TABEL DE CONCORDANȚĂ

1. Directiva UE care se transpune:

Directiva (UE) 2022/2555 a PARLAMENTULUI EUROPEAN ŞI 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 şi a Directivei (UE) 2018/1972 şi de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2)

2. Actul normativ care asigură transpunerea directivei:

Ordonanța de urgență nr. (...) privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil

DIRECTIVA (UE) 2022/2555 A PARLAMENTULUI EUROPEAN ŞI 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 şi a Directivei (UE) 2018/1972 şi de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2)		**Ordonanța de urgență nr. (...) privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil**		**Observații**
Art. 1	(1) Prezenta directivă stabileşte măsuri care vizează obținerea unui nivel comun ridicat de securitate cibernetică în Uniune, cu scopul de a îmbunătăți funcționarea pieței interne.	Art. 1	Art. 1 Prezenta ordonanță de urgență stabileşte cadrul juridic şi instituțional, măsurile şi mecanismele necesare pentru asigurarea unui nivel comun ridicat de securitate cibernetică la nivel național.	
	(2) În acest scop, prezenta directivă stabileşte:			
	a) obligațiile statelor membre de a adopta strategii naționale de securitate cibernetică şi de a desemna sau de a înființa autorități competente, autorități de gestionare a crizelor cibernetice, puncte unice de contact în materie de Securitate cibernetică (denumite în continuare „puncte unice de contact") şi echipe de intervenție în caz de incidente de Securitate informatică (denumite în continuare „echipe CSIRT");	Art. 2 alin. (1) lit. c) Art. 22 alin. (1)	Art. 2 (1) Scopul prezentei ordonanțe de urgență îl constituie: (...) c) Desemnarea Directoratului Național de Securitate Cibernetică, denumit în continuare "DNSC", ca autoritate competentă responsabilă cu securitatea cibernetică şi cu sarcinile de supraveghere şi asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică, precum şi a altor entități de drept public sau privat cu competențe şi responsabilități în aplicarea prevederilor prezentei ordonanțe de urgență;	

		Art. 28 alin. (1)	d) Desemnarea punctului unic de contact la nivel național și a echipei naționale de răspuns la incidente de securitate cibernetică. Art. 22 (1) Strategia națională de securitate cibernetică este elaborată de către DNSC, cu consultarea celorlalte autorități cu atribuții în domeniul securității cibernetice conform prevederilor Legii nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, cu avizul COSC și este adoptată prin hotărâre a Guvernului, împreună cu planul de acțiune pentru implementarea strategiei, care este anexă la aceasta. 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.	
	b) măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare pentru entitățile de tipul celor menționate în anexa I sau II, precum și	Art. 2 alin. (1) lit. a)	Art. 2 (1) Scopul prezentei ordonanțe de urgență îl constituie:	Entitățile de tipul celor menționate în anexa I sau II din directivă sunt entități esențiale sau entități importante conform art. 5 și 6 din proiect.

	pentru entitățile identificate drept entități critice în temeiul Directivei (UE) 2022/2557	Art. 5 alin. (1) lit. c)	a) Stabilirea măsurilor de gestionare a riscurilor de securitate cibernetică şi a obligațiilor de raportare a incidentelor pentru entitățile esențiale şi importante; Art. 5 (1) Următoarele entități sunt considerate esențiale, indiferent de dimensiunea pe care o au: c) entitățile identificate drept entități critice conform dispozițiilor legale privind reziliența entităților critice;	
	c) normele şi obligațiile privind schimbul de informații în materie de securitate cibernetică;	Art. 2 alin. (1) lit. b)	(1) Scopul prezentei ordonanțe de urgență îl constituie: b) Stabilirea cadrului de cooperare la nivel național şi de participare la nivel european şi internațional în domeniul asigurării securității cibernetice;	
	d) obligațiile în materie de supraveghere şi de asigurare a respectării legii pentru statele membre.	Art. 2 alin. (1) lit. c) Art. 37 alin. (10) Art. 52	Art. 2 (1) Scopul prezentei ordonanțe de urgență îl constituie: c) Desemnarea Directoratului Național de Securitate Cibernetică, denumit în continuare "DNSC", ca autoritate competentă responsabilă cu securitatea cibernetică şi cu sarcinile de supraveghere şi asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică, precum şi a altor entități de drept public sau privat cu competențe şi responsabilități în aplicarea prevederilor prezentei ordonanțe de urgență; Art. 37 (10) Autoritățile competente sectorial sunt, de asemenea, împuternicite să	

			asigure supravegherea, controlul şi sancţionarea în aplicarea prevederilor prezentei ordonanţe de urgenţă, precum şi ale regulamentelor Uniunii Europene din domeniul securităţii cibernetice şi ale actelor de punere în aplicare a dispoziţiilor Directivei (UE) 2022/2555 care vizează entităţile din sectorul lor de competenţă potrivit prezentei ordonanţe de urgenţă, în cazul în care competenţele de supraveghere, control şi sancţionare ale Regulamentelor, respectiv ale actelor de punere în aplicare, nu au fost acordate altei autorităţi. Art. 52 DNSC poate propune împuternicirea prin hotărâre de Guvern a altor autorităţi competente sectorial în domeniul securităţii cibernetice pentru domeniul de competenţă corespunzător în vederea îndeplinirea atribuţiilor prevăzute la art. 46-51 şi art. 60-63.	

Art. 2	(1) Prezenta directivă se aplică entităților publice sau private de tipul celor menționate în anexa I sau II, care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE sau care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la alineatul (1) din respectivul articol și care prestează servicii sau își desfășoară activitățile în cadrul Uniunii. Articolul 3 alineatul (4) din anexa la recomandarea respectivă nu se aplică în sensul prezentei directive.	Art. 5 Art. 6 Art. 8	Art. 5 (1) Următoarele entități sunt considerate esențiale, indiferent de dimensiunea pe care o au: a) entitățile administrației publice centrale în conformitate cu anexa 1; b) entitățile din anexele 1 și 2 identificate în conformitate cu art. 9; c) entitățile identificate drept entități critice conform dispozițiilor legale privind reziliența entităților critice; d) furnizorii de servicii DNS; e) prestatorii 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 destinate publicului. (4) Sunt considerate esențiale, entitățile din categoria întreprinderilor mijlocii conform art. 8 și care sunt furnizori de servicii de securitate gestionate. 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	„Prestator de servicii de încredere" reprezintă sintagma adoptată în legislația națională.

			conform art. 5 şi indiferent de dimensiunea pe care o au: a) entităţile din anexele 1 şi 2 identificate în conformitate cu art. 9; b) furnizorii de reţele publice de comunicaţii electronice şi furnizorii de servicii de comunicaţii destinate publicului; c) prestatorii de servicii de încredere. Art. 8 (1) O entitate este considerată întreprindere mare dacă depăşeşte criteriile stabilite pentru întreprinderile mijlocii astfel cum sunt prevăzute la art. 4 alin. (1) lit. c) şi fără a aplica art. 4^5 din Legea nr. 346/2004 privind stimularea înfiinţării şi dezvoltării întreprinderilor mici şi mijlocii, cu modificările şi completările ulterioare. (2) O entitate este considerată întreprindere mijlocie dacă îndeplineşte criteriile prevăzute la art. 4 alin. (1) lit. c) şi fără a aplica art. 4^5 din Legea nr. 346/2004 privind stimularea înfiinţării şi dezvoltării întreprinderilor mici şi mijlocii, cu modificările şi completările ulterioare.	

	(2) Indiferent de dimensiunea lor, prezenta directivă se aplică, de asemenea, entităților de tipul celor menționate în anexa I sau II, în cazul în care:			
	a) serviciile sunt furnizate de: i. furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului; ii. prestatorii de servicii de încredere iii. registrele de nume de domenii de prim nivel și de furnizorii de servicii de sistem de nume de domenii;	Art. 5 Art. 6	Art. 5 (1) Următoarele entități sunt considerate esențiale, indiferent de dimensiunea pe care o au: a) entitățile administrației publice centrale în conformitate cu anexa 1; b) entitățile din anexele 1 și 2 identificate în conformitate cu art. 9; c) entitățile identificate drept entități critice conform dispozițiilor legale privind reziliența entităților critice; d) furnizorii de servicii DNS; e) prestatorii 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 destinate publicului. 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 şi indiferent de dimensiunea pe care o au: a) entităţile din anexele 1 şi 2 identificate în conformitate cu art. 9; b) furnizorii de reţele publice de comunicaţii electronice şi furnizorii de servicii de comunicaţii destinate publicului; c) prestatorii de servicii de încredere.	
	b) entitatea este singurul furnizor dintr-un stat membru al unui serviciu care este esenţial pentru susţinerea unor activităţi societale şi economice critice	Art. 9 lit. a)	O entitate este considerată esenţială sau importantă, dacă: a) entitatea este singurul furnizor al unui serviciu care este esenţial pentru susţinerea unor activităţi societale şi economice critice;	
	c) perturbarea serviciului furnizat de entitate ar putea avea un impact semnificativ asupra siguranţei publice, a securităţii publice sau a sănătăţii publice;	Art. 9 lit. b)	O entitate este considerată esenţială sau importantă, dacă: (...) b) perturbarea serviciului furnizat de entitate ar putea avea un impact semnificativ asupra siguranţei publice, a securităţii publice sau a sănătăţii publice;	
	d) 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;	Art. 9 lit. c)	O entitate este considerată esenţială sau importantă, dacă: (...) 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;	
	e) entitatea este critică din cauza importanţei sale specifice la nivel naţional sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente din statul membru;	Art. 9 lit. d)	O entitate este considerată esenţială sau importantă, dacă: (...) d) entitatea este critică datorită importanţei sale specifice la nivel naţional sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente.	
	f) entitatea este o entitate a administraţiei publice: i.a nivel central, astfel cum este definită de un stat membru în conformitate cu dreptul intern;	Art. 5 alin. (1) lit. a)	(1) Următoarele entităţi sunt considerate esenţiale, indiferent de dimensiunea pe care o au: a) entităţile administraţiei publice centrale în conformitate cu anexa 1;	Articolul 3 din Constituţia României republicată prevede, la alin. (3) faptul că: *Teritoriul este organizat, sub aspect administrativ, în comune, oraşe şi judeţe. În condiţiile legii, unele oraşe sunt declarate municipii.* Astfel, la nivelul teritoriului

