de gestionare a crizelor cibernetică, inclusiv integrarea acestora în cadrul național general de gestionare a crizelor și canalele de schimb de informații;
 - d) măsurile de pregătire, inclusiv exerciții și activități de formare;
 - e) părțile interesate relevante din sectorul public și privat și infrastructura implicată;
 - f) procedurile naționale și acordurile dintre autoritățile și organismele naționale relevante menite să asigure participarea efectivă a României la gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare și a crizelor la nivelul Uniunii Europene și sprijinul acordat de aceasta.
- (3) În termen de 90 de zile de la adoptarea sau modificarea Planului prevăzut la alin. (1), DNSC transmite Comisiei Europene și Rețelei europene a organizațiilor de legătură în materie de crize cibernetică, denumită în continuare „EU-CyCLONe”, informații relevante în legătură cu acesta, cu excepția informațiilor care pot aduce atingere securității naționale.
- (4) În termen de 90 de zile de la intrarea în vigoare a prezentei ordonanțe de urgență, DNSC notifică Comisiei Europene și EU-CyCLONe calitatea DNSC de autoritate națională de gestionare a crizelor cibernetică.

Secțiunea a 4-a - Echipele de răspuns la incidente de securitate cibernetică

Art. 30 - (1) Entitățile esențiale, entitățile importante și autoritățile competente sectorial pot constitui echipe de răspuns la incidente de securitate cibernetică, denumite în continuare „CSIRT”, proprii sau sectoriale ori pot achiziționa servicii de specialitate de la furnizori de servicii specifice CSIRT, autorizați de către DNSC.

(2) CSIRT-urile prevăzute la alin. (1) sunt autorizate de către DNSC în urma evaluării îndeplinirii condițiilor specifice de autorizare a acestui tip de serviciu, conform alin. (3) și art. 31-33.

(3) În vederea obținerii autorizării, CSIRT-urile prevăzute la alin. (1) trebuie să probeze deținerea unei infrastructuri de comunicare și de informații adecvate, sigure și reziliente care să permită schimbul de informații cu entitățile pe care acestea le deservesc și cu alte părți interesate relevante, precum și existența resurselor adecvate pentru îndeplinirea efectivă a sarcinilor ce le revin.

(4) CSIRT-urile prevăzute la alin. (1) cooperează și fac schimb de informații relevante cu comunitățile sectoriale sau trans-sectoriale formate din entități esențiale și entități importante.

(5) CSIRT-urile prevăzute la alin. (1) participă la grupuri de cooperare naționale și internaționale, evaluări inter pares, la Rețeaua CSIRT sau la alte formate asemănătoare la solicitarea CSIRT național.

(6) CSIRT-urile prevăzute la alin. (1) cooperează atât între ele, cât și cu CSIRT național.

(7) DNSC poate delega una sau mai multe persoane atât din personalul propriu de control, cât și de specialitate să își exercite temporar atribuțiile în cadrul unui CSIRT prevăzut la alin. (1).

Art. 31 - (1) CSIRT-urile proprii, sectoriale sau furnizorii de servicii specifice CSIRT care deservesc entitățile esențiale sau entitățile importante au următoarele obligații:

- a) să fie autorizate de către DNSC;

- b) să asigure compatibilitatea și interoperabilitatea sistemelor, procedurilor și metodelor utilizate cu cele ale CSIRT național;
- c) să furnizeze cel puțin pachetul minim de servicii de tip CSIRT necesar asigurării la nivel național a unei protecții unitare a entităților esențiale și a entităților importante, în condițiile alin. (2);
- d) să utilizeze în cadrul echipelor un număr corespunzător de persoane calificate;
- e) să se interconecteze la serviciul de alertă, monitorizare și cooperare al DNSC și să asigure un răspuns prompt la alertele și solicitările transmise de CSIRT național;
- f) să dispună de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor lor;
- g) să aloce anual bugetul necesar în vederea menținerii unui nivel ridicat al capabilităților atât din punct de vedere al resurselor umane, cât și tehnice.

(2) Normele tehnice privind compatibilitatea și interoperabilitatea prevăzute la alin. (1) lit. b), pachetul minim de servicii de tip CSIRT prevăzut la alin. (1) lit. c) și criteriile de stabilire a numărului de persoane calificate prevăzute la alin. (1) lit. d) se aprobă prin ordin al Directorului DNSC.

(3) DNSC elaborează tematicile pentru specializarea personalului din cadrul CSIRT-urilor în vederea autorizării conform art. 30 alin. (2), prin decizie a Directorului DNSC.

Art. 32 - (1) CSIRT-urile trebuie să îndeplinească următoarele cerințe:

- a) să asigure o disponibilitate ridicată a canalelor de comunicare proprii, evitând punctele unice de defecțiune, dispunând de mai multe mijloace pentru a fi conectate și pentru a contacta alte entități în orice moment;
- b) să specifice canalele de comunicare prevăzute la lit. a) și să le aducă la cunoștință bazei de utilizatori și parteneri de cooperare;
- c) să mențină sediile și sistemele informatice de suport în amplasamente securizate;
- d) să dispună de un sistem adecvat de gestionare și rutare a cererilor;
- e) să asigure confidențialitatea și credibilitatea operațiunilor lor;
- f) să dispună de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor lor;
- g) să fie echipate cu sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor lor, chiar și după un incident;
- h) să protejeze datele confidențiale și sensibile ale beneficiarilor serviciilor lor de accesul neautorizat, sustragerea, alterarea sau distrugerea lor, prin măsuri tehnice și procedurale suficiente, adecvate și proporționale.

(2) CSIRT-urile pot acorda prioritate unor cereri de sprijin în temeiul unei abordări bazate pe riscuri.

(3) CSIRT-urile stabilesc relații de cooperare cu părțile interesate relevante în vederea îndeplinirii atribuțiilor acestora.

(4) Pentru a facilita cooperarea prevăzută la alin. (3), CSIRT-urile promovează adoptarea și utilizarea unor practici, sisteme de clasificare și taxonomii comune sau standardizate în legătură cu:

- a) procedurile de gestionare a incidentelor;
- b) gestionarea crizelor;
- c) divulgarea coordonată a vulnerabilităților, în temeiul art. 36.

(5) Pachetul minim de servicii de tip CSIRT trebuie să acopere cel puțin funcțiile și controalele sau elementele aferente funcțiilor, de prioritate medie și înaltă, așa cum sunt definite de standardele și cadrele sau platformele recunoscute la nivel internațional în domeniul răspunsului la incidente și al managementului riscului de securitate cibernetică, ce vor fi precizate și actualizate periodic prin ordin al Directorului DNSC.

Art. 33 - (1) CSIRT-urile au următoarele responsabilități:

- a) monitorizarea și analiza amenințărilor cibernetice, a vulnerabilităților și a incidentelor la nivel național și, la cerere, acordarea de asistență entităților esențiale și entităților importante implicate cu privire la monitorizarea rețelei lor și a sistemelor lor informatice în conformitate cu necesitățile acestora;
- b) asigurarea unor mecanisme de avertizare timpurie, alerte, anunțuri și diseminare de informații către entitățile esențiale și entitățile importante, precum și către autoritățile competente și alte părți interesate relevante cu privire la amenințări cibernetice, vulnerabilități și incidente în timp aproape real;
- c) răspunsul la incidente și acordarea de asistență entităților esențiale și entităților importante implicate, după caz;
- d) colectarea și analiza datelor și furnizarea de analize dinamice de risc și de incident și conștientizarea situației în materie de securitate cibernetică;
- e) furnizarea, la cererea unei entități esențiale sau a unei entități importante, a unei scanări de securitate a rețelelor și sistemelor informatice ale entității implicate pentru a detecta vulnerabilitățile cu un impact potențial semnificativ;
- f) participarea la implementarea unor instrumente securizate de schimb de informații, în conformitate cu art. 20.

(2) Scanările prevăzute la alin. (1) lit. e) sunt neintruzive și se efectuează pentru a detecta rețelele și sistemele informatice vulnerabile sau configurate în mod nesigur și nu aduc niciun efect negativ funcționalității serviciilor entităților în cauză.

Art. 34 - (1) CSIRT-urile care deservește entități esențiale sau entități importante se autorizează de către DNSC.

(2) În acest sens, DNSC are următoarele atribuții generale:

- a) elaborează și adoptă, prin ordin al Directorului DNSC, regulamentul privind autorizarea și verificarea CSIRT-urilor care deservește entitățile esențiale și entitățile importante și stabilește condițiile de valabilitate pentru autorizațiile acordate, cât și tematicile pentru formarea personalului CSIRT-urilor;
- b) acordă, prelungește, suspendă sau retrage, prin decizie a Directorului DNSC, autorizarea pentru CSIRT-uri;
- c) acordă, prelungește, suspendă sau retrage, prin decizie a Directorului DNSC, autorizarea furnizorilor de servicii de formare pentru activitățile specifice CSIRT;
- d) verifică, în urma sesizărilor sau din oficiu, îndeplinirea de către CSIRT-urile autorizate a obligațiilor ce le revin.

(3) Autorizările prevăzute la alin. (2) lit. b) au o valabilitate de trei ani.

Art. 35 – DNSC, în calitate de CSIRT național, poate asigura sprijin pentru gestionarea incidentelor:

- a) entităților esențiale și entităților importante, la solicitarea acestora;
- b) echipelor de răspuns la incidente de securitate cibernetică.

Art. 36 - (1) DNSC, în calitate de CSIRT național, este responsabil de gestionarea procesului de divulgare coordonată a vulnerabilităților și este desemnat drept coordonator care acționează ca intermediar de încredere, facilitând, atunci când este necesar, interacțiunea dintre persoana fizică sau juridică care raportează o vulnerabilitate și producătorul sau furnizorul de produse TIC sau servicii TIC potențial vulnerabile, la cererea oricărei părți.

(2) În îndeplinirea alin. (1), DNSC:

- a) asigură primirea, stocarea și evaluarea raportărilor referitoare la orice vulnerabilitate a unui produs sau serviciu TIC, înaintate în condițiile alin. (3);
- b) asigură posibilitatea anonimatului persoanei care raportează o vulnerabilitate;
- c) identifică și contactează entitățile care produc, dețin sau administrează produse sau servicii TIC care fac obiectul raportării conform alin. (3), cărora le comunică vulnerabilitățile raportate;

