**Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice**

Legea 362/2018 din 2019.01.09

Status: Acte în vigoare

Versiune de la: 31 Decembrie 2024

**Intră în vigoare:**
12 Ianuarie 2019 An

# Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice

Dată act: 28-dec-2018

**Emitent: Parlamentul**

**Parlamentul României** adoptă prezenta lege.

## CAPITOLUL I:

[textul din capitolul I a fost abrogat la 31-dec-2024 de Art. 66, alin. (1), litera A. din capitolul X din Ordonanta urgenta 155/2024]

## CAPITOLUL II:

[textul din capitolul II a fost abrogat la 31-dec-2024 de Art. 66, alin. (1), litera A. din capitolul X din Ordonanta urgenta 155/2024]

## CAPITOLUL III:

[textul din capitolul III a fost abrogat la 31-dec-2024 de Art. 66, alin. (1), litera A. din capitolul X din Ordonanta urgenta 155/2024]

## CAPITOLUL IV:Asigurarea securităţii reţelelor şi sistemelor informatice

### SECŢIUNEA 1:Cerinţele minime de securitate

**Art. 25**

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

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

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

a)managementul drepturilor de acces;

b)conştientizarea şi instruirea utilizatorilor;

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

d)testarea şi evaluarea securităţii reţelelor şi sistemelor informatice;

e)managementul configuraţiilor reţelelor şi sistemelor informatice;

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

g)managementul continuităţii funcţionării serviciului esenţial;

h)managementul identificării şi autentificării utilizatorilor;

i)răspunsul la incidente;

j)mentenanţa reţelelor şi sistemelor informatice;

k)managementul suporturilor de memorie externă;

l)asigurarea protecţiei fizice a reţelelor şi sistemelor informatice;

m)realizarea planurilor de securitate;

n)asigurarea securităţii personalului;

o)analizarea şi evaluarea riscurilor;

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

q)managementul vulnerabilităţilor şi alertelor de securitate.

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

a)securitatea sistemelor şi a instalaţiilor;

b)gestionarea incidentelor;

c)gestionarea continuităţii activităţii;

d)monitorizarea, auditarea şi testarea;

e)conformitatea cu standardele europene şi internaţionale.

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

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

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

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

d)previn accesul neautorizat la reţelele şi sistemele informatice;

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

f)implementează un sistem de management al riscului;

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

h)asigură continuitatea serviciilor.

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

## SECŢIUNEA 2: Notificarea incidentelor de securitate

**Art. 26**

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

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

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

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

b)descrierea incidentului;

c)perioada de desfăşurare a incidentului;

d)impactul estimat al incidentului;

e)măsuri preliminare adoptate;

f)lista de autorităţi ale statului afectate de incident;

g)întinderea geografică potenţială a incidentului;

h)date despre efecte potenţial transfrontaliere ale incidentului.

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

a)informaţii clasificate;

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

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

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

(7)Notificările privind incidentele ce fac obiectul prezentei legi pot fi făcute şi de către echipele CSIRT ale entităţilor de drept public sau privat ori care deservesc un anumit sector de activitate ori de către furnizorii de servicii de securitate aflaţi în relaţie contractuală, conform atribuţiilor ce le revin în baza actului de înfiinţare ori a contractului de prestări servicii, după caz.

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

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

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

(11)DNSC tratează notificările obligatorii cu prioritate faţă de notificările voluntare.

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

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

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

## SECŢIUNEA 3: Managementul incidentelor

### Art. 27

După primirea notificării, DNSC, în calitate de CSIRT naţional:

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

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

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

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

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

f)poate lua măsurile prevăzute la art. 41;

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

### Art. 28

(1)**Impactul unui incident se determină ţinând cont cel puţin de următorii parametri:**

1. **(i)în cazul operatorilor de servicii esenţiale:**

a)numărul de utilizatori afectaţi de perturbarea serviciului esenţial;

b)durata incidentului;

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

2. **(ii) în cazul furnizorilor de servicii digitale:**

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

b)durata incidentului;

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

d)amploarea perturbării funcţionării serviciului;

e)amploarea impactului asupra activităţilor economice şi societale.

(2)DNSC, după consultarea GdLINIS, elaborează şi actualizează normele tehnice de stabilire a impactului pentru categoriile de operatori şi furnizori prevăzuţi de prezenta lege care se aprobă prin hotărâre a Guvernului iniţiată de Directoratul Naţional de Securitate Cibernetică.

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

**Art. 29**

(1)DNSC poate înştiinţa publicul, atunci când informarea este necesară pentru a preveni un incident sau pentru a se administra un incident în curs.