	ii.la nivel regional, astfel cum este definită de un stat membru în conformitate cu dreptul intern, care, în urma unei evaluări bazate pe riscuri, furnizează servicii a căror întrerupere ar putea avea un impact semnificativ asupra activităților societale sau economice critice			României nu există organizarea în regiuni și în acest fel lit. ii) din Directivă nu este aplicabilă și nu necesită transpunere.
	(3) Prezenta directivă se aplică entităților identificate ca fiind entități critice în temeiul Directivei (UE) 2022/2557, indiferent de dimensiunea lor.	Art. 5 alin. (1) lit. c)	(1) Următoarele entități sunt considerate esențiale, indiferent de dimensiunea pe care o au: (...) c) entitățile identificate drept entități critice conform dispozițiilor legale privind reziliența entităților critice;	
	(4) Prezenta directivă se aplică entităților care furnizează servicii de înregistrare a numelor de domenii, indiferent de dimensiunea lor.	Art. 5 alin. (1) lit. d)	(1) Următoarele entități sunt considerate esențiale, indiferent de dimensiunea pe care o au: (...) d) furnizorii de servicii DNS;	
	(5) Statele membre pot prevedea ca prezenta directivă să se aplice: a) entităților administrației publice de la nivel local; b) instituțiilor de învățământ, în special în cazul în care acestea desfășoară activități critice de cercetare.	Art. 18 alin. (17)	Art. 18 (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).	
	(6) Prezenta directivă nu aduce atingere responsabilității statelor membre de a proteja securitatea națională și competenței acestora de a proteja alte funcții esențiale ale statului, inclusiv asigurarea integrității teritoriale a statului și menținerea ordinii publice.	Art. 39 alin. (1) și alin. (2) lit. a) Art. 63	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; 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.	
	(7) Prezenta directivă nu se aplică entităților administrației publice care își desfășoară activitățile în domeniile securității naționale, siguranței publice, apărării sau aplicării legii, inclusiv prevenirii, investigării, depistării și urmăririi penale a infracțiunilor.	Art. 2 alin. (2)	(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.	Entitățile din domeniul apărării, ordinii publice și securității naționale sunt cele care, la nivel național, realizează inclusiv activități de prevenire, investigare, depistare și urmărire penală a infracțiunilor. De asemenea, cu privire la sistemele informatice și de comunicații care vehiculează informații clasificate, acestea au fost introduse deoarece se regăsesc la nivelul mai multor instituții și autorități publice ale statului, iar caracterul de excepție poartă asupra infrastructurilor respective, astfel încât acesta este transferat instituțiilor și autorităților publice care le dețin. Menționăm faptul că acestea se regăsesc în Anexa nr. 1 punctul 10.

	(8) Statele membre pot exonera anumite entități care desfășoară activități în domeniile securității naționale, siguranței publice, apărării sau aplicării legii, inclusiv în domeniul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, sau care furnizează servicii exclusiv entităților administrației publice menționate la alineatul (7) de la prezentul articol, de obligațiile prevăzute la articolul 21 sau la articolul 23 în ceea ce privește activitățile sau serviciile respective. În astfel de cazuri, măsurile de supraveghere și de asigurare a respectării legii menționate în capitolul VII nu se aplică în legătură cu aceste activități sau servicii specifice. În cazul în care entitățile desfășoară activități sau prestează servicii exclusiv de tipul celor menționate în prezentul alineat, statele membre pot decide, de asemenea, să exonereze respectivele entități de obligațiile prevăzute la articolele 3 și 27.	Art. 2 alin. (2)	(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.	Exceptarea de la alin. (2) al art. 2 include toate activitățile subsumate alin. (8) din Directivă.
	(9) Alineatele (7) și (8) nu se aplică în cazul în care o entitate acționează ca prestator de servicii de încredere.	Art. 2 alin. (4)	(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.	
	(10) Prezenta directivă nu se aplică entităților pe care statele membre le-au exclus din domeniul de aplicare al Regulamentului (UE) 2022/2554 în conformitate cu articolul 2 alineatul (4) din regulamentul respectiv.	Art. 2 alin. (3)	(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,	Entităților cărora li se aplică Regulamentul 2022/2554 li se vor aplica prevederile Directivei 2022/2555 doar cu privire la înregistrarea și raportarea incidentelor, acestea reprezentând norma generală în materie, iar Regulamentul 2022/2554 fiind norma specială care nu includ aceste dispoziții.

			(UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 şi (UE) 2016/1011, denumit în continuare „Regulamentul DORA" le sunt incidente doar dispoziţiile art. 5-10 şi art. 18.	
	(11) Obligaţiile prevăzute în prezenta directivă nu implică furnizarea de informaţii a căror divulgare ar contraveni intereselor esenţiale ale statelor membre în materie de securitate naţională, siguranţă publică sau apărare.			Prevederile alin. (11) se regăsesc intrinsec la nivelul întregului text al proiectului de act normativ, interpretându-l sistematic, astfel cum recunoaşte sistemul de drept continental.
	(12) Prezenta directivă se aplică fără a aduce atingere Regulamentului (UE) 2016/679, Directivei 2002/58/CE, Directivelor 2011/93/UE (27) şi 2013/40/UE (28) ale Parlamentului European şi ale Consiliului şi Directivei (UE) 2022/2557.	Art. 62 alin. (2) - (4) Art. 15 alin. (16) Art. 37 alin. (2) si (12)	Art. 62 (2) DNSC nu aplică dispoziţiile art. 48 alin. (1) pentru fapte cu impact în domeniul protecţiei datelor cu caracter personal cu privire la care s-a efectuat sau se efectuează o investigaţie de către ANSPDCP. (3) Prelucrările de date cu caracter personal ce intră sub incidenţa prezentei ordonanţe de urgenţă se efectuează cu respectarea reglementărilor legale privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal. (4) Raportările realizate în temeiul prezentei ordonanţe de urgenţă 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. Art. 15 (16) DNSC furnizează Centrului Naţional de Coordonare a Protecţiei Infrastructurilor Critice, denumit în continuare „CNCPIC", informaţii cu	

		Art. 46 alin. (3) Art. 51 alin. (1) si (2)	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 dispozițiilor legale privind reziliența entităților critice. Art. 37 (2) În vederea asigurării unui nivel comun ridicat de securitate cibernetică la nivel național, DNSC se coordonează cu CNCPIC și face schimb de informații periodic 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 acestea. (12) Autoritățile competențe 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 legale privind reziliența entităților critice. Art. 46 (3) Activitatea de supraveghere și control se realizează de către DNSC inclusiv la solicitarea motivată a CNCPIC pentru entitățile identificate critice conform dispozițiilor legale privind reziliența entităților critice. 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 legale privind reziliența entităților critice. (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 legale privind reziliența entităților critice.	
	(13) Fără a aduce atingere articolului 346 din TFUE, informațiile confidențiale în conformitate cu normele Uniunii sau cu cele naționale, precum cele privind secretul comercial, fac obiectul schimbului de informații cu Comisia și cu alte autorități relevante în conformitate cu prezenta directivă, numai dacă acest lucru este necesar pentru aplicarea prezentei directive. Informațiile care fac obiectul schimbului se limitează la informații relevante pentru scopul urmărit și proporționale cu acesta. Schimbul de informații păstrează confidențialitatea respectivelor informații și protejează securitatea și interesele comerciale ale entităților în cauză.	Art. 29 alin. (2) și (3)	(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 cibernetice și prevede cel puțin: a) obiectivele măsurilor și ale activităților de pregătire; b) sarcinile și responsabilitățile autorităților de gestionare a crizelor cibernetice; c) procedurile de gestionare a crizelor cibernetice, 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 trei luni de la adoptarea sau modificarea Planului prevăzut la alin. (1), DNSC transmite Comisiei Europene şi Reţelei europene a organizaţiilor de legătură în materie de crize cibernetice, denumită în continuare „EU-CyCLONe", informaţii relevante în legătură cu acesta, cu excepţia informaţiilor care pot aduce atingere securităţii naţionale.	
	(14) Entităţile, autorităţile competente, punctele unice de contact şi echipele CSIRT prelucrează datele cu caracter personal în măsura necesară pentru scopurile prezentei directive şi în conformitate cu Regulamentul (UE) 2016/679; în special această prelucrare se bazează pe articolul 6 din respectivul regulament. Prelucrarea datelor cu caracter personal în temeiul prezentei directive de către furnizorii de reţele publice de comunicaţii electronice sau de către furnizorii de servicii de comunicaţii electronice accesibile publicului se efectuează în conformitate cu dreptul Uniunii privind protecţia datelor şi cu dreptul Uniunii privind protejarea confidenţialităţii, în special cu Directiva 2002/58/CE	Art. 62 alin. (3) şi (4)	Art. 62 (3) Prelucrările de date cu caracter personal ce intră sub incidenţa prezentei ordonanţe de urgenţă se efectuează cu respectarea reglementărilor legale privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal. (4) Raportările realizate în temeiul prezentei ordonanţe de urgenţă 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.	

Art. 3	(1) În sensul prezentei directive, următoarele entități sunt considerate a fi entități esențiale: a) entitățile de tipul celor menționate în anexa I care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la articolul 2 alineatul (1) din anexa la Recomandarea 2003/361/CE b) prestatorii de servicii de încredere calificați și registrele de nume de domenii de prim nivel, precum și prestatorii de servicii DNS, indiferent de dimensiunea lor c) furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE d) entitățile administrației publice menționate la articolul 2 alineatul (2) litera (f) punctul (i); e) orice alte entități de tipul celor menționate în anexa I sau II care sunt identificate de un stat membru drept entități esențiale în temeiul articolului 2 alineatul (2) literele (b)-(e) f) entitățile identificate drept entități critice în temeiul Directivei (UE) 2022/2557, menționate la articolul 2 alineatul (3) din prezenta directivă g) în cazul în care statul membru prevede acest lucru, entitățile pe care statul membru respectiv le-a identificat înainte de 16 ianuarie 2023 ca operatori de servicii esențiale în conformitate cu Directiva (UE) 2016/1148 sau cu dreptul intern.	Art. 5 Art. 9	Art. 5 (1) Următoarele entități sunt considerate esențiale, indiferent de dimensiunea pe care o au: a) entitățile administrației publice centrale în conformitate cu anexa 1; b) entitățile din anexele 1 și 2 identificate în conformitate cu art. 9; c) entitățile identificate drept entități critice conform dispozițiilor legale privind reziliența entităților critice; d) furnizorii de servicii DNS; e) prestatorii 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 destinate publicului. (4) Sunt considerate esențiale, entitățile din categoria întreprinderilor mijlocii conform art. 8 și care sunt furnizori de servicii de securitate gestionate. 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,	Nu a fost introdusă o prevedere pentru transpunerea art. 3 alin. (1) lit. g) din Directivă deoarece toate entitățile, indiferent dacă au fost sau nu identificate anterior ca operatori de servicii esențiale sau furnizori de servicii digitale , vor trece din nou prin procesul de identificare.