- d) facilitează, în măsura în care este necesar, atunci când acționează drept intermediar de încredere, interacțiunea dintre persoana care raportează o vulnerabilitate și producătorul, deținătorul, administratorul sau furnizorul de produse sau servicii TIC potențial vulnerabile, la cererea uneia dintre părți și cu acordul celeilalte părți;
 - e) dispune măsuri adecvate, conform atribuțiilor sale legale, în legătură cu gestionarea vulnerabilităților raportate de către entitățile care produc, dețin, administrează sau furnizează produse sau servicii TIC care fac obiectul raportării conform alin. (3);
 - f) efectuează, după caz, verificări asupra vulnerabilităților în sistemele informatice, cu sprijinul producătorilor, deținătorilor, administratorilor sau furnizorilor de produse sau servicii TIC potențial vulnerabile;
 - g) negociază cu entitățile afectate calendarele de divulgare și gestionare a vulnerabilităților care afectează mai multe entități;
 - h) atunci când o vulnerabilitate raportată ar putea avea un impact semnificativ transfrontalier, cooperează, după caz, cu CSIRT-urile desemnate din cadrul Rețelei CSIRT;
 - i) emite proceduri, norme tehnice și ghiduri conținând cerințe minime și recomandări pentru raportarea vulnerabilităților și conduita raportorilor, gestionarea acestora de către entități și îndeplinirea de către acestea a obligațiilor conexe, programele private de divulgare a vulnerabilităților și relațiile dintre entități și raportori;
 - j) poate asista persoanele care raportează o vulnerabilitate.
- (3) Orice persoană fizică sau juridică poate raporta către DNSC vulnerabilități ale unor produse sau servicii TIC, cu respectarea prevederilor legale.
- (4) Producătorii și furnizorii de produse sau servicii TIC au obligațiile de a transmite către DNSC toate informațiile cu privire la vulnerabilitățile pe care le identifică, precum și cu privire la vulnerabilitățile care le sunt semnalate de către terți și care le afectează propriile produse sau servicii și de a remedia respectivele vulnerabilități într-un termen stabilit de comun acord cu DNSC.
- (5) Persoana fizică sau juridică care raportează conform alin. (3), respectă cel puțin următoarele:
- a) activitatea de cercetare pentru descoperirea de vulnerabilități raportate se efectuează cu bună-credință, exclusiv cu scopul de a contribui la îmbunătățirea securității cibernetice și cu respectarea prevederilor legale;
 - b) activitatea de cercetare se desfășoară fără accesarea sau copierea neautorizată a conținutului fișierelor din sistemele informatice care fac obiectul activității de cercetare;
 - c) în cadrul activității de cercetare nu sunt șterse sau modificate date din sistemele informatice care fac obiectul activității de cercetare;
 - d) activitatea de cercetare se desfășoară fără încălcarea sau ocolirea unor bariere tehnice precum parole sau detalii de identificare, prin tehnici precum atacuri brute-force, prin phishing sau alte procedee de inginerie socială;
 - e) nu se cauzează nicio întrerupere sau deteriorare a produselor sau serviciilor TIC ale terților;
 - f) activitatea de cercetare nu se desfășoară pentru a derula atacuri, nu produce prejudicii și nu utilizează produse de tip malware sau tehnici de natură să afecteze disponibilitatea serviciilor TIC;
 - g) nu a dezvăluit public informații cu privire la vulnerabilitatea identificată, anterior sau ulterior momentului raportării, fără acordul DNSC.
- (6) Raportarea de la alin. (3) se realizează în termen de cel mult 48 de ore de la identificarea vulnerabilității.
- (7) Entitățile care fac obiectul prezentei ordonanțe de urgență au obligația de a institui la nivelul acestora procese de management al vulnerabilităților TIC aferente produselor și serviciilor pe care le oferă și care includ cel puțin următoarele măsuri:
- a) asigură primirea raportărilor de vulnerabilități, analiza acestora în vederea confirmării sau infirmării validității celor semnalate, precum și pentru remedierea vulnerabilităților confirmate, inclusiv soluții temporare până la remediere pentru persoanele afectate;
 - b) cooperarea cu DNSC în procesele de management al vulnerabilităților și de divulgare coordonată a vulnerabilităților;

c) stabilirea și publicarea în cadrul detaliilor de contact tehnic în documente și pe pagina de internet, a modalităților de contact și de comunicare privind vulnerabilitățile, precum și a termenilor și condițiilor pentru raportarea de vulnerabilități;

d) asigurarea comunicării și cooperării cu raportorii și cu DNSC în procesul divulgare coordonată a vulnerabilităților, precum și după caz, cu utilizatorii produselor sau serviciilor potențial vulnerabile.

Capitolul IV - Cooperare

Secțiunea 1 - Cooperare la nivel național

Art. 37 - (1) În vederea asigurării unui nivel comun ridicat de securitate cibernetică la nivel național, DNSC se consultă și cooperează cu următoarele:

a) Autoritatea Națională pentru Administrare și Reglementare în Comunicații, denumită în continuare „ANCOM” care este autoritate competentă sectorial în domeniul securității cibernetice, potrivit prevederilor prezentei ordonanțe de urgență, pentru sectorul „8. Infrastructură digitală”: „Furnizorii de IXP (internet exchange point)”, „Furnizorii de rețele publice de comunicații electronice” și „Furnizorii de servicii de comunicații electronice accesibile publicului” din Anexa 1 și pentru Sectorul „1. Servicii poștale și de curierat” din Anexa 2;

b) autoritățile, astfel cum acestea se identifică în temeiul art. 6 din Regulamentul (UE) 203/2023 al Comisiei din 27 octombrie 2022 de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, impuse organizațiilor care intră sub incidența Regulamentelor (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei, precum și autorităților competente care intră sub incidența Regulamentelor (UE) nr. 748/2012, (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340 și (UE) nr. 139/2014 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei, și de modificare a Regulamentelor (UE) nr. 1178/2011, (UE) nr. 748/2012, (UE) nr. 965/2012, (UE) nr. 139/2014, (UE) nr. 1321/2014, (UE) 2015/340 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei și art. 2 alin. (2) din Regulamentul delegat (UE) 2024/1366 al Comisiei din 11 martie 2024 de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică.

c) alte autorități competente sectorial în domeniul securității cibernetice, conform anexelor 1 și 2.

(2) În vederea asigurării unui nivel comun ridicat de securitate cibernetică la nivel național, DNSC se coordonează cu CNCPIC și face schimb de informații pentru identificarea entităților esențiale identificate ca fiind entități critice în ceea ce privește riscurile, incidentele și amenințările cibernetice și de altă natură decât cibernetică care le privesc și le afectează, precum și cu privire la măsurile luate ca răspuns la astfel de riscuri.

(3) DNSC cooperează și colaborează cu Banca Națională a României, denumită în continuare „BNR” și Autoritatea de Supraveghere Financiară, denumită în continuare „ASF”, pentru evaluarea și gestionarea riscurilor cibernetice, identificarea vulnerabilităților și implementarea măsurilor de protecție adecvate entităților esențiale și entităților importante din domeniul bancar și al infrastructurilor pieței financiare, astfel:

a) BNR și ASF transmit în timp util către DNSC informații privind incidentele majore legate de TIC și amenințările cibernetice semnificative, raportate de către entitățile cărora li se aplică cerințele Regulamentului DORA, iar DNSC transmite către BNR și ASF informații privind incidentele majore și amenințările cibernetice, raportate de către entitățile esențiale sau importante cărora li se aplică prezenta

ordonanță de urgență și care au fost desemnate conform Regulamentului DORA drept furnizori terți esențiali de servicii TIC;

b) BNR și ASF pot solicita orice tip de consultanță și asistență tehnică relevantă din partea DNSC, în limita capacităților și resurselor DNSC și pot stabili acorduri de cooperare pentru a permite crearea unor mecanisme de coordonare eficiente și rapide.

(4) DNSC aplică dispozițiile art. 3 alin. (4) și art. 5 lit. h) punctele 8-9 din OUG nr. 104/2021 privind înființarea DNSC în vederea îndeplinirii dispozițiilor prezentei ordonanțe de urgență.

(5) Atunci când există conflict de competență între două sau mai multe instituții publice, autoritatea competentă sectorial va fi desemnată de către ministerele de resort în cooperare cu DNSC, prin hotărâre de Guvern.

(6) Atunci când o entitate desfășoară activitate în două sau mai multe sectoare, astfel cum sunt prevăzute în anexele 1 și 2, acestea i se aplică măsurile tehnice, operaționale și organizatorice proporționale și adecvate pentru a gestiona riscurile aferente securității rețelelor și a sistemelor informatice de nivelul cel mai ridicat.

(7) Autoritățile, astfel cum sunt stabilite la alin. (1), pot:

a) constitui CSIRT-uri sectoriale, sens în care monitorizează, identifică, analizează și răspund la amenințările de securitate cibernetică din sectorul corespunzător și oferă servicii publice de tip preventiv, de tip reactiv sau de consultanță pentru managementul securității cibernetice sau pot achiziționa servicii de specialitate de la furnizorii de servicii specifice CSIRT, autorizați de către DNSC;

b) colecta raportări de incidente din propriul sector, potrivit ordinelor comune prevăzute la alin. (8) lit. b);

c) derula activități de investigare a incidentelor, sub coordonarea CSIRT național;

d) derula activități tehnice specifice de identificare a vulnerabilităților rețelelor și sistemelor informatice pe care le au în administrare, sens în care se consultă și cooperează cu CSIRT național;

e) derula activități de evaluare a incidentelor în scopul identificării principalelor cauze, astfel încât să reducă riscul apariției unor astfel de incidente;

f) elabora ghiduri și recomandări în domeniul securității cibernetice din domeniul de competență pentru asigurarea unei capacități adecvate de identificare, evaluare și adoptare a unor măsuri de management al riscului, răspuns la incidente și atacuri cibernetice, de asigurare a securității lanțului de aprovizionare, precum și de gestionare a situațiilor de criză;

(8) Autoritățile, astfel cum sunt stabilite la alin. (1), au următoarele atribuții:

a) transmit către DNSC, în măsura în care le dețin, informații și date privind amenințările cibernetice, inclusiv de indicatori de compromitere, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare atunci când aceste schimburi de informații și date vizează sporirea rezilienței operaționale digitale a entităților din domeniul de competență a acestora prin sensibilizarea cu privire la amenințările cibernetice, limitarea sau împiedicarea răspândirii amenințărilor cibernetice, sprijinirea gamei de capacități defensive ale entităților, tehnicile de detectare a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare;

b) emit ordine comune, împreună cu DNSC, în domeniul securității cibernetice din domeniul de competență, în vederea asigurării unui nivel comun ridicat de securitate cibernetică la nivel național, inclusiv în ceea ce privește măsurile tehnice, operaționale și organizatorice de gestionare a riscurilor, proporționale și adecvate pe care entitățile din domeniul de competență au obligația de a le lua în desfășurarea activității lor, procedura de notificare și de răspuns la incidentele de securitate cibernetică aplicabile entităților din domeniul de competență, pragurile specifice și criteriile de stabilire a impactului incidentelor de securitate din domeniul de competență;

c) monitorizează respectarea actelor normative din domeniul securității cibernetice, elaborate potrivit lit.

b), de către entitățile din domeniul de competență și realizează activități de supraveghere și control, potrivit prevederilor prezentei ordonanțe de urgență, aplicând în mod corespunzător art. 46-50.

(9) Autoritățile, astfel cum sunt stabilite la alin. (1), au următoarele obligații:

- a) sprijină DNSC în identificarea entităților esențiale și entităților importante din domeniul de competență conform art. 5-10;
- b) participă la elaborarea criteriilor de stabilire a impactului incidentelor, la cererea DNSC;
- c) asigură armonizarea reglementărilor sectoriale în domeniul securității cibernetice cu dispozițiile actelor de reglementare emise de către DNSC;
- d) se coordonează cu DNSC cu privire la planificarea și derularea activităților de control care au ca obiect aspecte de securitate cibernetică;
- e) transmit către DNSC informațiile privitoare la încălcările dispozițiilor prezentei ordonanțe de urgență, în vederea sprijinirii DNSC în stabilirea măsurilor de remediere și a sancțiunii.

(10) Autoritățile competente sectorial sunt, de asemenea, împuternicite să asigure supravegherea, controlul și sancționarea în aplicarea prevederilor prezentei ordonanțe de urgență și ale regulamentelor Uniunii Europene din domeniul securității cibernetice, a măsurilor luate în aplicarea acestora, precum și a drepturilor și obligațiilor entităților aflate în sectorul lor de competență.

(11) Controlul realizat în temeiul alin. (10) se desfășoară, după caz, împreună cu personal de control sau de specialitate din cadrul DNSC.

(12) Autoritățile competente sectorial își pot exercita atribuțiile de supraveghere și control prevăzute de prezenta ordonanță de urgență inclusiv la solicitarea motivată a CNCPIC, pentru entitățile identificate critice conform dispozițiilor Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului.