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

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

**Art. 30**

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

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

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

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

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

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

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

(8)În scopul îndeplinirii atribuţiilor ori furnizării serviciilor prevăzute de prezenta lege, precum şi în scopul prevenirii şi răspunsului la incidentele de securitate informatică ori al cooperării la nivel naţional, comunitar şi internaţional în prevenirea şi răspunsul la incidentele de securitate informatică, DNSC colectează, primeşte, prelucrează şi transmite date şi informaţii ce pot constitui sau pot conţine date cu caracter personal, în limitele legislaţiei aplicabile, cu asigurarea respectării prevederilor alin. (6).

## CAPITOLUL V:Audit şi autorizare

### SECŢIUNEA 1:Auditul de securitate a reţelelor şi sistemelor informatice aparţinând operatorilor de servicii esenţiale sau furnizorilor de servicii digitale

**Art. 31**

Poate fi auditor de securitate a reţelelor şi sistemelor informatice persoana fizică sau persoana juridică ce realizează audit de securitate a reţelelor şi sistemelor informatice, adică desfăşoară acea activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor şi măsurilor de protecţie implementate la nivelul reţelelor şi sistemelor informatice, în vederea identificării disfuncţiilor şi vulnerabilităţilor şi a furnizării unor soluţii de remediere a acestora.

**Art. 32**

(1)Auditul de securitate specificat la art. 8 alin. (4), respectiv art. 10 alin. (2) lit. b) şi art. 12 alin. (2) lit. b) se realizează de către auditorii de securitate informatică ce deţin atestat valabil eliberat de către DNSC pentru a audita reţele şi sisteme informatice ce deservesc servicii esenţiale sau servicii digitale în sensul prezentei legi.

(2)**În acest sens DNSC:**

a)întreţine şi actualizează Registrul auditorilor menţionaţi la alin. (1);

b)elaborează şi transmite spre aprobare Directoratului Naţional de Securitate Cibernetică, în conformitate cu prevederile art. 20 lit. e) şi s), regulamentul pentru atestarea şi verificarea auditorilor de securitate informatică pentru reţelele şi sistemele informatice aparţinând operatorilor de servicii esenţiale sau furnizorilor de servicii digitale şi stabileşte condiţiile de valabilitate pentru atestatele acordate;

c)acordă, prelungeşte, suspendă sau retrage atestarea pentru auditorii de securitate informatică pentru reţelele şi sistemele informatice aparţinând operatorilor de servicii esenţiale sau furnizorilor de servicii digitale, în conformitate cu prevederile regulamentului prevăzut la lit. b);

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

e)elaborează şi aprobă, prin decizie a directorului general publicată în Monitorul Oficial al României, Partea I, tematicile pentru specializarea auditorilor în vederea atestării prevăzute la lit. c) şi autorizează, verifică, suspendă sau retrage autorizarea formatorilor din domeniul auditului de securitate informatică pentru reţelele şi sistemele informatice ale operatorilor de servicii esenţiale şi furnizorilor de servicii digitale.

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

a)auditorii atestaţi care asigură în mod curent servicii de securitate informatică ori servicii de tip

CSRIT operatorului de servicii esenţiale sau furnizorului de servicii digitale ori sunt angajaţi ai acestora;
b)auditorul care are un contract de prestări servicii pentru reţeaua şi sistemul supus auditului aflat în desfăşurare la momentul la care se efectuează auditul sau într-un termen mai mic de un an;
c)auditorul care a mai efectuat 3 audituri consecutive la acelaşi operator de servicii esenţiale sau furnizor de servicii digitale.

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

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

(6)Atestatele au o valabilitate de 3 ani.

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

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

## SECŢIUNEA 2: Autorizarea echipelor CSIRT ce deservesc reţele şi sisteme informatice din categoria serviciilor esenţiale şi serviciilor digitale

**Art. 33**

(1)Echipele CSIRT care deservesc operatori de servicii esenţiale ori furnizori de servicii digitale se autorizează de către DNSC în calitate de autoritate competentă la nivel naţional.

(2)**În acest sens DNSC:**
a)întreţine şi actualizează Registrul echipelor CSIRT prevăzute la alin. (1);
b)elaborează şi transmite spre aprobare Directoratului Naţional de Securitate Cibernetică, în conformitate cu prevederile art. 20 lit. e) şi s), regulamentul pentru autorizarea şi verificarea echipelor CSIRT care deservesc operatorii de servicii esenţiale sau furnizorii de servicii digitale şi stabileşte condiţiile de valabilitate pentru autorizaţiile acordate;

c)acordă, prelungeşte, suspendă sau retrage autorizarea pentru echipele CSIRT, în conformitate cu prevederile regulamentului prevăzut la lit. b);
d)verifică în urma sesizărilor sau din oficiu, în conformitate cu prevederile art. 35-42, îndeplinirea de către echipele CSIRT autorizate în temeiul prezentei legi a obligaţiilor legale ce le revin;
e)elaborează tematicile pentru formarea membrilor echipelor CSIRT în vederea autorizării prevăzute la lit. c) şi autorizează, verifică, suspendă sau retrage autorizarea formatorilor din domeniul asigurării de servicii de tip CSIRT pentru reţelele şi sistemele informatice ale operatorilor de servicii esenţiale şi furnizorilor de servicii digitale.