			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.	
	(2) În sensul prezentei directive, entitățile de tipul celor menționate în anexa I sau II care nu se califică drept entități esențiale în temeiul alineatului (1) de la prezentul articol sunt considerate a fi entități importante. Sunt incluse aici entitățile identificate de statele membre ca fiind entități importante în temeiul articolului 2 alineatul (2) literele (b)-(e)	Art. 6 alin. (1) si (2)	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	

		Art. 9	conform art. 5 şi indiferent de dimensiunea pe care o au: a) entităţile din anexele 1 şi 2 identificate în conformitate cu art. 9; b) furnizorii de reţele publice de comunicaţii electronice şi furnizorii de servicii de comunicaţii electronice destinate publicului; c) prestatorii de servicii de încredere. Art. 9 O entitate este considerată esenţială sau importantă, dacă: a) entitatea este singurul furnizor al unui serviciu care este esenţial pentru susţinerea unor activităţi societale şi economice critice; b) perturbarea serviciului furnizat de entitate ar putea avea un impact semnificativ asupra siguranţei publice, a securităţii publice sau a sănătăţii 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 importanţei sale specifice la nivel naţional sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente.	
	(3) Până la 17 aprilie 2025, statele membre întocmesc o listă a entităţilor esenţiale şi a entităţilor importante, precum şi a entităţilor care furnizează servicii de înregistrare a numelor de domenii. Statele membre revizuiesc lista în mod regulat, cel puţin o dată la doi ani, şi o actualizează atunci când este cazul.	Art. 18 alin. (1) - (3) lit. a), (8) si (10)	Art. 18 (1) DNSC păstrează un registru al entităţilor esenţiale şi al entităţilor importante identificate. (2) Entităţile care desfăşoară activitate în sectoarele din anexele 1 şi 2, notifică DNSC în vederea înregistrării în cel mult 30 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă 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; (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 2 săptămâni 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 3 luni de la data modificării. (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, furnizorilor 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. Punctul unic de contact revizuiește informațiile prevăzute în mod regulat și cel puțin o dată la doi ani. Până la 17 aprilie 2025 și la cererea	

			Comisiei Europene, punctul unic de contact național notifică Comisiei Europene denumirile entităților esențiale și ale entităților importante identificate conform art. 9.	
	(4) În scopul întocmirii listei menționate la alineatul (3), statele membre solicită entităților menționate la respectivul alineat să prezinte autorităților competente cel puțin următoarele informații:	Art. 18 alin. (2) si (3)	(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 entității;		a) denumirea;	
	b) adresa și datele de contact actualizate, inclusiv adresele de e-mail, gama de IP-uri și numerele de telefon;		b) adresa sediului social principal și datele de contact actualizate, inclusiv adresele de e-mail și numerele de telefon; 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;	
	c) dacă este cazul, sectorul și subsectorul relevante menționate în anexa I sau II; precum și		f) sectorul, subsectorul și tipul de entitate, astfel cum acestea se încadrează în anexa 1 sau în anexa 2;	

	d) după caz, o listă a statelor membre în care furnizează servicii care intră în domeniul de aplicare al prezentei directive.		g) statele membre în care prestează servicii, după caz;	
	Entitățile menționate la alineatul (3) notifică fără întârziere orice modificări ale detaliilor transmise în temeiul primului paragraf de la prezentul alineat și, în orice caz, în termen de două săptămâni de la data modificării.	Art. 18 alin. (8)	(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 2 săptămâni de la data modificării;	
	Comisia, cu sprijinul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), oferă, fără întârzieri nejustificate, orientări și modele privind obligațiile prevăzute în prezentul alineat.			Nu este necesara transpunerea. Obligație pentru ENISA
	Statele membre pot institui mecanisme naționale prin care entitățile să se înregistreze.	Art. 18 alin. (1), (2), (4), (5), (12) - (17)	(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. (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. (12) După expirarea termenului prevăzut la alin. (2), 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 radierii 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).	

	(5) Până la 17 aprilie 2025 și, ulterior, o dată la doi ani, autoritățile competente notifică: a) Comisiei și Grupului de cooperare numărul entităților esențiale și al entităților importante enumerate în temeiul alineatului (3) pentru fiecare sector și subsector menționat în anexa I sau II; și	Art. 18 alin. (10)	(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, furnizorilor 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. Punctul unic de contact revizuiește informațiile prevăzute în mod regulat și cel puțin o dată la doi ani. Până la 17 aprilie 2025 și la cererea Comisiei Europene, punctul unic de contact național notifică Comisiei Europene denumirile entităților esențiale și ale entităților importante identificate conform art. 9.	
	b) Comisiei informațiile relevante privind numărul de entități esențiale și de entități importante identificate în temeiul articolului 2 alineatul (2) literele (b)-(e), sectorul și subsectorul menționate în anexa I sau II din care fac parte, tipul de servicii pe care le furnizează și dispoziția, dintre cele prevăzute la articolul 2 alineatul (2) literele (b)-(e), în temeiul căreia au fost identificate. (6) Până la 17 aprilie 2025 și la cererea Comisiei, statele membre pot notifica Comisiei denumirile entităților esențiale și ale entităților importante menționate la alineatul (5) litera (b).	Art. 18 alin. (10)	(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, furnizorilor 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. Punctul unic de contact revizuieşte informaţiile prevăzute în mod regulat şi cel puţin o dată la doi ani. Până la 17 aprilie 2025 şi la cererea Comisiei Europene, punctul unic de contact naţional notifică Comisiei Europene denumirile entităţilor esenţiale şi ale entităţilor importante identificate conform art. 9.	
Art. 4	(1) În cazul în care actele juridice sectoriale ale Uniunii impun entităţilor esenţiale sau entităţilor importante să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să notifice incidentele semnificative, iar cerinţele respective au un efect cel puţin echivalent cu efectul obligaţiilor prevăzute în prezenta directivă, dispoziţiile relevante ale prezentei directive, inclusiv dispoziţiile privind supravegherea şi asigurarea respectării legii prevăzute în capitolul VII, nu se aplică acestor entităţi. În cazul în care actele juridice sectoriale ale Uniunii nu acoperă toate entităţile dintr-un anumit sector care intră în domeniul de aplicare al prezentei directive, dispoziţiile relevante ale prezentei directive se aplică în continuare entităţilor care nu fac obiectul respectivelor acte juridice sectoriale ale Uniunii.	Art. 37 alin. (14) şi (15)	(14) În cazul în care actele juridice sectoriale ale Uniunii Europene impun entităţilor esenţiale sau entităţilor importante să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să raporteze incidentele semnificative, iar cerinţele respective au un efect cel puţin echivalent cu efectul obligaţiilor prevăzute în prezenta ordonanţă de urgenţă, dispoziţiile prezentei ordonanţe de urgenţă privind măsurile de gestionare a riscurilor, raportarea incidentelor, precum şi supravegherea, verificarea şi controlul nu se aplică acestor entităţi. În cazul în care actele juridice sectoriale ale Uniunii Europene nu acoperă toate entităţile dintr-un anumit sector care intră în domeniul de aplicare al prezentei ordonanţe de urgenţă, dispoziţiile relevante ale prezentei ordonanţe de urgenţă se aplică în continuare entităţilor care nu fac obiectul respectivelor acte juridice sectoriale ale Uniunii Europene. (15) Cerinţele menţionate la alin. (14) sunt considerate echivalente în privinţa efectului cu obligaţiile prevăzute în prezenta ordonanţă de urgenţă, în cazul în care îndeplineşte cel puţin o condiţie 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.	
	(2) Cerințele menționate la alineatul (1) din prezentul articol sunt considerate echivalente în privința efectului cu obligațiile prevăzute în prezenta directivă, în cazul în care: a) măsurile de gestionare a riscurilor în materie de securitate cibernetică sunt cel puțin echivalente în privința efectului cu cele prevăzute la articolul 21 alineatele (1) și (2); sau b) actul juridic sectorial al Uniunii prevede accesul imediat, după caz automat și direct, la notificările incidentelor pentru echipele CSIRT, autoritățile competente sau punctele unice de contact în temeiul prezentei directive și dacă cerințele de notificare a incidentelor semnificative au un efect cel puțin echivalent cu cele prevăzute la articolul 23 alineatele (1)-(6) din prezenta directivă	Art. 37 alin. (15)	(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.	
	(3) Comisia, până la 17 iulie 2023, oferă orientări care clarifică aplicarea alineatelor (1) și (2). Comisia revizuiește orientările respective în mod periodic. La elaborarea acestor orientări, Comisia ia în considerare observațiile Grupului de cooperare și ale ENISA			Nu este necesara transpunerea. Obligație pentru Comisie
Art. 5	Prezenta directivă nu împiedică statele membre să adopte sau să mențină dispoziții care asigură			Prezentul proiect de act normativ, în întregul său, nu împiedică ci, dimpotrivă, încurajează

	un nivel mai ridicat de securitate cibernetică, cu condiția ca aceste dispoziții să fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii.			reglementarea unor dispoziții care să asigure un nivel mai ridicat de securitate cibernetică la nivel sectorial, acestea având rol de legislație specială în materie.
Art. 6	În sensul prezentei directive, se aplică următoarele definiții:			
	1. „rețea și sistem informatic" înseamnă: a) o rețea de comunicații electronice, astfel cum este definită la articolul 2 punctul 1 din Directiva (UE) 2018/1972; b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale; sau c) datele digitale stocate, prelucrate, recuperate sau transmise de elemente reglementate în temeiul literelor (a) și (b) în vederea funcționării, utilizării, protejării și întreținerii lor;	Art. 4 lit. ff)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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.	
	2. „securitatea rețelelor și a sistemelor informatice" înseamnă capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărui eveniment care poate compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;	Art. 4 lit. ii)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: 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;	