(13) Aplicarea actelor juridice ale Uniunii Europene nu derogă de la celelalte obligații care revin entităților esențiale și entităților importante conform dispozițiilor prezentei ordonanțe de urgență.

(14) În cazul în care actele juridice sectoriale ale Uniunii Europene impun entităților esențiale sau entităților importante să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să raporteze incidentele semnificative, iar cerințele respective au un efect cel puțin echivalent cu efectul obligațiilor prevăzute în prezenta ordonanță de urgență, dispozițiile prezentei ordonanțe de urgență privind măsurile de gestionare a riscurilor, raportarea incidentelor, precum și supravegherea, verificarea și controlul nu se aplică acestor entități. În cazul în care actele juridice sectoriale ale Uniunii Europene nu acoperă toate entitățile dintr-un anumit sector care intră în domeniul de aplicare al prezentei ordonanțe de urgență, dispozițiile relevante ale prezentei ordonanțe de urgență se aplică în continuare entităților care nu fac obiectul respectivelor acte juridice sectoriale ale Uniunii Europene.

(15) Cerințele menționate la alin. (14) sunt considerate echivalente în privința efectului cu obligațiile prevăzute în prezenta ordonanță de urgență, în cazul în care îndeplinește cel puțin o condiție din următoarele:

- a) măsurile de gestionare a riscurilor în materie de securitate cibernetică sunt cel puțin echivalente în privința efectului cu cele prevăzute la art. 13;
- b) actul juridic sectorial al Uniunii Europene prevede accesul imediat, după caz, automat și direct, la raportarea incidentelor pentru CSIRT-uri, autoritățile competente sau punctele unice de contact în temeiul prezentei ordonanțe de urgență și dacă cerințele de raportare a incidentelor semnificative au un efect cel puțin echivalent cu cele prevăzute la art. 15.

(16) Dispozițiile alin. (7)-(14) nu se aplică BNR și ASF.

Art. 38 - (1) În exercitarea atribuțiilor prevăzute la art. 37 alin. (8) lit. b), DNSC și autoritatea competentă sectorial au obligația de a respecta procedura de consultare stabilită prin prezentul articol ori de câte ori măsurile pe care intenționează să le adopte sunt de natură să producă un impact semnificativ în domeniul securității cibernetice în sectorul corespunzător.

(2) DNSC și autoritatea competentă sectorial au obligația de a publica textul supus consultării pe paginile de internet proprii, precizând totodată și: data publicării documentului, data la care expiră termenul de depunere a observațiilor și data estimativă la care intenționează să adopte măsura care face obiectul consultării.

(3) De la data la care textul supus consultării este publicat pe paginile de internet, DNSC și autoritatea competentă sectorial vor acorda un termen de cel puțin 30 de zile pentru depunerea de observații, în scris, de către orice persoană interesată. În situațiile în care este necesară adoptarea unor măsuri în regim de urgență, DNSC și autoritatea competentă sectorial vor acorda pentru depunerea de observații un termen de 10 până la 30 de zile.

(4) Cel mai târziu la data publicării pe pagina de internet a proiectului ordinului prin care se adoptă măsura, DNSC și autoritatea competentă sectorial au obligația de a publica și un material de sinteză comun cu observațiilor primite, în care vor preciza și poziția lor față de aceste observații.

Art. 39 – (1) Pentru asigurarea unui nivel comun ridicat de securitate cibernetică la nivel național, DNSC se consultă și cooperează cu:

- a) Serviciul Român de Informații, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale a căror afectare aduce atingere securității naționale;
- b) Ministerul Apărării Naționale, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în sprijinul activităților privind apărarea națională;
- c) Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în domeniul lor de activitate și responsabilitate.

(2) DNSC se consultă și cooperează, după caz, cu:

- a) organele de urmărire penală;
- b) Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare „ANSPDCP”, în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, în condițiile legii.

Secțiunea a 2-a - Cooperare la nivel european și internațional

Art. 40 - (1) DNSC îndeplinește funcția de punct unic de contact la nivel național, calitate în care facilitează cooperarea pentru securitatea rețelelor și a sistemelor informatice cu autorități relevante din state membre, cu Comisia Europeană și cu ENISA, inclusiv pentru alte autorități competente din România.

(2) În calitate de punct unic de contact la nivel național, DNSC îi revin următoarele atribuții:

- a) exercită funcția de legătură între autoritățile competente din România și autoritățile cu competențe în aplicare de măsuri pentru un nivel comun ridicat de securitate cibernetică în statele membre, precum și cu Grupul de cooperare și Rețeaua CSIRT;
- b) informează celelalte state membre sau parteneri afectați dacă incidentul are un impact semnificativ asupra continuității serviciilor esențiale ori a serviciilor importante în statele respective;
- c) transmite Grupului de cooperare rapoarte de sinteză privind notificările primite și acțiunile întreprinse;
- d) transmite autorităților sau CSIRT-urilor naționale ale altor state membre, CSIRT-urilor autorizate de către DNSC conform prevederilor prezentei ordonanțe de urgență, Rețelei EU-CyCLONe, punctelor unice de contact din celelalte state membre, potrivit ariei de responsabilitate, notificările și solicitările privind incidentele ce afectează funcționarea serviciilor esențiale din unul sau mai multe sectoare stabilite în anexele 1 și 2;

- e) transmite autorităților competente notificările și cererile primite din partea altor state membre, potrivit ariei de responsabilitate;
- f) transmite către ENISA, o dată la 90 de zile, un raport de sinteză ce include date anonimizate și agregate privind incidentele semnificative, incidentele, amenințările cibernetice semnificative și incidentele evitate la limită raportate de către entitățile esențiale și entitățile importante către DNSC, precum și de către orice altă entitate, conform art. 15-16.

Art. 41 - (1) DNSC, în calitate de CSIRT național, participă la Rețeaua CSIRT în scop operațional.

(2) În îndeplinirea acestei calități, DNSC îi revin următoarele atribuții:

- a) participă la partajarea, transferul și schimbul de tehnologie între CSIRT-urile parte la Rețea;
- b) participă la schimbul de informații privind măsuri, politici, instrumente, procese, bune practici și cadre relevante între CSIRT-urile parte la Rețea;
- c) participă la schimbul de informații relevante privind incidentele, incidentele evitate la limită, amenințările cibernetice, riscurile și vulnerabilitățile;
- d) participă la schimbul de informații în ceea ce privește publicațiile și recomandările în materie de securitate cibernetică;
- e) participă la elaborarea unui răspuns coordonat al Rețelei pentru managementul unui incident identificat pe teritoriul unui alt stat membru;
- f) implementează și utilizează specificațiile și protocoalele referitoare la schimbul de informații care să asigure interoperabilitatea cu celelalte CSIRT-uri din cadrul Uniunii Europene;
- g) colaborează cu CSIRT-ul național al statului afectat de un incident pentru a facilita schimbul de informații referitoare la incident, la amenințările cibernetice, riscurile și vulnerabilitățile asociate acestuia, la solicitarea statului afectat, membru al Rețelei;
- h) sprijină statele membre în abordarea incidentelor cu caracter transfrontalier, în condițiile Legii nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative;
- i) participă la schimbul de bune practici și cooperează cu alte CSIRT-urilor desemnate coordonator în ceea ce privește gestionarea divulgării coordonate a vulnerabilităților care ar putea avea un impact semnificativ transfrontalier;
- j) participă la bilanțul exercițiilor de securitate cibernetică, inclusiv al celor desfășurate de ENISA;
- k) cooperează și participă la schimbul de informații cu centrele operaționale de securitate de la nivel regional și de la nivelul Uniunii Europene pentru a îmbunătăți conștientizarea comună a situației cu privire la incidente și amenințări cibernetice;
- l) evaluează rapoartele privind evaluarea inter pares, după caz;
- m) oferă orientări pentru a facilita convergența practicilor operaționale în ceea ce privește aplicarea dispozițiilor prezentei ordonanțe de urgență referitoare la cooperarea operațională;
- n) transmite, după caz, solicitările de sprijin către ceilalți membri ai Rețelei pentru elaborarea unui răspuns coordonat al Rețelei pentru managementul unui incident identificat pe teritoriul României.

Art. 42 - În scopul facilitării cooperării strategice și schimbului de informații între statele membre, DNSC, în calitatea sa de autoritate competentă responsabilă cu securitatea cibernetică și cu sarcinile de supraveghere și asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică, participă la Grupul de cooperare instituit la nivelul Uniunii Europene.

Art. 43 - DNSC, în calitate de CNGCSC, participă la EU-CyCLONe pentru a sprijini gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor și

pentru a asigura schimbul periodic de informații relevante între statele membre și instituțiile, organizațiile, oficiile și agențiile Uniunii Europene.

Art. 44 - (1) Evaluările inter pares reprezintă procese voluntare și de cooperare desfășurate între statele membre în care experți în securitate cibernetică, desemnați de către cel puțin două state diferite de statul care face obiectul evaluării, analizează reciproc punerea în aplicare a măsurilor de securitate cibernetică și a capacităților operaționale și implică vizite fizice sau întâlniri virtuale, precum și schimburi de date și informații.

(2) În conformitate cu principiul bunei cooperări, DNSC furnizează experților în materie de securitate cibernetică desemnați informațiile necesare pentru evaluare, fără a aduce atingere dreptului național sau dreptului Uniunii privind protecția informațiilor confidențiale sau clasificate și protejării funcțiilor esențiale ale statului, cum ar fi securitatea națională.

(3) Evaluările inter pares acoperă cel puțin unul dintre următoarele:

- a) nivelul punerii în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare stabilite în temeiul prezentei ordonanțe de urgență;
- b) nivelul capacităților, inclusiv resursele financiare, tehnice și umane disponibile, precum și eficacitatea exercitării sarcinilor autorităților competente;
- c) capacitățile operaționale ale CSIRT-urilor;
- d) nivelul de punere în aplicare a asistenței reciproce;
- e) nivelul de punere în aplicare a acordurilor privind schimbul de informații în materie de securitate cibernetică;
- f) aspecte specifice de natură transfrontalieră sau trans-sectorială.

(4) DNSC desemnează experți în securitate cibernetică pentru efectuarea evaluărilor inter pares pe baza unei metodologii care include criterii obiective, nediscriminatorii, echitabile și transparente, elaborate de către Grupul de cooperare.

(5) DNSC se asigură că orice risc de conflict de interese în ceea ce privește experții în materie de securitate cibernetică desemnați este dezvăluit celorlalte state membre, Grupului de cooperare, Comisiei și ENISA, înainte de începerea evaluării inter pares.

(6) Statul membru supus evaluării inter pares se poate opune desemnării anumitor experți în materie de securitate cibernetică din motive justificate corespunzător, comunicate DNSC.

(7) Experții în materie de securitate cibernetică care participă la evaluări inter pares elaborează rapoarte cu privire la constatările și concluziile evaluărilor inter pares.

(8) DNSC, atunci când face obiectul unei evaluări inter pares, poate prezenta observații cu privire la proiectele de rapoarte care îl privesc, iar aceste observații se anexează la rapoarte.

(9) DNSC, atunci când face obiectul unei evaluări inter pares, poate decide să pună la dispoziția publicului raportul său sau o versiune anonimizată a acestuia.

Art. 45 - (1) Atunci când o entitate înregistrată în România ca entitate esențială sau importantă furnizează servicii în mai multe state membre sau furnizează servicii în unul sau mai multe state membre iar rețeaua și sistemele sale informatice sunt situate în unul sau mai multe alte state membre, DNSC cooperează cu celelalte autorități competente omoloage de la nivelul Uniunii Europene și își oferă asistență reciprocă.

(2) În situația alin. (1), DNSC poate solicita autorităților competente omoloage de la nivelul Uniunii Europene să exercite atribuții de supraveghere și control și, după caz, DNSC poate aplica amenzi pentru neregulile constatate de către acestea.