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

(4)Autorizaţiile au o valabilitate de 3 ani.

## CAPITOLUL VI:

[textul din capitolul VI a fost abrogat la 31-dec-2024 de Art. 66, alin. (1), litera A. din capitolul X din Ordonanta urgenta 155/2024]

## CAPITOLUL VII:

[textul din capitolul VII a fost abrogat la 31-dec-2024 de Art. 66, alin. (1), litera A. din capitolul X din Ordonanta urgenta 155/2024]

## CAPITOLUL VIII:

[textul din capitolul VIII a fost abrogat la 31-dec-2024 de Art. 66, alin. (1), litera A. din capitolul X din Ordonanta urgenta 155/2024]

## CAPITOLUL IX:

[textul din capitolul IX a fost abrogat la 31-dec-2024 de Art. 66, alin. (1), litera A. din capitolul X din Ordonanta urgenta 155/2024]

-****-

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

| |
|---|
| p. PREŞEDINTELE CAMEREI DEPUTAŢILOR, |

**FLORIN IORDACHE**

PREŞEDINTELE SENATULUI

**CĂLIN-CONSTANTIN-ANTON POPESCU-TĂRICEANU**

**ANEXĂ:Sectoare de activitate şi tipuri de entităţi**

| Sectorul | Subsectorul | Tipul de entitate |
|---|---|---|
| 1. Energie | a) electricitate | - operatori economici din domeniul energiei electrice, astfel cum sunt definiţi la art. 3 pct. 42 din Legea energiei electrice şi a gazelor naturale nr. 123/2012, cu modificările şi completările ulterioare; |
| | | - operatori de distribuţie, astfel cum sunt definiţi la art. 3 pct. 39 din Legea nr. 123/2012, cu modificările şi completările ulterioare; |
| | | - operatori de transport şi de sistem, astfel cum sunt definiţi la art. 3 pct. 40 din Legea nr. 123/2012, cu modificările şi completările ulterioare; |
| | b) petrol | - operatori de conducte de transport al petrolului; |
| | | - operatori ai instalaţiilor de producţie, de rafinare şi de tratare a petrolului, de depozitare şi de transport; |
| | c) gaze naturale | - furnizori persoane fizice sau juridice, astfel cum sunt definiţi la art. 100 pct. 44 din Legea nr. 123/2012, cu modificările şi completările ulterioare; |
| | | - operatori de distribuţie, astfel cum sunt definiţi la art. 100 pct. 63 din Legea nr. 123/2012, cu modificările şi completările ulterioare; |
| | | - operatori de transport şi de sistem, astfel cum sunt definiţi la art. 100 pct. 65 din Legea nr. 123/2012, cu modificările şi completările ulterioare; |
| | | - operatori de înmagazinare, astfel cum sunt definiţi la art. 100 |

| | | |
|---|---|---|
| | | pct. 64 din Legea nr. 123/2012, cu modificările şi completările ulterioare; |
| | | - operatori ai terminalelor GNL, astfel cum sunt definiţi la art. 100 pct. 60 din Legea nr. 123/2012, cu modificările şi completările ulterioare; |
| | | - operatori economici din sectorul gazelor naturale, astfel cum sunt definiţi la art. 100 pct. 67 din Legea nr. 123/2012, cu modificările şi completările ulterioare; |
| | | - operatori de instalaţie de rafinare şi de tratare a gazelor naturale |
| 2. Transport | a) transport aerian | - transportatori aerieni, astfel cum sunt definiţi la art. 3 pct. 4 din Regulamentul (CE) nr. 300/2008 al Parlamentului European şi al Consiliului din 11 martie 2008 privind norme comune în domeniul securităţii aviaţiei civile şi de abrogare a Regulamentului (CE) nr. 2.320/2002; |
| | | - organe de administrare a aeroportului, astfel cum sunt definite la art. 4 din Hotărârea Guvernului nr. 455/2011 privin d tarifele de aeroport, inclusiv aeroporturile principale enumerate în secţiunea 2 din anexa II la Regulamentul (UE) nr. 1.315/2013 al Parlamentului European şi al Consiliului din 11 decembrie 2013 privind orientările Uniunii pentru dezvoltarea reţelei transeuropene de transport şi de abrogare a Deciziei nr. 661/2010/UE, precum şi entităţi care operează instalaţii auxiliare în cadrul aeroporturilor; |
| | | - operatori de control al gestionării traficului care prestează servicii de control al traficului aerian (ATC), astfel cum sunt definite la art. 2 pct. 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European şi al Consiliului din 10 martie 2004 de stabilire a cadrului pentru crearea cerului unic European (regulament-cadru); |