	3. „securitate cibernetică" înseamnă securitate cibernetică astfel cum este definită la articolul 2 alineatul (1) din Regulamentul (UE) 2019/881;	Art. 4 lit. hh)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: 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;	Art. 2 lit. y) din Legea nr. 58/2023 - „securitate cibernetică" - stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic ale resurselor și serviciilor publice sau private din spațiul cibernetic. Art. 2 pct. (1) din Regulamentul (UE) 2019/881 - „securitate cibernetică" înseamnă activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice. Ținând cont de deciziile Curții Constituționale a României (ex. Decizia nr. 17/2015), securitatea cibernetică este parte a securității naționale, astfel încât unica autoritate competentă în acest domeniu rămâne statul membru, în speță România.
	4. „strategie națională de securitate cibernetică" înseamnă un cadru coerent al unui stat membru care prevede obiective și priorități strategice în domeniul securității cibernetice și guvernanța necesară pentru realizarea acestora în statul membru respectiv;	Art. 21 alin. (1) Art. 22 alin. (3) Art. 23 alin. (1)	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. Art. 22 (3) Strategia națională de securitate cibernetică prevede obiectivele strategice, resursele necesare pentru	

			atingerea obiectivelor respective şi măsurile de politică şi de reglementare adecvate în vederea atingerii şi menţinerii unui nivel ridicat de securitate cibernetică. Art. 23 (1) Strategia naţională de securitate cibernetică elaborată conform art. 22 cuprinde cel puţin următoarele: a) obiectivele şi priorităţile strategiei naţionale de securitate cibernetică, care acoperă în special sectoarele menţionate în anexele 1 şi 2; b) un cadru de guvernanţă pentru realizarea obiectivelor şi priorităţilor menţionate la lit. a), inclusiv politicile publice; c) un cadru de guvernanţă care clarifică rolurile şi responsabilităţile părţilor interesate relevante la nivel naţional, care sprijină cooperarea şi coordonarea la nivel naţional între autorităţile competente, punctele unice de contact şi echipele de răspuns la incidente de securitate cibernetică în temeiul prezentei ordonanţe de urgenţă, precum şi coordonarea şi cooperarea dintre aceste organisme şi autorităţile competente în temeiul actelor juridice sectoriale ale Uniunii Europene; d) un mecanism care să identifice activele relevante şi o evaluare a riscurilor la nivel naţional; e) o identificare a măsurilor de asigurare a pregătirii pentru incidente la nivel naţional, a capacităţii de răspuns la acestea şi a redresării în urma acestora, inclusiv cooperarea dintre sectorul public şi cel privat; f) o listă a diferitelor autorităţi şi părţi interesate care participă la punerea în	

			aplicare a strategiei naţionale de securitate cibernetică; g) un cadru de politică menit să asigure o mai bună coordonare între autorităţile competente în temeiul prezentei ordonanţe de urgenţă şi al dispoziţiilor legale privind reziliența entităţilor critice în scopul schimbului de informaţii privind riscurile, ameninţările cibernetice şi incidentele, precum şi privind riscurile, ameninţările şi incidentele fără caracter cibernetic şi al exercitării sarcinilor de supraveghere, după caz; h) un plan care să cuprindă inclusiv măsurile necesare pentru a spori nivelul general de sensibilizare a cetăţenilor cu privire la securitatea cibernetică.	
	5. „incident evitat la limită" înseamnă un eveniment care ar fi putut compromite disponibilitatea, autenticitatea, integritatea sau confidenţialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de reţele şi sisteme informatice sau accesibile prin intermediul acestora, dar care a fost împiedicat cu succes să se materializeze sau care nu s-a materializat	Art. 4 lit. o)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) o) *incident evitat la limită* înseamnă un eveniment care ar fi putut compromite disponibilitatea, autenticitatea, integritatea sau confidenţialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de reţele şi sisteme informatice sau accesibile prin intermediul acestora, dar care a fost împiedicat cu succes să se materializeze sau care nu s-a materializat;	
	6. „incident" înseamnă un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidenţialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de reţele şi sisteme informatice sau accesibile prin intermediul acestora;	Art. 4 lit. m)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) m) *incident* înseamnă un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidenţialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de reţele şi sisteme informatice sau accesibile prin intermediul acestora;	

	7. „incident de securitate cibernetică de mare amploare" înseamnă un incident care provoacă un nivel de perturbare care depăşeşte capacitatea unui stat membru de a răspunde la acesta sau care are un impact semnificativ asupra a cel puţin două state membre;	Art. 4 lit. n)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) n) *incident de securitate cibernetică de mare amploare* înseamnă un incident care provoacă perturbări care depăşesc capacităţile de răspuns ale unui singur stat membru al Uniunii Europene sau care are un impact semnificativ asupra a cel puţin două state membre ale Uniunii Europene;	
	8. „gestionarea incidentului" înseamnă toate acţiunile şi procedurile care vizează prevenirea, detectarea, analizarea şi limitarea unui incident, sau vizează răspunsul la acesta şi redresarea în urma incidentului	Art. 4 lit. l)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) l) *gestionarea incidentului* înseamnă toate acţiunile şi procedurile care vizează prevenirea, detectarea, analizarea şi limitarea unui incident, sau vizează răspunsul la acesta şi redresarea în urma incidentului;	
	9. „risc" înseamnă potenţialul de pierderi sau de perturbări cauzate de un incident şi trebuie exprimat ca o combinaţie între amploarea unei astfel de pierderi sau perturbări şi probabilitatea producerii incidentului;	Art. 4 lit. gg)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) gg) *risc* înseamnă potenţialul de pierderi sau de perturbări cauzate de un incident şi trebuie exprimat ca o combinaţie între amploarea unei astfel de pierderi sau perturbări şi probabilitatea producerii incidentului;	
	10. „ameninţare cibernetică" înseamnă o ameninţare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;	Art. 4 lit. a)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: a) *ameninţare cibernetică* înseamnă o ameninţare astfel cum aceasta este definită la art. 2 lit. f) din OUG nr. 104/2021 privind Înfiinţarea Directoratului Naţional de Securitate Cibernetică;	Art. 2 lit. f) din OUG nr. 104/2021 „ameninţare cibernetică" - orice circumstanţă, eveniment sau acţiune potenţială care ar putea cauza daune sau perturbări la nivelul reţelelor şi al sistemelor informatice, precum şi la nivelul utilizatorilor unor astfel de sisteme şi al altor persoane sau care poate avea un alt fel de impact negativ asupra acestora. Art. 2 pct. (8) din Regulamentul (UE) 2019/881 „ameninţare cibernetică" înseamnă orice circumstanţă, eveniment sau acţiune potenţială care ar putea cauza daune sau perturbări la nivelul

				rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora.
	11. „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;	Art. 4 lit. b)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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;	
	12. „produs TIC" înseamnă un produs astfel cum este definit la articolul 2 punctul 12 din Regulamentul (UE) 2019/881;	Art. 4 lit. aa)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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);	
	13. „serviciu TIC" înseamnă un serviciu TIC astfel cum este definit la articolul 2 punctul 13 din Regulamentul (UE) 2019/881	Art. 4 lit. pp)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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) şi privind certificarea securităţii cibernetice pentru tehnologia informaţiei şi comunicaţiilor şi de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică);	
	14. „proces TIC" înseamnă un proces TIC astfel cum este definit la articolul 2 punctul 14 din Regulamentul (UE) 2019/881;	Art. 4 lit. z)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) z) *proces TIC* înseamnă un proces TIC în sensul articolului 2 punctul 14 din Regulamentul (UE) 2019/881 al Parlamentului European şi al Consiliului din 17 aprilie 2019 privind ENISA (Agenţia Uniunii Europene pentru Securitate Cibernetică) şi privind certificarea securităţii cibernetice pentru tehnologia informaţiei şi comunicaţiilor şi de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică);	
	15. „vulnerabilitate" înseamnă un punct slab, o susceptibilitate sau o deficienţă a unor produse TIC sau a unor servicii TIC care poate fi exploatată de o ameninţare cibernetică;	Art. 4 lit. tt)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) tt) *vulnerabilitate* înseamnă un punct slab, o susceptibilitate sau o deficienţă a unor produse TIC sau a unor servicii TIC care poate fi exploatată de o ameninţare cibernetică.	
	16. „standard" înseamnă un standard astfel cum este definit la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European şi al Consiliului;	Art. 4 lit. ss)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) ss) *standard* înseamnă un standard în sensul art. 2 alin. (1) din Regulamentul (UE) nr. 1025/2012 al Parlamentului European şi al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor	

			89/686/CEE şi 93/15/CEE ale Consiliului şi a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE şi 2009/105/CE ale Parlamentului European şi ale Consiliului şi de abrogare a Deciziei 87/95/CEE a Consiliului şi a Deciziei nr. 1673/2006/CE a Parlamentului European şi a Consiliului;	
	17. „specificaţie tehnică" înseamnă o specificaţie tehnică astfel cum este definită la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012;	Art. 4 lit. rr)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) rr) *specificaţie tehnică* înseamnă o specificaţie tehnică astfel cum este definită la art. 2 punctul 4 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European şi al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE şi 93/15/CEE ale Consiliului şi a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE şi 2009/105/CE ale Parlamentului European şi ale Consiliului şi de abrogare a Deciziei 87/95/CEE a Consiliului şi a Deciziei nr. 1673/2006/CE a Parlamentului European şi a Consiliului;	
	18. „internet exchange point" înseamnă o facilitate a reţelei care permite interconectarea a mai mult de două reţele autonome independente (sisteme autonome), în special în scopul facilitării schimbului de trafic de internet, care furnizează interconectare doar pentru sisteme autonome şi care nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre orice pereche de sisteme autonome	Art. 4 lit. p)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) p) *internet exchange point* înseamnă o facilitate a reţelei care permite interconectarea a mai mult de două reţele autonome independente, în special în scopul facilitării schimbului de trafic de internet, care furnizează	

	participante şi nici nu modifică sau interacţionează într-un alt mod cu acest trafic		interconectare doar pentru sisteme autonome şi care nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre orice pereche de sisteme autonome participante şi nici nu modifică sau interacţionează într-un alt mod cu acest trafic;	
	19. „sistem de nume de domenii DNS" sau „DNS" înseamnă un sistem ierarhic şi distribuit de atribuire de nume care face posibilă identificarea serviciilor şi a resurselor de pe internet, permiţând dispozitivelor utilizatorilor finali să utilizeze serviciile de rutare şi conectivitate pe internet pentru a accesa serviciile şi resursele respective	Art. 4 lit. qq)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) qq) *sistem de nume de domenii sau DNS* înseamnă un sistem de denumire ierarhic şi distribuit care permite identificarea serviciilor şi resurselor de internet, care permite dispozitivelor utilizatorilor finali să utilizeze servicii de rutare şi conectivitate a internetului pentru a accesa aceste servicii şi resurse;	
	20. „furnizor de servicii DNS" înseamnă o entitate care furnizează: a) servicii de rezoluţie a numelor de domenii recursive accesibile publicului pentru utilizatorii finali de internet; sau b) servicii de rezoluţie a numelor de domenii cu autoritate pentru utilizarea de către terţi, cu excepţia serverelor pentru nume primare;	Art. 4 lit. i)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) i) *furnizor de servicii DNS* înseamnă o entitate care furnizează: 1. servicii de rezoluţie recursivă a numelor de domenii accesibile publicului pentru utilizatorii finali ai internetului; 2. servicii de rezoluţie a numelor de domenii cu autoritate destinate utilizării de către terţi, cu excepţia serverelor de nume rădăcină;	
	21. „registru de nume de domenii de prim nivel" sau „registru de nume TLD" (top-level domain – TLD) înseamnă o entitate căreia i s-a delegat un anumit TLD şi care este responsabilă cu administrarea TLD-ului, inclusiv cu înregistrarea numelor de domenii în cadrul TLD-ului şi cu exploatarea tehnică a TLD-ului, inclusiv exploatarea serverelor sale de nume, întreţinerea bazelor sale de date şi distribuirea	Art. 4 lit. bb)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) bb) *registru de nume TLD* înseamnă o entitate căreia i-a fost delegat un anumit domeniu de prim nivel şi care răspunde de administrarea domeniului de prim nivel, inclusiv de înregistrarea	

	fișierelor zonale TLD între serverele de nume, indiferent dacă oricare dintre aceste operațiuni este efectuată de entitatea însăși sau este externalizată, dar excluzând situațiile în care numele TLD sunt utilizate de un registru numai pentru uzul propriu;		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;	
	22. „entitate care furnizează servicii de înregistrare a numelor 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;	Art. 4 lit. i)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...0 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;	
	23. „serviciu digital" înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului;	Art. 4 lit. jj)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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 şi completările ulterioare şi care se încadrează într-una din categoriile: 1. piaţă online; 2. motor de căutare online; 3. serviciu de cloud computing.	
	24. „serviciu de încredere" înseamnă un serviciu de încredere astfel cum este definit la articolul 3 punctul 16 din Regulamentul (UE) nr. 910/2014;	Art. 4 lit. nn)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) nn) *serviciu de încredere* înseamnă un serviciu de încredere în sensul articolului 3 punctul 16 din Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE ("Regulamentul eIDAS");	
	25. „prestator de servicii de încredere" înseamnă un prestator de servicii de încredere astfel cum este definit la articolul 3 punctul 19 din Regulamentul (UE) nr. 910/2014;	Art. 4 lit. x)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) 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 şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE;	
	26. „serviciu de încredere calificat" înseamnă un serviciu de încredere calificat astfel cum este definit la articolul 3 punctul 17 din Regulamentul (UE) nr. 910/2014;	Art. 4 lit. oo)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) 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 şi al	

			Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE ("Regulamentul eIDAS");	
	27. „prestator de servicii de încredere calificat" înseamnă un prestator de servicii de încredere calificat astfel cum este definit la articolul 3 punctul 20 din Regulamentul (UE) nr. 910/2014;	Art. 4 lit. y)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) 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 şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE;	
	28. „piaţă online" înseamnă o piaţă online astfel cum este definită la articolul 2 litera (n) din Directiva 2005/29/CE a Parlamentului European şi a Consiliului;	Art. 4 lit. u)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) u) *piaţă online* înseamnă un serviciu astfel cum este definit la art. 2 lit. o) din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianţilor în relaţia cu consumatorii şi armonizarea reglementărilor cu legislaţia europeană privind protecţia consumatorilor, cu modificările şi completările ulterioare;	
	29. „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 şi al Consiliului;	Art. 4 lit. q)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) 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 şi al	

			Consiliului din 20 iunie 2019 de promovare a echității și a transparenței pentru întreprinderile utilizatoare de servicii de intermediere online;	
	30. „serviciu de cloud computing" înseamnă un serviciu digital care permite administrarea la cerere și accesul amplu la distanță la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun, inclusiv atunci când aceste resurse sunt distribuite în mai multe locații;	Art. 4 lit. ll)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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;	
	31. „serviciu de centre de date" înseamnă un serviciu care cuprinde structuri sau grupuri de structuri dedicate găzduirii, interconectării și exploatării centralizate a tehnologiei informației și a echipamentelor de rețea care furnizează servicii de stocare, prelucrare și transport de date, împreună cu toate instalațiile și infrastructurile de distribuție a energiei electrice și de control al mediului	Art. 4 lit. kk)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) kk) *serviciu de centre de date* înseamnă un serviciu care cuprinde structuri sau grupuri de structuri dedicate găzduirii, interconectării și exploatării centralizate a echipamentelor informatice și de rețea care furnizează servicii de stocare, prelucrare și transport de date, împreună cu toate instalațiile și infrastructurile de distribuție a energiei electrice și de control al mediului;	
	32. „rețea de furnizare de conținut" înseamnă o rețea de servere distribuite geografic cu scopul de a asigura o disponibilitate ridicată, accesibilitate sau furnizare rapidă de conținut digital și servicii către utilizatorii de internet în numele furnizorilor de conținut și de servicii;	Art. 4 lit. dd)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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;	
	33. „platformă de servicii de socializare în rețea" înseamnă o platformă care le permite utilizatorilor finali să se conecteze, să partajeze, să descopere și să comunice între ei prin intermediul mai multor dispozitive, în special prin chat, postări, materiale video și recomandări	Art. 4 lit. v)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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;	
	34. „reprezentant" înseamnă o persoană fizică sau juridică stabilită în Uniune care este desemnată în mod explicit să acționeze în numele unui furnizor de servicii DNS, al unui registru de nume TLD, al unei entități care furnizează servicii de înregistrare a numelor de domenii, al unui furnizor de servicii de cloud computing, al unui furnizor de servicii de centre de date, al unui furnizor de rețele de furnizare de conținut, al unui furnizor de servicii gestionate, al unui furnizor de servicii de securitate gestionate sau al unui furnizor al unei piețe online, al unui motor de căutare online sau al unei platforme de servicii de socializare în rețea, care nu este stabilit în Uniune, căreia o autoritate națională competentă sau o echipă CSIRT i se poate adresa în locul entității în cauză în ceea ce privește obligațiile entității respective în temeiul prezentei directive;	Art. 4 lit. cc)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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 de nume TLD, al unei entități care furnizează servicii de înregistrare a numelor de domenii, al unui furnizor de servicii 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 gestionate, un furnizor al unei piețe online, furnizor al unui motor de căutare online sau un furnizor de platforme de servicii de socializare în rețea care nu este stabilit în Uniunea Europeană, care poate fi contactat de autoritatea competentă în domeniul securității cibernetice în legătură cu obligațiile entității respective în temeiul dispozițiilor prezentei ordonanțe de urgență;	

	35. „entitate a administrației publice" înseamnă o entitate recunoscută ca atare într-un stat membru în conformitate cu dreptul intern, cu excepția sistemului judiciar, a parlamentelor și a băncilor centrale, care îndeplinește următoarele criterii: a) a fost înființată în scopul de a răspunde unor necesități de interes general și nu are un caracter industrial sau comercial; b) are personalitate juridică sau este abilitată prin lege să acționeze în numele unei alte entități cu personalitate juridică; c) este finanțată, în cea mai mare parte, de stat, de autoritățile regionale sau de alte organisme de drept public, este supusă controlului de gestiune din partea autorităților sau a organismelor respective sau are un consiliu de administrație, de conducere sau de supraveghere ai cărui membri sunt desemnați în proporție de peste 50 % de stat, de autoritățile regionale sau de alte organisme de drept public; d) are competența de a adresa persoanelor fizice sau juridice decizii administrative sau de reglementare care le afectează drepturile în ceea ce privește circulația transfrontalieră a persoanelor, mărfurilor, serviciilor sau capitalurilor;	Art. 4 lit. g)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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;	Identificarea în legislația națională în vigoare a entităților administrației publice este diferită, astfel încât am enumerat instituțiile și autoritățile publice care pot intra în scopul prezentei ordonanțe de urgență conform scopului Directivei: k) autoritatea publică - organ de stat sau al unității administrativ-teritoriale care acționează în regim de putere publică pentru satisfacerea unui interes public; l) autoritatea administrației publice - autoritate publică care acționează pentru organizarea executării sau executarea în concret a legii sau pentru prestarea serviciilor publice; w) instituția publică - structură funcțională care acționează în regim de putere publică și/sau prestează servicii publice și care este finanțată din venituri bugetare și/sau din venituri proprii, în condițiile legii finanțelor publice; kk) serviciul public - activitatea sau ansamblul de activități organizate de o autoritate a administrației publice ori de o instituție publică sau autorizată/autorizate ori delegată de aceasta, în scopul satisfacerii unei nevoi cu caracter general sau a unui interes public, în mod regulat și continuu
	36. „rețea publică de comunicații electronice" înseamnă o rețea publică de comunicații electronice astfel cum este definită la articolul 2 punctul 8 din Directiva (UE) 2018/1972;	Art. 4 lit. ee)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) 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;	
	37. „serviciu de comunicații electronice" înseamnă un serviciu de comunicații electronice astfel cum este definit la articolul 2 punctul 4 din Directiva (UE) 2018/1972;	Art. 4 lit. mm)	În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație: (...) mm) *serviciu de comunicații electronice* înseamnă un serviciu de	

			comunicaţii electronice în sensul articolului 4 alin. (1) punctul 9 din OUG nr. 111/2011 privind comunicaţiile electronice;	
	38. „entitate" înseamnă o persoană fizică sau juridică constituită şi recunoscută ca atare în temeiul dreptului intern al locului său de stabilire care poate, acţionând în nume propriu, să exercite drepturi şi să fie supusă unor obligaţii;	Art. 4 lit. f)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) f) *entitate* înseamnă o persoană fizică sau juridică constituită şi recunoscută ca atare în temeiul dreptului intern al locului său de stabilire care poate, acţionând în nume propriu, să exercite drepturi şi să fie supusă unor obligaţii;	
	39. „furnizor de servicii gestionate" înseamnă o entitate care furnizează servicii legate de instalarea, gestionarea, funcţionarea sau întreţinerea produselor, reţelelor, infrastructurii, aplicaţiilor TIC sau a oricăror alte reţele şi sisteme informatice, prin intermediul asistenţei sau al administrării active efectuate fie la sediul clienţilor, fie la distanţă;	Art. 4 lit. j)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) j) *furnizor de servicii gestionate* înseamnă o entitate care furnizează servicii legate de instalarea, gestionarea, funcţionarea sau întreţinerea produselor, reţelelor, infrastructurilor sau aplicaţiilor TIC sau a altor reţele şi sisteme informatice, prin asistenţă sau administrare activă, fie la sediul clientului, fie de la distanţă;	
	40. „furnizor de servicii de securitate gestionate" înseamnă un furnizor de servicii gestionate care efectuează sau furnizează asistenţă pentru activităţi legate de gestionarea riscurilor în materie de securitate cibernetică;	Art. 4 lit. k)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) k) *furnizor de servicii de securitate gestionate* înseamnă un furnizor de servicii gestionate care efectuează sau furnizează asistenţă pentru activităţi legate de gestionarea riscurilor în materie de securitate cibernetică;	
	41. „organizaţie de cercetare" înseamnă o entitate care are ca obiectiv principal să desfăşoare activităţi de cercetare aplicată sau de dezvoltare experimentală în vederea exploatării rezultatelor cercetării respective în scopuri	Art. 4 lit. r)	În înţelesul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarea semnificaţie: (...) r) *organism de cercetare* înseamnă o entitate al cărei obiectiv principal este	

	comerciale, dar care nu include instituțiile de învățământ		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;	
Art. 7	(1) Fiecare stat membru adoptă o strategie națională de securitate cibernetică care 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. Strategia națională de securitate cibernetică include următoarele elemente:	Art. 21 alin. (1) Art. 22 alin. (1) și (3) Art. 23 alin. (1)	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. Art. 22 (1) Strategia națională de securitate cibernetică este elaborată de către DNSC, cu consultarea celorlalte autorități cu atribuții în domeniul securității cibernetice conform prevederilor Legii nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, cu avizul COSC și este adoptată prin hotărâre a Guvernului, împreună cu planul de acțiune pentru implementarea strategiei, care este anexă la aceasta.. (3) Strategia națională de securitate cibernetică prevede obiectivele strategice, resursele necesare pentru atingerea obiectivelor respective și	