(3) Atunci când o entitate furnizează servicii în mai multe state membre, printre care și România, sau furnizează servicii în unul sau mai multe state membre iar rețeaua și sistemele sale informatice sunt

situate în unul sau mai multe alte state membre, printre care și România, DNSC cooperează cu celelalte autorități competente omoloage de la nivelul Uniunii Europene și își oferă asistență reciprocă.

(4) În situația alin. (3), DNSC poate exercita atribuții de supraveghere și control la solicitarea expresă a autorităților competente omoloage de la nivelul Uniunii Europene.

Capitolul V - Supraveghere, verificare și control

Secțiunea 1 - Entități esențiale și entități importante

Art. 46 - (1) În scopul asigurării respectării dispozițiilor prezentei ordonanțe de urgență, precum și a actelor normative subsecvente de către entități, DNSC, poate:

a) derula activități de supraveghere, verificare și control efectuate de persoane desemnate în acest sens prin decizie a Directorului DNSC;

b) dispune efectuarea de audituri de securitate ad-hoc, realizate de un auditor de securitate cibernetică atestat;

c) solicita informații necesare pentru a evalua măsurile de gestionare a riscurilor în materie de securitate cibernetică adoptate de entitatea în cauză, inclusiv politicile de securitate cibernetică documentate, precum și respectarea obligației de a transmite informații către DNSC în temeiul art. 18;

d) solicita acces la date, la documente și la orice informații necesare pentru îndeplinirea sarcinilor lor de supraveghere;

e) solicita date, documente și orice informații care atestă punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate cibernetică efectuate de un auditor atestat și mijloacele de probă care stau la baza acestora.

(2) Activitatea de control se realizează în baza planului de control anual aprobat prin decizie a Directorului DNSC, după avizarea acestuia de către adjunctul directorului DNSC care coordonează activitatea de reglementare și control sau în următoarele cazuri, fără a fi limitate la acestea:

a) unui incident semnificativ;

b) indiciilor temeinice cu privire la încălcarea dispozițiilor prezentei ordonanțe de urgență de către o entitate.

(3) Activitatea de supraveghere și control se realizează de către DNSC inclusiv la solicitarea motivată a CNCPIC pentru entitățile identificate critice conform dispozițiilor Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului.

(4) În cazul entităților importante, supravegherea conform alin. (1) lit. a) se realizează doar pentru punerea în aplicare a art. 48 alin. (2) lit. b)-g).

(5) În vederea punerii în aplicare a alin. (1) lit. a) cu privire la entitățile esențiale și entitățile importante, DNSC poate efectua scanări de securitate cibernetică neintruzive și proactive, bazate pe criterii obiective, nediscriminatorii, echitabile și transparente pentru evaluarea riscurilor, cu notificarea prealabilă a entității în cauză și, după caz, în cooperare cu aceasta.

(6) În vederea punerii în aplicare a alin. (2), DNSC poate solicita accesul la date, echipamente hardware și software, precum și informații de la personalul entităților în vederea îndeplinirii sarcinilor de supraveghere și control.

(7) Cu ocazia desfășurării auditului de securitate cibernetică prevăzut la art. 12 alin. (5), se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul unor rețele și sisteme informatice, în vederea identificării disfuncționalităților și vulnerabilităților și recomandării măsurilor de remediere a acestora.

(8) În termen de cel mult 5 zile de la finalizarea oricărui audit de securitate cibernetică, entitatea auditată transmite către DNSC rezultatele acestuia.

(9) Costurile generate de auditul de securitate cibernetică, inclusiv cel ad-hoc, sunt suportate de către entitatea auditată.

Art. 47 – (1) În aplicarea dispozițiilor privind solicitările prevăzute la art. 46 alin. (1) lit. c)-e), DNSC va preciza scopul și informațiile solicitate, precum și termenul în care entitatea trebuie să se conformeze, ținând cont de urgența solicitării.

(2) Constatările urmare a îndeplinirii activităților de supraveghere, verificare și control prevăzute la alin. (1) sunt consemnate de personalul de control desemnat în nota de constatare.

(3) În cazul în care prin nota de constatare preliminară prevăzută la alin. (2) sunt reținute fapte care ar putea constitui una dintre contravențiile prevăzute la art. 60, nota de constatare se comunică entității în cauză pentru a transmite un punct de vedere cu privire la deficiențele constatate, solicitându-se, dacă este cazul, un plan de măsuri pentru remedierea acestora.

(4) Punctul de vedere prevăzut la dispozițiile alin. (3) va fi comunicat în termen de trei zile de la primirea notei de constatare transmise de către DNSC, cu excepția cazului în care entitatea notificată solicită prelungirea termenului în vederea obținerii unor acte doveditoare în susținerea punctului de vedere menționat, caz în care termenul nu poate depăși 10 zile.

(5) În cel mult 15 zile lucrătoare de la data primirii notei de constatare conform alin. (3) sau transmiterii punctului de vedere conform alin. (3), după caz, entitățile sunt obligate să întocmească și să transmită către DNSC planul de măsuri pentru remedierea tuturor deficiențelor constatate și termenele asumate pentru implementarea acestora.

(6) Termenele prevăzute la alin. (5) trebuie să fie justificate prin prisma circumstanțierii măsurii prin care se remediază deficiența.

(7) Nota de constatare prevăzută la alin. (2), punctul de vedere prevăzut la alin. (3), precum și planul de măsuri prevăzut la alin. (5), atunci când acestea au fost furnizate, stau la baza deciziei Directorului DNSC prin care se constată contravenția și se dispune sancțiunea corespunzătoare.

(8) Normele de aplicare și metodologia de prioritizare pe bază de risc a activităților de supraveghere, verificare și control sunt emise prin ordin al Directorului DNSC.

Art. 48 - (1) În vederea îndeplinirii atribuțiilor care îi revin, precum și pentru asigurarea respectării dispozițiilor prezentei ordonanțe de urgență de către entități, DNSC aplică următoarele sancțiuni:

a) avertisment;

b) amendă contravențională.

(2) DNSC poate dispune, după caz, următoarele:

a) adoptarea unor măsuri atunci când acestea sunt necesare pentru a preveni sau remedia un incident, precum și termene limită pentru punerea în aplicare a acestor măsuri, inclusiv a unui audit ad-hoc;

b) remedierea deficiențelor identificate în aplicarea lit. a);

c) încetarea conduitei entităților prin care încalcă dispozițiile prezentei ordonanțe de urgență;

d) punerea în aplicare a recomandărilor formulate ca urmare a unui audit de securitate;

e) desemnarea unei persoane din cadrul personalului de control, cu sarcini bine definite pe o perioadă de timp determinată, responsabile cu supravegherea respectării de către entitatea esențială în cauză a dispozițiilor art. 11-14;

f) respectarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică prevăzute la art. 11-14 și a obligațiilor de raportare prevăzute la art. 15, într-o anumită modalitate și într-un interval de timp;

g) ca încălcările dispozițiilor prezentei ordonanțe de urgență să fie făcute publice de către entitatea responsabilă.

(3) Atunci când, în urma aplicării art. 46 alin. (1) lit. b), auditul ad-hoc relevă încălcarea prevederilor prezentei ordonanțe de urgență, aceasta este sancționabilă conform alin. (1) lit. a).

(4) DNSC poate dispune entităților să informeze, într-un termen anume determinat, persoanele cărora le prestează un serviciu, dacă acestea au fost sau pot fi afectate de o amenințare cibernetică semnificativă, de următoarele:

- a) caracterul amenințării;
- b) măsurile de protecție sau de remediere pe care persoanele afectate le pot adopta în vederea prevenirii producerii incidentului semnificativ sau în vederea remedierii acestuia.

(5) Măsurile prevăzute la dispozițiile alin. (1) și (2) se dispun prin decizie a Directorului DNSC și se comunică entității în cauză în cel mult 60 de zile de la emiterea deciziei.

Art. 49 - (1) Atunci când măsurile prevăzute la art. 48 nu sunt suficiente pentru a determina respectarea de către entitățile esențiale a solicitărilor de remediere a deficiențelor într-un termen rezonabil, prin decizie a Directorului DNSC, se poate dispune:

- a) sesizarea autorităților, instituțiilor sau entităților competente sectorial în vederea suspendării temporare a certificării sau a autorizării emise pentru entitatea în cauză, pentru o parte sau pentru toate serviciile relevante furnizate sau pentru activitățile relevante desfășurate de entitatea respectivă;
 - b) sesizarea autorităților, instituțiilor sau entităților competente pentru a impune interdicția temporară de a exercita funcția de conducere la nivel de director executiv sau de reprezentant legal în entitatea în cauză.
- (2) Suspendarea și interdicția temporară impuse în temeiul alin. (1) se aplică până când DNSC notifică autoritățile, instituțiile sau entitățile competente conform alin. (1) încetarea cauzei pentru care acestea au fost dispuse.

(3) Măsurile prevăzute la alin. (1) nu se aplică entităților din administrația publică care intră în domeniul de aplicare al prezentei ordonanțe de urgență.

Art. 50 - (1) Stabilirea măsurilor prevăzute la art. 48-49 se face cu evaluarea a cel puțin:

- a) durata faptei;
- b) existența unei abateri anterioare;
- c) prejudiciile materiale sau non-materiale cauzate prin faptă;
- d) măsurile adoptate de entitate în vederea prevenirii sau remedierii efectelor faptei;
- e) conduita entității în raport cu mecanismele de certificare la care a aderat sau codurile de conduită asumate;
- f) conduita persoanelor responsabile în raport cu autoritățile competente.

(2) Următoarele fapte constituie încălcări grave:

- a) încălcări repetate;
- b) neîndeplinirea obligației de notificare sau de remediere a incidentelor semnificative;
- c) neîndeplinirea obligației de remediere a deficiențelor constatate de către autoritățile competente;
- d) obstrucționarea auditurilor sau a activității de monitorizare dispuse de DNSC în urma constatărilor;
- e) furnizarea de informații false sau vădit denaturate în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate cibernetică prevăzute la art. 12 și art. 13 sau obligațiile de raportare prevăzute la art. 17;
- f) îngrădirea accesului personalului desemnat în acest sens de către DNSC în spațiile supuse controlului, cât și asupra datelor și informațiilor necesare controlului;
- g) nerespectarea dispozițiilor DNSC emise în temeiul art. 48 alin. (2).

(3) Organele de conducere ale entității răspund pentru permiterea accesului personalului, desemnat în acest sens de către DNSC, în spațiile supuse controlului, cât și asupra datelor și informațiilor necesare controlului.

Art. 51 - (1) DNSC informează CNCPIC atunci când își exercită competențele de supraveghere și control asupra unei entități esențiale identificate drept entitate critică în conformitate cu dispozițiile Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului.

(2) CNCPIC poate solicita DNSC să își exercite competențele de supraveghere și control asupra unei entități esențiale identificate drept entitate critică în conformitate cu dispozițiile Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului.

Art. 52 - DNSC poate propune împuternicirea prin hotărâre de Guvern a altor autorități competente sectorial în domeniul securității cibernetice pentru domeniul de competență corespunzător în vederea îndeplinirii atribuțiilor prevăzute la art. 46-51 și art. 60-63.

Secțiunea a 2-a – CSIRT-uri, auditori și furnizori de servicii de formare pentru securitate cibernetică

Art. 53 - (1) DNSC supraveghează, verifică și controlează activitatea CSIRT-urilor proprii ale entităților esențiale și entităților importante sau CSIRT-urilor sectoriale, a furnizorilor de servicii specifice CSIRT, precum și a auditorilor de securitate cibernetică, atunci când acestea prestează servicii de specialitate entităților esențiale și entităților importante.