| | | |
|---|---|---|
| | b) transport feroviar | - administratori de infrastructuri, astfel cum sunt definiţi la art. 3 pct. 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spaţiul feroviar unic european; |
| | | - întreprinderi feroviare, astfel cum sunt definite la art. 3 pct. 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spaţiul feroviar unic european; |
| | c) transport pe apă | - companii de transport de mărfuri şi pasageri pe ape interioare, maritime şi de coastă, astfel cum sunt definite pentru transportul maritim în anexa I la Regulamentul (CE) nr. 725/2004 al Parlamentului European şi al Consiliului din 31 martie 2004 privind consolidarea securităţii navelor şi a instalaţiilor portuare, fără a include navele individuale operate de companiile respective; |
| | | - organe de gestionare a porturilor, astfel cum sunt definite la art. 3 din Ordinul ministrului transporturilor nr. 290/2007 pent ru introducerea măsurilor de întărire a securităţii portuare, inclusiv instalaţiile portuare ale acestora, astfel cum sunt definite la art. 2 pct. 11 din Regulamentul (CE) nr. 725/2004, şi entităţile care operează lucrări şi echipamente în cadrul porturilor; |
| | | - operatori de servicii de trafic naval, astfel cum sunt definiţi la art. 3 din Hotărârea Guvernului nr. 1.016/2010 pentru stabilirea Sistemului de informare şi monitorizare a traficului navelor maritime care intră/ies în/din apele naţionale navigabile ale României, cu modificările şi completările ulterioare; |
| | d) transport rutier | - autorităţi rutiere, astfel cum sunt definite la art. 2 pct. 12 din Regulamentul delegat (UE) 2015/962 al Comisiei din 18 decembrie 2014 de completare a Directivei 2010/40/UE a Parlamentului European şi a Consiliului în ceea ce priveşte prestarea la nivelul UE a unor servicii de informare în timp |

| | | |
|---|---|---|
| | | real cu privire la trafic, responsabile pentru controlul gestionării traficului; |
| | | - operatori de sisteme de transport inteligente, astfel cum sunt definiţi la art. 4 din Ordonanţa Guvernului nr. 7/2012 privind implementarea sistemelor de transport inteligente în domeniul transportului rutier şi pentru realizarea interfeţelor cu alte moduri de transport, aprobată prin Legea nr. 221/2012 |
| 3. Sectorul bancar | | - instituţii de credit, astfel cum sunt definite la art. 4 pct. 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European şi al Consiliului din 26 iunie 2013 privind cerinţele prudenţiale pentru instituţiile de credit şi societăţile de investiţii şi de modificare a Regulamentului (UE) nr. 648/2012 |
| 4. Infrastructuri ale pieţei financiare | | - operatori de locuri de tranzacţionare, astfel cum sunt definite la art. 4 pct. 24 din Directiva 2014/65/UE a Parlamentului European şi a Consiliului din 15 mai 2014 privind pieţele instrumentelor financiare şi de modificare a Directivei 2002/92/CE şi a Directivei 2011/61/UE; |
| | | - contrapartide centrale, astfel cum sunt definite la art. 2 pct. 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European şi al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărţile centrale şi registrele centrale de tranzacţii |
| 5. Sectorul sănătăţii | instituţii de asistenţă medicală (inclusiv spitale şi clinici private) | - furnizori de servicii medicale, astfel cum sunt definiţi în Hotărârea Guvernului nr. 304/2014 pentru aprobarea Normelor metodologice privind asistenţa medicală transfrontalieră, cu modificările ulterioare |
| 6. Furnizarea şi distribuirea de apă potabilă | | - furnizori şi distribuitori de apă destinată consumului uman, astfel cum sunt definiţi la art. 2 din Legea nr. 458/2002 privind calitatea apei potabile, republicată, cu modificările şi |

| | | |
|---|---|---|
| | | completările ulterioare, excluzând distribuitorii pentru care distribuţia de apă destinată consumului uman reprezintă doar o parte din activitatea lor generală de distribuire a altor produse de bază şi produse care nu sunt considerate servicii esenţiale |
| 7. Infrastructură digitală | | - IXP; |
| | | - DNS; |
| | | - TLD |

Publicat în Monitorul Oficial cu numărul 21 din data de 9 ianuarie 2019