			măsurile de politică şi de reglementare adecvate în vederea atingerii şi menţinerii unui nivel ridicat de securitate cibernetică. Art. 23 (1) Strategia naţională de securitate cibernetică elaborată conform art. 22 cuprinde cel puţin următoarele:	
	a) obiectivele şi priorităţile strategiei de securitate cibernetică a statului membru, care acoperă în special sectoarele menţionate în anexele I şi II	Art. 23 alin. (1) lit. a)	a) obiectivele şi priorităţile strategiei naţionale de securitate cibernetică, care acoperă în special sectoarele menţionate în anexele 1 şi 2;	
	b) un cadru de guvernanţă pentru realizarea obiectivelor şi priorităţilor menţionate la litera (a) de la prezentul alineat, inclusiv politicile menţionate la alineatul (2);	Art. 23 alin. (1) lit. b)	b) un cadru de guvernanţă pentru realizarea obiectivelor şi priorităţilor menţionate la lit. a), inclusiv politicile publice;	
	c) un cadru de guvernanţă care clarifică rolurile şi responsabilităţile părţilor interesate relevante la nivel naţional, care sprijină cooperarea şi coordonarea la nivel naţional între autorităţile competente, punctele unice de contact şi echipele CSIRT în temeiul prezentei directive, precum şi coordonarea şi cooperarea dintre aceste organisme şi autorităţile competente în temeiul actelor juridice sectoriale ale Uniunii;	Art. 23 alin. (1) lit. c)	c) un cadru de guvernanţă care clarifică rolurile şi responsabilităţile părţilor interesate relevante la nivel naţional, care sprijină cooperarea şi coordonarea la nivel naţional între autorităţile competente, punctele unice de contact şi echipele de răspuns la incidente de securitate cibernetică în temeiul prezentei ordonanţe de urgenţă, precum şi coordonarea şi cooperarea dintre aceste organisme şi autorităţile competente în temeiul actelor juridice sectoriale ale Uniunii Europene;	
	d) un mecanism care să identifice activele şi o evaluare a riscurilor din statul membru respectiv;	Art. 23 alin. (1) lit. d)	d) un mecanism care să identifice activele relevante şi o evaluare a riscurilor la nivel naţional;	
	e) o identificare a măsurilor de asigurare a pregătirii pentru incidente, a capacităţii de răspuns la acestea şi a redresării în urma acestora, inclusiv cooperarea dintre sectorul public şi cel privat;	Art. 23 alin. (1) lit. e)	e) o identificare a măsurilor de asigurare a pregătirii pentru incidente la nivel naţional, a capacităţii de răspuns la acestea şi a redresării în urma acestora, inclusiv cooperarea dintre sectorul public şi cel privat;	
	f) o listă a diferitelor autorităţi şi părţi interesate care participă la punerea în	Art. 23 alin. (1) lit. f)	f) o listă a diferitelor autorităţi şi părţi interesate care participă la punerea în	

	aplicare a strategiei naţionale de securitate cibernetică;		aplicare a strategiei naţionale de securitate cibernetică;	
	g) un cadru de politică menit să asigure o mai bună coordonare între autorităţile competente în temeiul prezentei directive şi al Directivei (UE) 2022/2557 în scopul schimbului de informaţii privind riscurile, ameninţările cibernetice şi incidentele, precum şi privind riscurile, ameninţările şi incidentele fără caracter cibernetic şi al exercitării sarcinilor de supraveghere, după caz;	Art. 23 alin. (1) lit. g)	g) un cadru de politică menit să asigure o mai bună coordonare între autorităţile competente în temeiul prezentei ordonanţe de urgenţă şi al dispoziţiilor legale privind reziliența entităţilor critice în scopul schimbului de informaţii privind riscurile, ameninţările cibernetice şi incidentele, precum şi privind riscurile, ameninţările şi incidentele fără caracter cibernetic şi al exercitării sarcinilor de supraveghere, după caz;	
	h) un plan, inclusiv măsurile necesare pentru a spori nivelul general de sensibilizare a cetăţenilor cu privire la securitatea cibernetică.	Art. 23 alin. (1) lit. h)	h) un plan care să cuprindă inclusiv măsurile necesare pentru a spori nivelul general de sensibilizare a cetăţenilor cu privire la securitatea cibernetică.	
	(2) În cadrul strategiei naţionale de securitate cibernetică, statele membre adoptă politici:	Art. 23 alin. (2)	(2) În cadrul strategiei naţionale de securitate cibernetică se prevăd cel puţin următoarele politici publice:	
	a) care abordează securitatea cibernetică în lanţul de aprovizionare pentru produsele TIC şi serviciile TIC utilizate de entităţi pentru furnizarea serviciilor lor	Art. 23 alin. (2) lit. a)	a) care abordează securitatea cibernetică a lanţului de aprovizionare pentru produsele TIC şi serviciile TIC utilizate de entităţi pentru furnizarea serviciilor lor;	
	b) privind includerea şi specificarea cerinţelor legate de securitatea cibernetică pentru produsele TIC şi serviciile TIC în cadrul achiziţiilor publice, inclusiv în legătură cu certificarea de securitate cibernetică, criptarea şi utilizarea produselor de securitate cibernetică cu sursă deschisă	Art. 23 alin. (2) lit. b)	b) care privesc includerea şi specificarea cerinţelor legate de securitatea cibernetică pentru produsele TIC şi serviciile TIC în cadrul achiziţiilor publice, inclusiv în legătură cu certificarea de securitate cibernetică, criptarea şi utilizarea produselor de securitate cibernetică cu sursă deschisă;	
	c) de gestionare a vulnerabilităţilor, inclusiv promovarea şi facilitarea divulgării coordonate a vulnerabilităţilor în temeiul articolului 12 alineatul (1);	Art. 23 alin. (2) lit. c)	c) de gestionare a vulnerabilităţilor, inclusiv promovarea şi facilitarea divulgării coordonate a vulnerabilităţilor;	
	d) legate de menţinerea disponibilităţii, integrităţii şi confidenţialităţii generale a nucleului public al internetului deschis,	Art. 23 alin. (2) lit. d)	d) legate de menţinerea disponibilităţii, integrităţii şi confidenţialităţii generale a nucleului public al internetului deschis, inclusiv securitatea cibernetică	

	inclusiv securitatea cibernetică a cablurilor de comunicații submarine, după caz;		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;	Art. 23 alin. (2) lit. e)	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;	Art. 23 alin. (2) lit. f)	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;	Art. 23 alin. (2) lit. g)	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;	Art. 23 alin. (2) lit. h)	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 directive, prin furnizarea de orientări și asistență ușor accesibile pentru nevoile lor specifice;	Art. 23 alin. (2) lit. i)	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.	Art. 23 alin. (2) lit. j)	j) de promovare a unei protecții cibernetice active.	

	(3) Statele membre notifică Comisiei strategiile lor naționale de securitate cibernetică în termen de trei luni de la adoptarea acestora. Statele membre pot exclude din astfel de notificări informații care se referă la securitatea lor națională.	Art. 22 alin. (5)	(5) În termen de trei luni de la data adoptării strategiei naționale de securitate cibernetică, DNSC transmite Comisiei Europene aceasta.	
	(4) Statele membre își evaluează periodic, dar cel puțin o dată la cinci ani, strategiile naționale de securitate cibernetică pe baza indicatorilor-cheie de performanță și, dacă este necesar, le actualizează. ENISA sprijină statele membre, la cererea acestora, la elaborarea sau actualizarea unei strategii naționale de securitate cibernetică și a unor indicatori-cheie de performanță pentru evaluarea strategiei respective, în vederea alinierii acesteia la cerințele și obligațiile prevăzute în prezenta directivă	Art. 22 alin. (2) si (4)	(2) În elaborarea sau actualizarea strategiei naționale de securitate cibernetică, DNSC poate solicita asistența ENISA. (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.	
Art. 8	(1) Fiecare stat membru desemnează sau instituie una sau mai multe autorități competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere menționate în capitolul VII (autorități competente).	Art. 24 alin. (1)	(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.	Doar DNSC este autoritate competentă la nivel național în domeniul securității cibernetice
	(2) Autoritățile competente menționate la alineatul (1) monitorizează punerea în aplicare a prezentei directive la nivel național.	Art. 25 alin. (1)	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; 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	

		Art. 53 Art. 54	domeniul de aplicare al prezentei ordonanțe de urgență; d) administrează și gestionează resursele pentru punerea în aplicarea 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 deservesc 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;	

		Art. 55 Art. 56	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 TIC, serviciilor TIC și proceselor TIC ce corespund cerințelor de standardizare și certificare în domeniul securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881 și a serviciilor de încredere calificate, cu respectarea standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice; n) reglementează și gestionează procesul de divulgare coordonată a vulnerabilităților. 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.	
	(3) Fiecare stat membru desemnează sau instituie un punct unic de contact. În cazul în care un stat membru desemnează sau instituie o singură autoritate competentă conform alineatului (1), autoritatea competentă respectivă servește, de asemenea, drept punct unic de contact pentru statul membru respectiv.	Art. 40 alin. (1)	(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.	Nu este necesara transpunerea art. 8 alin. (3) teza 2 din directiva. In temeiul art. 8 alin. (1) din directiva, la nivel national sunt desemnate mai multe autoritati competente si, dintre acestea, DNSC asigura punctul unic de contact.
	(4) Fiecare punct unic de contact exercită o funcție de legătură menită să asigure cooperarea transfrontalieră a autorităților din statul membru de care aparține cu autoritățile relevante din alte state membre, și, acolo unde este cazul, cu Comisia și cu ENISA, dar și să asigure cooperarea transsectorială cu alte autorități competente din statul membru de care aparține.	Art. 40 alin. (2) lit. a) și b) Art. 37 alin. (1) lit. d)	(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, acolo unde este cazul, cu Comisia Europeană, ENISA, Grupul de cooperare și Rețeaua CSIRT; b) informează celelalte state membre sau partenere afectate dacă incidentul are un impact semnificativ asupra continuității serviciilor esențiale ori a serviciilor importante în statele respective; Art. 37 (1) În vederea asigurării unui nivel comun ridicat de securitate cibernetică la nivel național, DNSC se consultă și cooperează cu următoarele: (...) d) alte autorități competente sectorial în domeniul securității cibernetice, conform anexelor 1 și 2.	
	(5) Statele membre se asigură că autoritățile lor competente și punctele unice de contact dispun de resurse adecvate pentru a-și îndeplini în mod	Art. 24 alin. (3)	(3) În vederea îndeplinirii atribuțiilor ce îi revin în temeiul prevederilor prezentei ordonanțe de urgență, DNSC se asigură că deține personal suficient	