(2) DNSC, în exercitarea atribuțiilor de supraveghere, verificare și control, în cazul neîndeplinirii obligațiilor de către CSIRT-urile proprii ale entităților esențiale și entităților importante sau CSIRT-urile sectoriale, furnizorii de servicii specifice CSIRT, precum și auditorii de securitate cibernetică, desfășoară activități de control cu scopul verificării îndeplinirii obligațiilor prevăzute la art. 31-33, emite dispoziții cu caracter obligatoriu în vederea conformării și remedierii deficiențelor constatate și stabilește termene în vederea conformării acestora, instituie măsuri de supraveghere și aplică sancțiuni.

Art. 54 - (1) DNSC supraveghează, verifică și controlează activitatea furnizorilor de servicii de formare pentru securitate cibernetică pentru auditori și CSIRT-uri.

(2) DNSC, în exercitarea atribuțiilor de supraveghere, verificare și control, în cazul neîndeplinirii obligațiilor de către furnizorii de servicii de formare pentru securitate cibernetică pentru auditori și CSIRT-uri, desfășoară activități de control cu scopul verificării îndeplinirii prevederilor ordinului de la alin. (3), emite dispoziții cu caracter obligatoriu în vederea conformării și remedierii deficiențelor constatate și stabilește termene în vederea conformării acestora, instituie măsuri de supraveghere și aplică sancțiuni.

(3) DNSC elaborează regulamentul privind autorizarea, verificarea și revocarea furnizorilor de servicii de formare pentru securitate cibernetică pentru auditori și CSIRT-uri și stabilește condițiile de valabilitate pentru autorizațiile acordate acestora prin ordin al Directorului DNSC.

Art. 55 - (1) În cazul în care, în urma verificărilor, se constată abateri grave, DNSC poate dispune suspendarea atestatului auditorilor de securitate cibernetică sau autorizației CSIRT-urilor pentru o perioadă determinată de timp, în vederea remedierii, sau, după caz, revocarea acestora.

(2) Anual, în primul trimestru, auditorii de securitate cibernetică vor transmite DNSC, în format electronic, o situație a auditurilor de securitate desfășurate în anul calendaristic precedent, respectiv numărul, beneficiarii, perioadele, neregulile grave constatate și vulnerabilitățile constatate.

Art. 56 - (1) DNSC exercită supravegherea, verificarea și controlul respectării prevederilor prezentei ordonanțe de urgență în ceea ce privește obligațiile ce revin urmare a activităților de autorizare și atestare a acestora pentru CSIRT-urile proprii ale entităților esențiale și entităților importante sau CSIRT-urile sectoriale, furnizorii de servicii specifice CSIRT, precum și auditorii de securitate cibernetică.

(2) Normele de aplicare a dispozițiilor privind supravegherea, verificarea și controlul pentru CSIRT-urile proprii ale entităților esențiale și entităților importante sau CSIRT-urile sectoriale, furnizorii de servicii specifice CSIRT, precum și auditorii de securitate cibernetică se aprobă prin ordin al Directorului DNSC.

(3) Autorizarea, suspendarea și retragerea autorizării, precum și reautorizarea furnizorilor de servicii de formare pentru securitate cibernetică pentru auditori și CSIRT-uri se dispune prin decizie a Directorului DNSC.

(4) Autorizația de furnizor de servicii de formare pentru securitate cibernetică pentru auditori și CSIRT-uri este emisă de DNSC pe baza criteriilor de evaluare, cu valabilitate limitată de patru ani.

Capitolul VI - Auditul de securitate cibernetică

Art. 57 - (1) Auditul de securitate cibernetică poate fi:

- a) periodic, care se desfășoară cu regularitate, conform ordinului de la art. 12 alin. (1);
- b) ad-hoc, în baza deciziei Directorului DNSC conform alin. (2).

(2) Auditul de securitate cibernetică ad-hoc are caracter excepțional și reprezintă acea activitate de auditare efectuată de un auditor atestat conform dispozițiilor prezentei ordonanțe de urgență, cu privire la o entitate esențială sau o entitate importantă, la solicitarea motivată a DNSC, ca urmare a:

- a) unui incident semnificativ;
- b) o schimbare cu impact semnificativ la nivelul rețelelor și sistemelor informatice, dar nu mai târziu de 180 de zile de la apariția acesteia;
- c) indiciilor temeinice cu privire la încălcarea dispozițiilor prezentei ordonanțe de urgență de către o entitate esențială.

(3) Atunci când se dispune un audit ad-hoc, DNSC comunică entității atât motivele, cât și obiectivele auditului.

(4) Entitatea auditată are dreptul de a selecta auditorul.

(5) Schimbarea cu impact semnificativ la nivelul rețelelor și sistemelor informatice prevăzută la alin. (2) lit. b) este generată prin:

- a) introducerea unei noi rețele sau unui nou sistem informatic implicat în furnizarea serviciului;
- b) introducerea unei noi tehnologii pentru furnizarea serviciului;
- c) schimbarea modului de operare a serviciului;
- d) schimbarea calității entității, din entitate importantă în entitate esențială.

(6) Indiciile temeinice prevăzute la alin. (2) lit. c) pot lua naștere ca urmare a desfășurării măsurii de control efectuate de către personal din cadrul DNSC, a informațiilor primite de la autoritățile prevăzute la art. 10 din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, CNCPIC, autoritățile competente sectorial prevăzute la art. 37, precum și de la alte entități conform art. 25 din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative sau ca urmare a analizelor privind incidentele raportate prin platforma de raportare a incidentelor.

(7) Cu ocazia desfășurării auditului de securitate cibernetică periodic, se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul unor rețele și sisteme informatice, în vederea identificării disfuncționalităților și vulnerabilităților și recomandării măsurilor de remediere a acestora.

(8) În cel mult 15 zile lucrătoare de la data primirii raportului de audit, entitățile sunt obligate să întocmească și să transmită către DNSC, în baza recomandărilor emise de către auditor, planul de măsuri pentru remedierea tuturor deficiențelor constatate și termenele asumate pentru implementarea acestora.

(9) Entitățile sunt obligate să implementeze planul de măsuri prevăzut la alin. (8) în termenul asumat.

(10) Entitatea în cauză notifică DNSC cu privire la implementarea tuturor măsurilor prevăzute la alin. (8) și pune la dispoziție acte doveditoare în acest sens, în cel mult cinci zile de la împlinirea termenului asumat.

(11) Termenele prevăzute la alin. (8) trebuie să fie justificate prin prisma circumstanțierii măsurii prin care se remediază deficiența.

Art. 58 - (1) Auditul de securitate cibernetică se realizează de către auditorii de securitate cibernetică ce dețin atestat valabil eliberat de către DNSC, cu excepția auditului de securitate cibernetică realizat la nivelul instituțiilor cu responsabilități în domeniul apărării, ordinii publice și securității naționale, precum și pentru serviciile puse la dispoziție de către acestea.

(2) În acest sens, DNSC:

- a) menține evidența auditorilor de securitate cibernetică;
- b) elaborează regulamentul privind atestarea și verificarea auditorilor de securitate cibernetică și stabilește condițiile de valabilitate pentru atestatele acordate acestora prin ordin al Directorului DNSC;

- c) acordă, prelungește, suspendă sau retrage atestatul auditorilor de securitate cibernetică, conform regulamentului prevăzut la lit. b);
 - d) verifică, în urma sesizărilor sau din oficiu, îndeplinirea de către auditorii atestați a obligațiilor legale ce le revin;
 - e) elaborează tematicile pentru specializarea auditorilor în vederea atestării prevăzute la lit. c), prin decizie a Directorului DNSC.
- (3) Nu pot realiza audit de securitate cibernetică:
- a) auditorii atestați care asigură în mod curent servicii de securitate cibernetică ori servicii de tip CSIRT entităților esențiale sau entităților importante în cauză ori sunt angajați ai acestora;
 - b) auditorul care are un contract de prestări servicii pentru rețeaua sau sistemul supus auditului aflat în desfășurare 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 aceeași entitate esențială sau entitate importantă.
- (4) Activitatea de audit se efectuează potrivit standardelor și specificațiilor europene și internaționale aplicabile în domeniu.
- (5) Tematicile de audit vor ține seama de normele tehnice în vigoare privind securitatea rețelelor și sistemelor informatice ale entităților esențiale și entităților importante, elaborate în temeiul prezentei ordonanțe de urgență.
- (6) Atestatele au o valabilitate de 3 ani.
- (7) Lista standardelor și specificațiilor europene și internaționale prevăzute la dispozițiile alin. (4) se elaborează și se aprobă prin decizie a Directorului DNSC, care se actualizează ori de câte ori este necesar.
- (8) În desfășurarea unei activități de audit de securitate, auditorul de securitate cibernetică trebuie:
- a) să dea dovadă de integritate profesională, acționând cu onestitate și corectitudine în toate angajamentele profesionale, oferind evaluări adevărate și precise;
 - b) să respecte codurile etice emise de către DNSC și Corpul Auditorilor de Sisteme Informatice din România, să dea dovadă și să mențină transparența în comunicări;
 - c) să nu fie în conflict de interese care ar putea afecta independența sa, fie că sunt de natură financiară, personală sau profesională pentru a putea lua decizii în mod independent, și fără vreo influență din partea entității auditate sau a altor părți interesate;
 - d) să protejeze confidențialitatea informațiilor obținute în timpul procesului de audit, sens în care trebuie să se asigure că accesul la informații sensibile este restricționat doar la personalul autorizat și că aceste informații sunt stocate în siguranță, în acord cu reglementările relevante care guvernează practicile de audit, inclusiv cele specifice securității cibernetică.

Art. 59 - (1) În vederea atribuirii și retragerii atestatului de auditor de securitate cibernetică, precum și pentru organizarea și coordonarea activității de audit de securitate cibernetică, se înființează Corpul Auditorilor de Sisteme Informatice din România prin hotărâre de Guvern elaborată de către DNSC, în termen de doi ani de la intrarea în vigoare a prezentei ordonanțe de urgență.

- (2) Corpul Auditorilor de Sisteme Informatice din România se organizează și va funcționa ca organizație profesională de utilitate publică fără scop lucrativ, cu personalitate juridică, în coordonarea DNSC.
- (3) Corpul Auditorilor de Sisteme Informatice din România are ca obiect principal de activitate reglementarea standardelor, cât și a Codului de etică pentru practica profesională a auditului de securitate cibernetică și monitorizarea continuă a activităților de audit de sisteme informatice în România.
- (4) Structura organizatorică a Corpului Auditorilor de Sisteme Informatice din România se aprobă prin ordin al Directorului DNSC.
- (5) DNSC coordonează activitatea de elaborare a regulamentelor de organizare și funcționare și de ordine interioară.
- (6) Corpul Auditorilor de Sisteme Informatice din România poate avea în structură subunități cu sau fără personalitate juridică, departamente, secții și poate dobândi calitatea de asociat sau de acționar fondator în cadrul altor societăți comerciale ori structuri organizatorice necesare realizării obiectului său de activitate.