	eficace şi eficient atribuţiile şi a realiza astfel obiectivele prezentei directive.		şi competent şi că dispune de resurse adecvate pentru a-şi îndeplini în mod eficace şi eficient atribuţiile.	
	(6) Fiecare stat membru notifică fără întârzieri nejustificate Comisiei identitatea autorităţii competente menţionate la alineatul (1) şi a punctului unic de contact menţionat la alineatul (3), sarcinile respectivelor autorităţi şi orice modificare ulterioară a acestora. Fiecare stat membru face publică identitatea autorităţii sale competente. Comisia face publică lista punctelor unice de contact	Art. 29 alin. (4)	(4) În termen de trei luni de la intrarea în vigoare a prezentei ordonanţe de urgenţă, punctul unic de contact naţional notifică Comisiei Europene şi EU-CyCLONe calitatea DNSC de autoritate naţională de gestionare a crizelor cibernetice, precum şi orice modificări ulterioare ale acestei calităţi.	
Art. 9	(1) Fiecare stat membru desemnează sau instituie una sau mai multe autorităţi competente responsabile cu gestionarea incidentelor de securitate cibernetică de mare amploare şi a crizelor (denumite în continuare „autorităţi de gestionare a crizelor cibernetice"). Statele membre se asigură că respectivele autorităţi dispun de resurse adecvate pentru a îndeplini, în mod eficace şi eficient, sarcinile care le-au fost încredinţate. Statele membre asigură corelarea cu cadrele existente pentru gestionarea naţională generală a crizelor.	Art. 24 alin. (3) şi (4) Art. 28 alin. (1) Art. 29 alin. (1)	Art. 24 (3) În vederea îndeplinirii atribuţiilor ce îi revin în temeiul prevederilor prezentei ordonanţe de urgenţă, DNSC se asigură că deţine personal suficient şi competent şi că dispune de resurse adecvate pentru a-şi îndeplini în mod eficace şi eficient atribuţiile. (4) Pentru aplicarea alin. (3), din bugetul DNSC se asigură, cu respectarea prevederilor legale, următoarele categorii de cheltuieli: a) achiziţionarea de servicii de specialitate; b) achiziţia de echipamente şi software, inclusiv software dezvoltat la comandă; c) afilierea la reţele şi organizaţii internaţionale de profil şi participarea prin reprezentanţi la lucrările acestora precum şi la alte evenimente de profil; d) cursuri de formare şi perfecţionare precum şi certificări ale personalului propriu; e) editarea de publicaţii, ghiduri de specialitate, clipuri video de conştientizare; f) organizarea de conferinţe, seminare şi alte evenimente de profil; g) efectuarea de studii statistice şi activităţi de cercetare.	

			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. 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) În cazul în care un stat membru desemnează sau instituie mai mult de o autoritate de gestionare a crizelor cibernetice în temeiul alineatului (1), acesta indică în mod clar care dintre autoritățile respective servește drept coordonator pentru gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor.	Art. 28 alin. (1) Art. 29 alin. (1) și (4)	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. Art. 29	Singura autoritate competentă la nivel național responsabilă cu gestionarea incidentelor de securitate cibernetică de mare amploare și crize de securitate cibernetică este DNSC. Nefiind o altă autoritate menționată în cadrul acestei prevederi, reiese în mod clar că nu există alta în afară de DNSC. Printr-o interpretare contrară, considerăm că se adaugă la lege.

			(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. (4) În termen de trei luni de la intrarea în vigoare a prezentei ordonanțe de urgență, punctul unic de contact național notifică Comisiei Europene și EU-CyCLONe calitatea DNSC de autoritate națională de gestionare a crizelor cibernetice, precum și orice modificări ulterioare ale acestei calități.	
	(3) Fiecare stat membru identifică capacitățile, mijloacele și procedurile care pot fi utilizate în caz de criză în sensul prezentei directive.	Art. 29 alin. (1) si (2)	(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 cibernetice și prevede cel puțin: a) obiectivele măsurilor și ale activităților de pregătire; b) sarcinile și responsabilitățile autorităților de gestionare a crizelor cibernetice; c) procedurile de gestionare a crizelor cibernetice, 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 naţionale şi acordurile dintre autorităţile şi organismele naţionale relevante menite să asigure participarea efectivă a României la gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare şi a crizelor la nivelul Uniunii Europene şi sprijinul acordat de aceasta.	
	(4) Fiecare stat membru adoptă un plan naţional de răspuns la incidente de securitate cibernetică de mare amploare şi crize, în care sunt stabilite obiectivele şi modalităţile de gestionare a incidentelor de securitate cibernetică de mare amploare şi a crizelor. Planul respectiv stabileşte, în special:	Art. 29 alin. (1) si (2)	(1) Gestionarea la nivel naţional a incidentelor şi a crizelor de securitate cibernetică se realizează în conformitate cu Planul de management al crizelor de securitate cibernetică la nivel naţional pe timp de pace. (2) Planul de management al crizelor de securitate cibernetică la nivel naţional pe timp de pace are ca scop gestionarea incidentelor de securitate cibernetică de mare amploare şi al crizelor cibernetice şi prevede cel puţin:	
	a) obiectivele măsurilor şi ale activităţilor naţionale de pregătire;	Art. 29 alin. (2) lit. a)	a) obiectivele măsurilor şi ale activităţilor de pregătire;	
	b) sarcinile şi responsabilităţile autorităţilor de gestionare a crizelor cibernetice;	Art. 29 alin. (2) lit. b)	b) sarcinile şi responsabilităţile autorităţilor de gestionare a crizelor cibernetice;	
	c) procedurile de gestionare a crizelor cibernetice, inclusiv integrarea acestora în cadrul naţional general de gestionare a crizelor şi canalele de schimb de informaţii;	Art. 29 alin. (2) lit. c)	c) procedurile de gestionare a crizelor cibernetice, inclusiv integrarea acestora în cadrul naţional general de gestionare a crizelor şi canalele de schimb de informaţii;	
	d) măsurile naţionale de pregătire, inclusiv exerciţii şi activităţi de formare;	Art. 29 alin. (2) lit. d)	d) măsurile de pregătire, inclusiv exerciţii şi activităţi de formare;	
	e) părţile interesate relevante din sectorul public şi privat şi infrastructura implicată;	Art. 29 alin. (2) lit. e)	e) părţile interesate relevante din sectorul public şi privat şi infrastructura implicată;	
	f) procedurile naţionale şi acordurile dintre autorităţile şi organismele naţionale relevante menite să asigure participarea efectivă a statului membru la gestionarea coordonată a incidentelor de securitate cibernetică de mare	Art. 29 alin. (2) lit. f)	f) procedurile naţionale şi acordurile dintre autorităţile şi organismele naţionale relevante menite să asigure participarea efectivă a României la gestionarea coordonată a incidentelor de securitate cibernetică de mare	

	amploare şi a crizelor la nivelul Uniunii şi sprijinul acordat de acesta.		amploare şi a crizelor la nivelul Uniunii Europene şi sprijinul acordat de aceasta.	
	(5) În termen de trei luni de la desemnarea sau instituirea autorităţii de gestionare a crizelor cibernetice menţionate la alineatul (1), fiecare stat membru notifică Comisiei identitatea autorităţii sale şi orice modificări ulterioare ale acesteia. Statele membre prezintă Comisiei şi Reţelei europene a organizaţiilor de legătură în materie de crize cibernetice (EU-CyCLONe) informaţii relevante referitoare la cerinţele de la alineatul (4) cu privire la planurile lor naţionale de răspuns la incidente de securitate cibernetică de mare amploare şi crize, în termen de trei luni de la adoptarea planurilor respective. Statele membre pot exclude informaţii în cazul şi în măsura în care o asemenea excludere este necesară pentru securitatea lor naţională.	Art. 29 alin. (3) si (4) Art. 3 alin. (1) şi (2) din OUG 104 din 22 septembrie 2021 privind înfiinţarea Directoratului Naţional de Securitate Cibernetică	(3) În termen de trei luni de la adoptarea sau modificarea Planului prevăzut la alin. (1), DNSC transmite Comisiei Europene şi Reţelei europene a organizaţiilor de legătură în materie de crize cibernetice, denumită în continuare „EU-CyCLONe", informaţii relevante în legătură cu acesta, cu excepţia informaţiilor care pot aduce atingere securităţii naţionale. (4) În termen de trei luni de la intrarea în vigoare a prezentei ordonanţe de urgenţă, punctul unic de contact naţional notifică Comisiei Europene şi EU-CyCLONe calitatea DNSC de autoritate naţională de gestionare a crizelor cibernetice, precum şi orice modificări ulterioare ale acestei calităţi. Art. 3 (1) Principala responsabilitate a DNSC este asigurarea securităţii cibernetice a spaţiului cibernetic naţional civil, în colaborare cu instituţiile şi autorităţile competente. (2) DNSC este autoritatea competentă la nivel naţional pentru spaţiul cibernetic naţional civil, precum şi pentru gestionarea riscurilor şi a incidentelor de securitate cibernetică.	
Art. 10	(1) Fiecare stat membru desemnează sau instituie una sau mai multe echipe CSIRT. Echipele CSIRT pot fi desemnate sau instituite din cadrul unei autorităţi competente. Echipele CSIRT respectă cerinţele prevăzute la articolul 11 alineatul (1), acoperă cel puţin sectoarele, subsectoarele şi tipurile de entităţi menţionate în anexele I şi II şi sunt responsabile de gestionarea	Art. 24 alin. (2) Art. 29 alin. (2)	Art. 24 (2) DNSC îndeplineşte funcţia de echipă de răspuns la incidente de securitate cibernetică naţională, denumită în continuare „CSIRT naţional", în temeiul dispoziţiilor OUG nr. 104/2021 privind Înfiinţarea Directoratului Naţional de Securitate Cibernetică.	

	incidentelor în conformitate cu o procedură bine definită.	Art. 30 alin. (1) Art. 32 alin. (1) Art. 65 alin. (1) lit. f)	Art. 29 (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 cibernetice și prevede cel puțin: a) obiectivele măsurilor și ale activităților de pregătire; b) sarcinile și responsabilitățile autorităților de gestionare a crizelor cibernetice; c) procedurile de gestionare a crizelor cibernetice, 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. 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.	