Capitolul VII - Sancțiuni

Art. 60 - (1) Următoarele fapte constituie contravenții dacă nu au fost săvârșite în astfel de condiții încât să fie considerate infracțiuni potrivit legii:

- a) nerespectarea de către entitățile esențiale și importante a obligației privind luarea unor măsuri tehnice, operaționale și organizatorice prevăzute la art. 11 alin. (1) în condițiile și cu respectarea cerințelor impuse;
- b) nerespectarea de către entitățile esențiale și importante a obligației de a se supune unui audit de securitate cibernetică conform art. 11 alin. (5), în termenul indicat;
- c) nerespectarea de către entitățile esențiale și importante a obligației de a transmite datele solicitate conform art. 11 alin. (7) în termen de 30 de zile de la data comunicării cererii DNSC;
- d) nerespectarea de către entitățile esențiale și importante a obligației de a transmite datele solicitate conform art. 11 alin. (9) în termen de 30 de zile de la data comunicării cererii DNSC;
- e) nerespectarea de către entitățile esențiale și importante a obligației de a realiza și transmite autoevaluarea nivelului de maturitate conform art. 12 alin. (4), în termen de 30 de zile de la împlinirea termenului acordat;
- f) nerespectarea de către entitățile esențiale a obligației de a întocmi și transmite planul de măsuri pentru remedierea deficiențelor conform art. 12 alin. (5), în termen de 30 de zile de la împlinirea termenului acordat;
- g) nerespectarea de către organele de conducere ale entităților esențiale și importante a obligației de supraveghere a punerii în aplicare a măsurilor de gestionare a riscurilor conform art. 14 alin. (1);
- h) nerespectarea de către membrii organelor de conducere ale entităților esențiale și importante a obligației de a urma cursuri de formare profesională conform cu art. 14 alin. (2);
- i) nerespectarea de către organele de conducere ale entităților esențiale și importante a obligației de stabilire a mijloacelor permanente de contact conform art. 14 alin. (3);
- j) nerespectarea de către organele de conducere ale entităților esențiale și importante a obligației de alocare a resurselor conform art. 14 alin. (3);
- k) nerespectarea de către organele de conducere ale entităților esențiale și importante a obligației de desemnare a responsabililor cu securitatea rețelelor și sistemelor informatice conform art. 14 alin. (3) și cu îndeplinirea condițiilor prevăzute la art. 14 alin. (4), în termenele prevăzute la art. 18;
- l) nerespectarea de către entitățile esențiale și importante a obligației de raportare în temeiul art. 15 alin. (1) cu respectarea termenelor și condițiilor impuse conform art. 15;
- m) nerespectarea de către entitățile esențiale și importante a obligației de notificare a destinatarilor serviciilor conform art. 15 alin. (1);
- n) nerespectarea de către entitățile esențiale și importante a obligației de raportare a informațiilor conform art. 15 alin. (3) în termenele indicate;
- o) nerespectarea de către entitățile din sectoarele prevăzute în anexele 1 și 2 a obligației de notificare conform art. 18 alin. (2) în termenul indicat;
- p) nerespectarea de către entitățile din sectoarele prevăzute în anexele 1 și 2 a obligației de furnizare a informațiilor conform art. 18 alin. (3) în termenul indicat;
- q) nerespectarea de către entitățile esențiale și importante a obligației de transmitere a evaluării nivelului de risc conform art. 18 alin. (6) în termenul indicat;
- r) nerespectarea de către entitățile esențiale și importante a obligației de autoevaluare a nivelului de maturitate conform art. 18 alin. (7) în termenul indicat;
- s) nerespectarea de către entitățile esențiale și importante a obligației de comunicare a modificărilor conform art. 18 alin. (8) în termenele indicate;
- t) nerespectarea de către entitățile esențiale și importante a obligației de notificare conform art. 18 alin. (13) în termenul indicat;
- u) nerespectarea de către registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii a obligației de a colecta date conform art. 19 alin. (1);

- v) nerespectarea de către registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii a obligației de a stabili politici și proceduri conform art. 19 alin. (3);
 - w) nerespectarea de către registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii a obligației de a pune la dispoziția publicului date conform art. 19 alin. (4);
 - x) nerespectarea de către registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii a obligației de a oferi acces la date conform art. 19 alin. (8);
 - y) nerespectarea de către registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii a obligației de a pune la dispoziția publicului politicile și procedurile privind divulgarea datelor conform art. 19 alin. (9);
 - z) nerespectarea de către registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii a obligației de a răspunde la cererile de acces conform art. 19 alin. (9);
 - aa) nerespectarea de către CSIRT-uri a obligației de a se autoriza conform art. 34;
 - bb) nerespectarea de către producătorii și furnizorii de produse sau servicii TIC a obligației de a transmite informații conform art. 36 alin. (4);
 - cc) nerespectarea de către producătorii și furnizorii de produse sau servicii TIC a obligației de a remedia vulnerabilitățile conform art. 36 alin. (4) în termenul stabilit de comun acord;
 - dd) nerespectarea de către entitățile esențiale și importante a obligației de instituire de procese de management al vulnerabilităților conform art. 36 alin. (7);
 - ee) nerespectarea de către entitățile esențiale și importante a obligației de transmitere a rezultatelor auditului conform art. 46 alin. (8), în termenul indicat;
 - ff) nerespectarea de către entitățile esențiale și importante a obligației de informare atunci când aceasta a fost dispusă de către DNSC conform art. 48 alin. (4), în termenul indicat;
 - gg) nerespectarea de către CSIRT-urile proprii ale entităților esențiale și entităților importante, CSIRT-urile sectoriale, furnizorii de servicii specifice CSIRT și auditorii de securitate cibernetică a dispozițiilor emise de către DNSC conform art. 53 alin. (2), în termenele indicate;
 - hh) nerespectarea de către furnizorii de servicii de formare pentru securitate cibernetică pentru auditori și CSIRT-uri a dispozițiilor emise de către DNSC conform art. 54 alin. (2), în termenele indicate;
 - ii) nerespectarea de către auditorii de securitate cibernetică a obligației de transmitere de informații conform art. 55 alin. (2), în termen de 30 de zile de la împlinirea termenului acordat;
 - jj) nerespectarea de către entitățile esențiale și importante a obligației de întocmire și transmitere a planului de măsuri conform art. 57 alin. (8), în termenul indicat;
 - kk) nerespectarea de către entitățile esențiale și importante a obligației de implementare conform art. 57 alin. (9), în termenul asumat;
 - ll) nerespectarea de către entitățile esențiale și importante a obligației de notificare și punere la dispoziție a actelor doveditoare conform art. 57 alin. (10), în termenul indicat;
- (2) Prin derogare de la dispozițiile art. 8 alin. (2) lit. a) din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, cu modificările și completările ulterioare, sancțiunile sunt:
- a) pentru entitățile importante până la 7 000 000 euro în echivalentul în lei sau cel mult 1,4% din cifra de afaceri netă, în situația alin. (1) lit. a)-d), f)-m), dd) și jj);
 - b) pentru entitățile esențiale până la 10 000 000 euro în echivalentul în lei sau cel mult 2% din cifra de afaceri netă, în situația alin. (1) lit. a)-m), dd) și jj);
 - c) pentru entitățile importante de la 1 000 lei la 300 000 lei, în cazul alin. (1) lit. n)-t), ee)-ff), kk)-mm);
 - d) pentru entitățile esențiale de la 1 500 lei la 500 000 lei, în cazul alin. (1) lit. n)-t), ee)-ff), kk)-mm);
 - e) de la 1 000 lei la 100 000 lei, în cazul alin. (1) lit. u)-z), aa)-cc) și gg)-ii).
- (3) Cifra de afaceri netă prevăzută la alin. (2) este cea înregistrată de către entitatea importantă sau esențială în ultimul exercițiu financiar.
- (4) În vederea individualizării sancțiunii prevăzute la alin. (2), se iau în considerare criteriile prevăzute la art. 50 alin. (1), iar atunci când sunt aplicabile dispozițiile art. 50 alin. (2), cuantumul amenzii poate fi stabilit până la dublul limitelor prevăzute la alin. (2).

(5) Pentru persoanele juridice nou-înființate și pentru persoanele juridice care nu au înregistrat cifra de afaceri în exercițiul financiar anterior sancționării, amenda prevăzută la alin. (2) se stabilește în cuantum de minimum unu și maximum 50 de salarii minime brute pe economie.

(6) În măsura în care prezenta ordonanță de urgență nu prevede altfel, contravențiilor prevăzute la alin. (1) li se aplică dispozițiile Ordonanței Guvernului nr. 2/2001, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare.

(7) Prin derogare de la prevederile art. 16 alin. (1) și ale art. 28 alin. (1) din Ordonanța Guvernului nr. 2/2001, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, și ale art. 22 alin. (2) din Legea nr. 203/2018 privind măsuri de eficientizare a achitării amenzilor contravenționale, cu modificările ulterioare, în cazul sancțiunilor aplicate pentru săvârșirea contravențiilor prevăzute la alin. (1), contravenientul poate achita, în termen de cel mult 15 zile de la data înmânării sau comunicării actului de constatare a contravenției și de aplicare a sancțiunii, jumătate din cuantumul amenzii aplicate, agentul constatatator făcând mențiune despre această posibilitate în procesul-verbal, respectiv în decizia prin care se aplică sancțiunea.

Art. 61 - (1) Constatarea contravențiilor prevăzute la art. 60 alin. (1) se realizează conform dispozițiilor art. 46-50.

(2) Constatarea contravențiilor prevăzute la art. 60 alin. (1), se realizează de către DNSC sau de către personalul de control al autorităților competente sectorial conform alin. (1), pentru entitățile esențiale sau importante, după caz, care își desfășoară activitatea în domeniul de competență al acestor autorități, aplicarea sancțiunii realizându-se, în cazul autorităților competente sectorial, prin decizie a conducerii acestora, cu aplicarea în mod corespunzător a alin. (3)-(8).

(3) Decizia Directorului DNSC de constatare a contravenției și de aplicare a sancțiunii cuprinde următoarele:

- a) datele de identificare ale contravenientului;
- b) data săvârșirii faptei;
- c) descrierea faptei contravenționale și a împrejurărilor care au fost avute în vedere la individualizarea sancțiunii;
- d) indicarea temeiului legal potrivit căruia se stabilește și se sancționează contravenția;
- e) sancțiunea aplicată;
- f) termenul și modalitatea de plată a amenzii;
- g) termenul de exercitare a căii de atac și instanța de judecată competentă.

(4) Prin derogare de la prevederile art. 13 din OG nr. 2/2001, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, aplicarea sancțiunii stabilite în temeiul prezentei ordonanțe de urgență se prescrie în termen de trei ani de la data săvârșirii faptei. În cazul încălcărilor care durează în timp sau al celor constând în săvârșirea, în baza aceleiași rezoluții, la intervale diferite de timp, a mai multor acțiuni sau inacțiuni, care prezintă, fiecare în parte, conținutul aceleiași contravenții, prescripția începe să curgă de la data constatării sau de la data încetării ultimului act ori fapt săvârșit, dacă acest moment intervine anterior constatării.

(5) Contravenientului i se comunică și înștiințarea de plată, care conține mențiunea privind obligativitatea achitării amenzii în termen de 30 de zile de la data comunicării actului.

(6) Decizia de constatare a contravenției și de aplicare a sancțiunii prevăzută la alin. (1) și (2), neatacată în termenul prevăzut la alin. (8), precum și hotărârea judecătorească definitivă prin care s-a soluționat acțiunea în contencios administrativ constituie titlu executoriu, fără vreo altă formalitate. Acțiunea în contencios administrativ în condițiile prevăzute la alin. (8) suspendă executarea numai în ceea ce privește achitarea amenzii, până la pronunțarea de către instanța de judecată a unei hotărâri definitive.

(7) Sumele provenite din amenzile aplicate în conformitate cu dispozițiile prezentului articol se fac venit integral la bugetul de stat. Executarea se realizează în conformitate cu dispozițiile legale privind executarea silită a creanțelor fiscale. În vederea punerii în executare a sancțiunii, DNSC și autoritățile competente sectorial prevăzute la art. 37, comunică, din oficiu, organelor de specialitate ale Agenției Naționale de Administrare Fiscală, decizia de constatare a contravenției și de aplicare a sancțiunii

prevăzută la alin. (1) sau (2), neatacată în termenul prevăzut la alin. (8), după expirarea termenului prevăzut în înștiințarea de plată sau după rămânerea definitivă a hotărârii judecătorești prin care s-a soluționat acțiunea în contencios administrativ.

(8) Prin derogare de la dispozițiile art. 7 din Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare și de la dispozițiile art. 32 alin. (1) din OG nr. 2/2001, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, actele administrative, deciziile și deciziile de constatare a contravenției și de aplicare a sancțiunii adoptate potrivit dispozițiilor prezentei ordonanțe de urgență pot fi atacate în contencios administrativ la Curtea de Apel București, fără parcurgerea procedurii prealabile, în termen de 30 de zile de la comunicarea acestora.

Art. 62 - (1) DNSC informează ANSPDCP atunci când, în exercitarea competențelor sale de supraveghere și control conform dispozițiilor prezentei ordonanțe de urgență, constată aspecte specifice politicilor sau incidentelor de securitate cibernetică care pot avea impact în planul protecției datelor cu caracter personal.

(2) DNSC nu aplică dispozițiile art. 48 alin. (1) pentru fapte cu impact în planul protecției datelor cu caracter personal și care au fost anterior sancționate contravențional de către ANSPDCP.

(3) Prelucrările de date cu caracter personal ce intră sub incidența prezentei ordonanțe de urgență se efectuează cu respectarea reglementărilor legale privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

(4) Raportările realizate în temeiul prezentei ordonanțe de urgență nu afectează obligațiile operatorilor de date cu caracter personal stabilite potrivit art. 33 și 34 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE.

Art. 63 - DNSC informează instituțiile cu atribuții de coordonare a activității și control în domeniul protecției informațiilor clasificate astfel cum sunt acestea stabilite prin Legea nr. 182/2002 privind protecția informațiilor clasificate, cu modificările și completările ulterioare și actele normative subsecvente dacă se constată că incidentele de securitate cibernetică pot avea impact în planul protecției datelor și informațiilor secrete de stat sau secrete de serviciu.

Capitolul VIII - Dispoziții tranzitorii și finale

Art. 64 - Măsurile adoptate sau impuse de ANCOM în temeiul dispozițiilor din Capitolul IV din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată, cu modificări și completări, prin Legea nr. 140/2012, cu modificările și completările ulterioare, prin Decizia nr. 70/2024, rămân în vigoare până la revizuirea acestora.

Art. 65 - (1) Prin ordin al Directorului DNSC, care se publică în Monitorul Oficial al României, Partea I, se aprobă:

- a) Criteriile și pragurile de determinare a gradului de perturbare a unui serviciu și metodologia de evaluare a nivelului de risc al entităților, în temeiul art. 10 alin. (2), în termen de 20 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
- b) Măsurile de gestionare a riscurilor, în temeiul art. 12 alin. (1), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
- c) Normele metodologice privind raportarea incidentelor, în temeiul art. 15 alin. (17), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
- d) Cerințele privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor, în temeiul art. 18 alin. (10), în termen de 15 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;

- e) Planul de management al crizelor de securitate cibernetică la nivel național pe timp de pace, în temeiul art. 28 alin. (2), în termen de 180 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
 - f) Normele tehnice privind compatibilitatea și interoperabilitatea sistemelor, procedurilor și metodelor utilizate de către CSIRT-uri și criteriile de stabilire a numărului de persoane calificate, în temeiul art. 31 alin. (2), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
 - g) Pachetul minim de servicii de tip CSIRT, în temeiul art. 32 alin. (5), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
 - h) Regulamentul privind autorizarea și verificarea CSIRT-urilor, condițiile de valabilitate pentru autorizațiile acordate și tematicile pentru formarea personalului CSIRT-urilor, în temeiul art. 34 alin. (2) lit. a), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
 - i) Normele de aplicare și metodologia de prioritizare pe bază de risc a activităților de supraveghere, verificare și control, în temeiul art. 47 alin. (8), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
 - j) Regulamentul privind autorizarea, verificarea și revocarea furnizorilor de servicii de formare pentru securitate cibernetică pentru auditori și CSIRT-uri și condițiile de valabilitate pentru autorizațiile acordate acestora, în temeiul art. 54 alin. (3), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
 - k) Normele de aplicare a dispozițiilor privind supravegherea, verificarea și controlul pentru CSIRT-uri, furnizorii de servicii specifice CSIRT, precum și pentru auditorii de securitate cibernetică, în temeiul art. 56 alin. (2), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
 - l) Regulamentul privind atestarea și verificarea auditorilor de securitate cibernetică și condițiile de valabilitate pentru atestatele acordate, în temeiul art. 58 alin. (2) lit. b), în termen de 120 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I.
- (2) Prin decizie a Directorului DNSC, care se publică în Monitorul Oficial al României, Partea I, se aprobă:
- a) Tematicile pentru specializarea auditorilor în vederea atestării, în temeiul art. 58 alin. (2) lit. e), în termen de 180 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I;
 - b) Tematicile pentru specializarea personalului din cadrul CSIRT-urilor în vederea autorizării, în temeiul art. 31 alin. (3), în termen de 180 de zile de la data publicării prezentei ordonanțe de urgență în Monitorul Oficial al României, Partea I.

Art. 66 – La data intrării în vigoare a prezentei ordonanțe de urgență, se abrogă:

- a) Legea nr. 362 din 28 decembrie 2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, publicată în Monitorul Oficial al României nr. 21 din 9 ianuarie 2019 cu excepția măsurilor adoptate sau impuse în temeiul dispozițiilor din Capitolele IV și V, care rămân în vigoare până la revizuirea acestora, conform art. 65.
- b) art. 4 alin. (1) pct. 54¹ și 54², precum și Capitolul IV: Securitatea rețelelor și serviciilor de comunicații electronice din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, publicată în Monitorul Oficial al României, Partea I, nr. 925 din 27 decembrie 2011, aprobată cu modificări și completări prin Legea nr. 140/2012, cu modificările și completările ulterioare;
- c) Legea nr. 146/2014 privind autorizarea plății cotizațiilor la Forumul Internațional al Echipelor de Răspuns la Incidente de Securitate Cibernetică (Forum of Incident Response and Security Teams-FIRST) și la Forumul TF/CSIRT Trusted Introducer (TI) din cadrul Asociației Transeuropene a Rețelelor din Domeniul Cercetării și al Educației (Transeuropean Research and Education Network Association-TERENA) în scopul menținerii participării Centrului Național de Răspuns la Incidente de Securitate Cibernetică CERT-RO la aceste două organisme neguvernamentale, actualizată;

d) Legea nr. 106/2015 privind aprobarea Ordonanței Guvernului nr. 3/2015 pentru modificarea și completarea Legii nr. 146/2014 privind autorizarea plății cotizațiilor la Forumul Internațional al Echipelor de Răspuns la Incidente de Securitate Cibernetică (Forum of Incident Response and Security Teams - FIRST) și la Forumul TF/CSIRT Trusted Introducer (TI) din cadrul Asociației Transeuropene a Rețelelor din Domeniul Cercetării și al Educației (Transeuropean Research and Education Network Association - TERENA) în scopul menținerii participării Centrului Național de Răspuns la Incidente de Securitate Cibernetică CERT - RO la aceste două organisme neguvernamentale.

Art. 67 - Anexele nr. 1 „Sectoare cu o importanță critică ridicată” și nr. 2 „Alte sectoare de importanță critică” fac parte integrantă din prezenta lege.

* *

*

Prezenta ordonanță de urgență transpune Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (Text cu relevanță pentru SEE), publicată în Jurnalul Oficial al Uniunii Europene (JOUE) nr. L333/80 din 27 decembrie 2022.

Ion-Marcel CIOLACU

PRIM-MINISTRU

Sectoare cu o importanță critică ridicată

Sectorul	Sub-sectorul	Tipul de entitate
1. Energie	(a) Electricitate	— Întreprinderile din domeniul energiei electrice, astfel cum sunt definite ca “operatori economici” la art. 3 pct. 73 din Legea nr. 123/2012 a energiei electrice și a gazelor naturale, care îndeplinesc funcția de „furnizare de energie electrică”, astfel cum este definită la art. 3 pct. 46 din Legea nr. 123/2012 a energiei electrice și a gazelor naturale
		— Operatorii de distribuție, astfel cum sunt definiți la art. 3 pct. 70 din Legea nr. 123/2012 a energiei electrice și a gazelor naturale
		— Operatorii de transport și de sistem, astfel cum sunt definiți la art. 3 pct. 71 din Legea nr. 123/2012 a energiei electrice și a gazelor naturale
		— Producătorii, astfel cum sunt definiți ca “producători de energie electrică” la art. 3 pct. 92 din Legea nr. 123/2012 a energiei electrice și a gazelor naturale
		— Operatorii desemnați ai pieței de energie electrică, astfel cum sunt definiți la art. 3 pct. 68 din Legea nr. 123/2012 a energiei electrice și a gazelor naturale
		— Participanții la piață, astfel cum sunt definiți la art. 3 pct. 79 din Legea nr. 123/2012 a energiei electrice și a gazelor naturale, care furnizează serviciile de agregare, consum dispecerizabil sau stocare de energie, astfel cum sunt definite la art. 3 pct. 6, 29 și respectiv 121 din aceeași lege.
		— Operatorii unui punct de reîncărcare, astfel cum este definit la art. 3 pct. 96 din Legea nr. 123/2012 a energiei electrice și a gazelor naturale, care sunt responsabili cu gestionarea și exploatarea unui punct de reîncărcare care furnizează un serviciu de reîncărcare clienților finali, astfel cum sunt definiți la art. 3 pct. 20 din aceeași lege, inclusiv în numele și în contul unui furnizor de servicii de mobilitate, astfel cum aceștia sunt definiți la Articolul 3 pct. 36 din Regulamentul (UE) 2023/1804 al Parlamentului European și al Consiliului din 13 septembrie 2023 privind instalarea infrastructurii pentru combustibili alternativi și de abrogare a Directivei 2014/94/UE
	(b) Încălzire centralizată și răcire centralizată	— Operatorii de încălzire centralizată sau răcire centralizată, astfel cum este definită la art. 2 lit. t din Legea nr. 220 din 27 octombrie 2008 (republicată) pentru stabilirea sistemului de promovare a producerii energiei din surse regenerabile de energie, cu modificările și completările ulterioare
	(c) Petrol	— Operatorii de conducte de transport al petrolului, astfel cum sunt definiți ca „transportatori” la art. 2 pct. 42 din Legea nr. 238 din 7 iunie 2004 a petrolului, cu modificările și completările ulterioare
		— Operatorii instalațiilor de producție, de rafinare și de tratare a petrolului, de depozitare și de transport
		— Entitățile centrale de stocare, astfel cum sunt definite la art. 2 lit. m) și n) din Legea nr. 85 din 30 martie 2018 privind constituirea și menținerea unor rezerve minime de țiței și/sau produse petroliere

2. Transport	(d) Gaze	— Întreprinderile de furnizare, astfel cum sunt definite ca „furnizori” la art. 100 pct. 44 din Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		— Operatorii de distribuție, astfel cum sunt definiți la art. 100 pct. 63 din Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		— Operatorii de transport și de sistem, astfel cum sunt definiți la art. 100 pct. 65 din Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		— Operatorii de înmagazinare, astfel cum sunt definiți la art. 100 pct. 64 din Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		— Operatorii de sistem GNL, astfel cum sunt definiți, ca “operatori ai terminalului GNL”, la art. 100 pct. 60 din Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		— Întreprinderile din sectorul gazelor naturale, astfel cum sunt definite, ca „operatori economici din sectorul gazelor naturale” la art. 100 pct. 67 din Legea nr. 123 din 10 iulie 2012 a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		— Operatorii de instalație de rafinare și de tratare a gazelor naturale
	(e) Hidrogen	— Operatorii de producție, stocare și transport de hidrogen
	(a) Transport aerian	— Transportatorii aerieni, astfel cum sunt definiți la art. 3 pct. 51 din Codul Aerian din 18 martie 2020, cu modificările și completările ulterioare, utilizați în scop comercial
		— Organele de administrare a aeroporturilor, astfel cum sunt definite ca “administratori ai aerodromului” la art. 3 pct. 6 din Codul Aerian din 18 martie 2020, cu modificările și completările ulterioare, aeroporturile, astfel cum sunt definite la art. 3 pct. 13 din aceeași lege, inclusiv aeroporturile principale enumerate în secțiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului din 11 decembrie 2013 privind orientările Uniunii pentru dezvoltarea rețelei transeuropene de transport și de abrogare a Deciziei nr. 661/2010/UE, precum și entitățile care operează instalații auxiliare în cadrul aeroporturilor
		— Operatorii de control al gestionării traficului care prestează servicii de control al traficului aerian (ATC), astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului din 10 martie 2004 de stabilire a cadrului pentru crearea cerului unic european (regulament-cadru)
		— Operatori mentenanță aeronave
		— Agenți aeronautici civili, astfel cum sunt definiți, ca “agenți aeronautici” la art. 3 pct. 15 din Codul Aerian din 18 martie 2020, cu modificările și completările ulterioare
	(b) Transport feroviar	— Administratorii infrastructurii, astfel cum sunt definiți la art. 3 pct. 3 din Legea nr. 202 din 4 noiembrie 2016 privind integrarea sistemului feroviar din România în spațiul feroviar unic european, cu modificările și completările ulterioare

		— Întreprinderile feroviare, astfel cum sunt definite ca “operatori de transport feroviar” la art. 3 pct. 18 din din Legea nr. 202 din 4 noiembrie 2016 privind integrarea sistemului feroviar din România în spațiul feroviar unic european, cu modificările și completările ulterioare, inclusiv operatorii unei infrastructuri de servicii, astfel cum sunt definiți la art. 3 pct. 19 din aceeași lege
	(c) Transport pe apă	— Companiile de transport de mărfuri și pasageri pe ape interioare, maritime și de coastă, astfel cum sunt definite pentru transportul maritim în anexa I la Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului din 31 martie 2004 privind consolidarea securității navelor și a instalațiilor portuare, fără a include navele individuale operate de companiile respective — Organele de gestionare a porturilor, astfel cum sunt definite la art. 3 din Ordinul ministrului transporturilor nr. 290/2007 pentru introducerea măsurilor de întărire a securității portuare, inclusiv instalațiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004, și entitățile care realizează lucrări și operează echipamente în cadrul porturilor — Operatorii de servicii de trafic maritim (STM), astfel cum sunt definiți la art. 3 lit. t) din Hotărârea Guvernului nr. 1016/2010 pentru stabilirea Sistemului de informare și monitorizare a traficului navelor maritime care intră/ies în/din apele naționale navigabile ale României, cu modificările și completările ulterioare
	(d) Transport rutier	— Autoritățile rutiere, astfel cum sunt definite la articolul 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 și a Consiliului în ceea ce privește prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic responsabile cu controlul gestionării traficului, cu excepția entităților publice în cazul cărora gestionarea traficului sau exploatarea sistemelor de transport inteligente reprezintă doar o parte neesențială a activității lor generale — Operatorii de sisteme de transport inteligente, astfel cum sunt definite la art. 4 lit. a din Ordonanța Guvernului nr. 7 din 25 ianuarie 2012 privind implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru realizarea interfețelor cu alte moduri de transport
3. Sectorul bancar		Instituțiile de credit, astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudenciale pentru instituțiile de credit și societățile de investiții și de modificare a Regulamentului (UE) nr. 648/2012
4. Infrastructuri ale pieței financiare		— Operatorii de locuri de tranzacționare, astfel cum sunt definite la articolul 3 alin. 1 pct. 40 din Legea nr. 126 din 11 iunie 2018 privind piețele de instrumente financiare — Contrapărțile centrale (CPC), astfel cum sunt definite la art. 3 alin. (1) pct. 16 din Legea nr. 126 din 11 iunie 2018 privind piețele de instrumente financiare, cu modificările și completările ulterioare
5. Sectorul sănătății		— Furnizorii de servicii medicale, astfel cum sunt definiți de art. 347 lit. c din Legea nr. 95 din 14 aprilie 2006 (republicată) privind reforma în domeniul sănătății, cu modificările și completările ulterioare

		— Laboratoarele de referință ale UE, astfel cum sunt definite la articolul 15 din Regulamentul (UE) 2022/2371 al Parlamentului European și al Consiliului din 23 noiembrie 2022 privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 1082/2013/UE — Entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor — Entitățile care fabrică produse farmaceutice de bază și preparate farmaceutice menționate în secțiunea C diviziunea 21 din NACE Rev. 2 — Entitățile care fabrică dispozitive medicale considerate a fi esențiale în contextul unei urgențe de sănătate publică (lista dispozitivelor esențiale pentru urgența de sănătate publică) în sensul articolului 22 din Regulamentul (UE) 2022/123 al Parlamentului European și al Consiliului din 25 ianuarie 2022 privind consolidarea rolului Agenției Europene pentru Medicamente în ceea ce privește pregătirea pentru situații de criză în domeniul medicamentelor și al dispozitivelor medicale și gestionarea acestora
6. Apă potabilă		Furnizorii și distribuitorii de apă, astfel cum sunt definiți ca „furnizori de apă” la art. 2 pct. c din Ordonanța nr. 7 din 18 ianuarie 2023 privind calitatea apei destinate consumului uman, cu modificările și completările ulterioare, destinată consumului uman, astfel cum aceasta este definită la art. 2 pct. a din aceeași Ordonanță, mai puțin apa folosită în orice unitate de tip alimentar pentru producerea, prelucrarea, conservarea sau comercializarea produselor sau substanțelor destinate consumului uman și excluzând distribuitorii pentru care distribuția de apă destinată consumului uman reprezintă o parte neesențială din activitatea lor generală de distribuție a altor produse de bază și bunuri care nu sunt considerate servicii esențiale
7. Ape uzate		Întreprinderile care colectează, evacuează sau tratează ape uzate urbane, ape uzate menajere sau ape uzate industriale, astfel cum acestea sunt definite la art. 2 pct. 1,2 și respectiv 3 din Anexa 1 - Norme Tehnice din 28 februarie 2002 privind colectarea, epurarea și evacuarea apelor uzate urbane, NTPA-011 la Hotărârea nr. 188 din 28 februarie 2002 pentru aprobarea unor norme privind condițiile de descărcare în mediul acvatic a apelor uzate, cu excepția întreprinderilor pentru care colectarea, evacuarea sau tratarea apelor uzate urbane, a apelor uzate menajere sau a apelor uzate industriale reprezintă o parte neesențială a activității lor generale
8. Infrastructură digitală		— Furnizorii de IXP (internet exchange point) — Furnizorii de servicii DNS, cu excepția operatorilor de servere pentru nume primare — Registrele de nume TLD — Furnizorii de servicii de cloud computing — Furnizorii de servicii de centre de date — Furnizorii de rețele de difuzare de conținut — Prestatorii de servicii de încredere — Furnizorii de rețele publice de comunicații electronice

		— Furnizorii de servicii de comunicații electronice accesibile publicului
9. Gestionarea serviciilor TIC (business-to-business)		— Furnizorii de servicii gestionate — Furnizorii de servicii de securitate gestionate
10. Administrație publică		— Entitățile administrației publice centrale, cu excepția celor din SNAOPSN, instituțiile de învățământ superior, domeniul juridicar, justiție, inclusiv Ministerul Public, ORNISS, Parlamentul României, Guvernul României, Administrația Prezidențială, ASF, BNR și ANCOM.
11. Spațiu		Operatorii de infrastructură terestră deținută, gestionată și operată de statul român sau de entități private pe teritoriul României, care sprijină furnizarea de servicii spațiale, cu excepția furnizorilor de rețele publice de comunicații electronice

Alte sectoare de importanță critică

Sectorul	Sub-sectorul	Tipul de entitate
1. Servicii poștale și de curierat		Furnizorii de servicii poștale, astfel cum sunt definiți la art. 2 pct. 2 din Ordonanța de Urgență nr. 13 din 6 martie 2013 privind serviciile poștale, cu modificările și completările ulterioare, inclusiv furnizori de servicii de curierat
2. Gestionarea deșeurilor		Întreprinderile care efectuează gestionarea deșeurilor, astfel cum aceasta este definită la pct. 19 din Anexa nr. 1 la Ordonanța de Urgență nr. 92 din 19 august 2021 privind regimul deșeurilor, cu modificările și completările ulterioare, cu excepția întreprinderilor pentru care gestionarea deșeurilor nu reprezintă principala activitate economică
3. Fabricarea, producția și distribuția de substanțe chimice		Întreprinderile care produc substanțe și distribuie substanțe sau amestecuri, astfel cum se menționează la articolul 3 punctele 9 și 14 din Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului din 18 decembrie 2006 privind înregistrarea, evaluarea, autorizarea și restricționarea substanțelor chimice (REACH), de înființare a Agenției Europene pentru Produse Chimice, de modificare a Directivei 1999/45/CE și de abrogare a Regulamentului (CEE) nr. 793/93 al Consiliului și a Regulamentului (CE) nr. 1488/94 al Comisiei, precum și a Directivei 76/769/CEE a Consiliului și a Directivelor 91/155/CEE, 93/67/CEE, 93/105/CE și 2000/21/CE ale Comisiei și întreprinderile care produc articole, astfel cum sunt definite la articolul 3 punctul 3 din regulamentul respectiv, din substanțe sau amestecuri
4. Producția, prelucrarea și distribuția de alimente		Întreprinderile cu profil alimentar, așa cum sunt definite la articolul 3 punctul (2) din Regulamentul (CE) nr. 178/2002 al Parlamentului European și al Consiliului din 28 ianuarie 2002 de stabilire a principiilor și a cerințelor generale ale legislației alimentare, de instituire a Autorității Europene pentru Siguranța Alimentară și de stabilire a procedurilor în domeniul siguranței produselor alimentare, care sunt implicate în distribuția cu ridicata și în producția și prelucrarea industrială
5. Fabricare	(a) Fabricarea de dispozitive medicale și de dispozitive medicale pentru diagnostic in vitro	Entitățile care fabrică dispozitive medicale, astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului, și entități care fabrică dispozitive medicale pentru diagnostic in vitro, astfel cum sunt definite la articolul 2 punctul 2 din Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic in vitro și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei, cu excepția entităților care fabrică dispozitive medicale menționate în anexa I punctul 5 a cincea liniuță din prezenta directivă
	(b) Fabricarea computerelor și a	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în diviziunea 26 din CAEN Rev. 2

	produselor electronice și optice	
	(c) Fabricarea echipamentelor electrice	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în diviziunea 27 din CAEN Rev. 2
	(d) Fabricarea altor mașini și echipamente n.c.a.	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în diviziunea 28 din CAEN Rev. 2
	(e) Fabricarea autovehiculelor, remorcilor și semiremorcilor	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în diviziunea 29 din CAEN Rev. 2
	(f) Fabricarea altor echipamente de transport	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în diviziunea 30 din CAEN Rev. 2
6. Furnizori digitali		— Furnizorii de piețe online
		— Furnizorii de motoare de căutare online
		— Furnizorii de platforme de servicii de socializare în rețea
7. Cercetare		Organizațiile de cercetare