			Art. 32 (1) CSIRT-urile trebuie să îndeplinească următoarele cerințe: (...) Art. 65 (1) Prin ordin al Directorului DNSC, care se publică în Monitorul Oficial al României, Partea I, se aprobă: (...) f) Normele tehnice privind compatibilitatea şi interoperabilitatea sistemelor, procedurilor şi metodelor utilizate de către CSIRT-uri şi 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;	
	(2) Statele membre se asigură că fiecare echipă CSIRT dispune de resurse adecvate pentru a-şi îndeplini efectiv sarcinile stabilite la articolul 11 alineatul (3).	Art. 24 alin. (2) si (3) Art. 30 alin. (3)	Art. 24 (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 temeiul prevederilor prezentei ordonanțe de urgență, DNSC se asigură că deține personal suficient şi competent şi că dispune de resurse adecvate pentru a-şi îndeplini în mod eficace şi eficient atribuțiile. Art. 30 (3) În vederea obținerii autorizării, CSIRT-urile prevăzute la alin. (1) trebuie să probeze deținerea unei infrastructuri de comunicare şi de informații adecvate, sigure şi 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.	
	(3) Statele membre se asigură că fiecare echipă CSIRT dispune de o infrastructură de comunicare și de informații adecvată, sigură și rezilientă prin care face schimb de informații cu entitățile esențiale și entitățile importante și cu alte părți interesate relevante. În acest scop, statele membre se asigură că fiecare echipă CSIRT contribuie la implementarea unor instrumente securizate de schimb de informații.	Art. 30 alin. (3) Art. 33 alin. (1) lit. f)	Art. 30 (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. Art. 33 (1) CSIRT-urile au următoarele responsabilități: (...) f) participarea la implementarea unor instrumente securizate de schimb de informații, în conformitate cu art. 20.	
	(4) Echipele CSIRT cooperează și, după caz, fac schimb de informații relevante în conformitate cu articolul 29 cu comunități sectoriale sau transsectoriale formate din entități esențiale și entități importante.	Art. 30 alin. (4)	(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, cât și cu CSIRT-uri din state terțe, inclusiv pentru a le oferi asistență în materie de securitate cibernetică.	
	(5) Echipele CSIRT participă la evaluările inter pares organizate în conformitate cu articolul 19.	Art. 30 alin. (5) Art. 41 alin. (1) și alin. (2) lit. l)	Art. 30 (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. 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: (...) l) evaluează rapoartele privind evaluarea inter pares, după caz;	
	(6) Statele membre asigură cooperarea efectivă, eficientă și sigură a propriilor echipe CSIRT în cadrul rețelei CSIRT.	Art. 30 alin. (5) si (6) Art. 41 alin. (1)	Art. 30 (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. Art. 41 (1) DNSC, în calitate de CSIRT național, participă la Rețeaua CSIRT în scop operațional, asigurand cooperarea efectivă, eficientă și sigură a tuturor echipelor CSIRT de la nivel national în cadrul rețelei CSIRT.	
	(7) Echipele CSIRT pot stabili relații de cooperare cu echipele naționale de intervenție în caz de incidente de securitate informatică din țări terțe. În cadrul acestor relații de cooperare, statele membre facilitează un schimb de informații eficace, eficient și securizat cu respectivele echipe naționale de intervenție în caz de incidente de securitate informatică din țări terțe, utilizând protocoalele relevante de schimb de informații, inclusiv „Traffic Light Protocol". Echipele CSIRT pot face schimb de informații relevante cu echipele naționale de intervenție în caz de incidente de securitate informatică din țări terțe, inclusiv de date cu caracter personal în conformitate cu dreptul Uniunii privind protecția datelor.	Art. 30 alin. (5) Art. 62 alin. (3) si (4)	Art. 30 (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. Art. 62 (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.	
	(8) Echipele CSIRT pot coopera cu echipele naționale de intervenție în caz de incidente de securitate informatică sau cu organisme echivalente din țări terțe, în special pentru a le oferi asistență în materie de securitate cibernetică.	Art. 32 alin. (3) Art. 40 alin. (2) Art. 41 alin. (2)	Art. 32 (3) CSIRT-urile stabilesc relații de cooperare cu părțile interesate relevante în vederea îndeplinirii atribuțiilor acestora. Art. 40 (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, acolo unde este cazul, cu Comisia Europeană, ENISA, Grupul de cooperare și Rețeaua CSIRT; b) informează celelalte state membre sau partenere afectate 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	

		Art. 4 lit. d) din OUG 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică Art. 5 lit. h) punctul 1, 5, 6 și 7 din OUG 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică Art. 16 alin. (3) din OUG 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică	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; Art. 41 (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; f) implementează și utilizează specificațiile și protocoalele referitoare la schimbul de informații care să asigure interoperabilitatea cu celelalte CSIRT-uri din cadrul Uniunii Europene; Art. 4 Principalele obiective ale DNSC sunt: d) crearea și operarea unei platforme naționale de colaborare care să permită schimbul de informații între constituenți, instituții ale statului, mediul academic și mediul privat în	

			domeniul incidentelor, vulnerabilităților și crizelor de natură cibernetică; Art. 5 În îndeplinirea obiectivelor, DNSC exercită următoarele funcții și atribuții: h) Funcția de cooperare și colaborare 1. asigură cadrul de cooperare în vederea derulării de activități specifice asigurării securității cibernetice, cercetării, schimbului de informații, instruirii, educației, conștientizării, elaborării de proiecte, precum și a oricăror altor activități necesare pentru asigurarea securității cibernetice a României, conform competențelor legale; 5. înființează, coordonează și gestionează Platforma Națională de Cooperare în Domeniul Securității Cibernetice, denumită în continuare PNCDSC, între instituțiile de stat, mediul privat, mediul academic și organizații nonguvernamentale, în scopul asigurării unui cadru național unitar de expertiză, cercetare, informare și orice alte acțiuni conexe domeniului de competență; 6. participă în grupuri de cooperare, de lucru sau de specialitate și în rețele de cooperare, forumuri și organizații din domeniul securității cibernetice constituite la nivel național, european și internațional; 7. dezvoltă relații de parteneriat cu alte structuri naționale sau internaționale cu competențe și responsabilități în domeniul securității cibernetice, în acest sens încheind memorandumuri și protocoale de cooperare cu persoane de drept public sau privat, naționale sau străine;	

			Art. 16 (3) Pentru asigurarea unei capacități adecvate de identificare, evaluare și adoptare a unor măsuri de management al riscului și/sau de răspuns la incidente și atacuri cibernetice, DNSC dezvoltă schimburi de informații și transfer de expertiză cu instituțiile și autoritățile cu responsabilități în domeniu, promovează și susține cooperarea între sectorul public și cel privat, precum și cooperarea cu mediile neguvernamentale și comunitatea academică.	
	(9) Fiecare stat membru notifică fără întârzieri nejustificate Comisiei identitatea echipei CSIRT menționate la alineatul (1) de la prezentul articol și a echipei CSIRT desemnată drept coordonator în conformitate cu articolul 12 alineatul (1), sarcinile acestora în legătură cu entitățile esențiale și entitățile importante, precum și orice modificări ulterioare.	Art. 24 alin. (2) Art. 36 alin. (1)	Art. 24 (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. 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.	
	(10) Statele membre pot solicita asistența ENISA pentru instituirea echipelor lor CSIRT.			Nu este necesar pentru România astfel încât nu am considerat oportun a transpune această facultate pusă la dispoziție de către Directivă.

Art. 11	(1) Echipele CSIRT trebuie să respecte următoarele cerințe:	Art. 32 alin. (1)	(1) CSIRT-urile trebuie să îndeplinească următoarele cerințe:	
	a) echipele CSIRT asigură o disponibilitate ridicată a canalelor lor de comunicare evitând punctele unice de defecțiune și dispun de mai multe mijloace pentru a fi contactate și pentru a contacta alte entități în orice moment; acestea specifică în mod clar canalele de comunicare și le aduc la cunoștința bazei de utilizatori și a partenerilor de cooperare;	Art. 32 alin. (1) lit. a) și b)	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 in mod clar canalele de comunicare prevăzute la lit. a) și să le aducă la cunoștință bazei de utilizatori și parteneri de cooperare;	
	b) localurile echipelor CSIRT și sistemele informatice de suport sunt situate în amplasamente securizate;	Art. 32 alin. (1) lit. c)	c) să mențină sediile și sistemele informatice de suport în amplasamente securizate;	
	c) echipele CSIRT dispun de un sistem adecvat de gestionare și rutare a cererilor, în special în vederea facilitării eficace și eficiente a transferurilor;	Art. 32 alin. (1) lit. d)	d) să dispună de un sistem adecvat de gestionare și rutare a cererilor;	
	d) echipele CSIRT asigură confidențialitatea și credibilitatea operațiunilor lor;	Art. 32 alin. (1) lit. e)	e) să asigure confidențialitatea și credibilitatea operațiunilor lor;	
	e) echipele CSIRT dispun de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor lor și se asigură că personalul lor este format în mod corespunzător;	Art. 24 alin. (2)-(3) si alin. (4) lit. d) Art. 32 alin. (1) lit. d) și f) Art. 54 alin. (1)	Art. 24 (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 temeiul prevederilor prezentei ordonanțe de urgență, 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: (...)	

			d) cursuri de formare şi perfecţionare precum şi certificări ale personalului propriu; Art. 32 (1)CSIRT-urile trebuie să îndeplinească următoarele cerinţe: (...) d) să utilizeze în cadrul echipelor un număr corespunzător de persoane calificate; f) să dispună de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor lor; Art. 54 (1) DNSC supraveghează, verifică şi controlează activitatea furnizorilor de servicii de formare pentru securitate cibernetică pentru auditori şi CSIRT-uri.	
	f) echipele CSIRT sunt echipate cu sisteme redundante şi spaţiu de lucru de rezervă pentru a asigura continuitatea serviciilor lor.	Art. 32 alin. (1) lit. g)	(1) CSIRT-urile trebuie să îndeplinească următoarele cerinţe: g) să fie echipate cu sisteme redundante şi spaţiu de lucru de rezervă pentru a asigura continuitatea serviciilor lor, chiar şi după un incident;	
	Echipele CSIRT pot participa la reţele internaţionale de cooperare.	Art. 24 alin. (2) - (4) lit. c) Art. 30 alin. (5)	Art. 24 (2) DNSC îndeplineşte funcţia de echipă de răspuns la incidente de securitate cibernetică naţională, denumită în continuare „CSIRT naţional", în temeiul dispoziţiilor OUG nr. 104/2021 privind Înfiinţarea Directoratului Naţional de Securitate Cibernetică. (3) În vederea îndeplinirii atribuţiilor ce îi revin în temeiul prevederilor prezentei ordonanţe de urgenţă, DNSC se asigură că deţine personal suficient şi competent şi că dispune de resurse adecvate pentru a-şi îndeplini în mod eficace şi eficient atribuţiile.	

			(4) Pentru aplicarea alin. (3), din bugetul DNSC se asigură, cu respectarea prevederilor legale, următoarele categorii de cheltuieli: (...) c) afilierea la rețele și organizații internaționale de profil și participarea prin reprezentanți la lucrările acestora precum și la alte evenimente de profil; Art. 30 (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.	
(2) Statele membre se asigură că echipele lor CSIRT dispun colectiv de capacitățile tehnice necesare pentru a-și îndeplini sarcinile menționate la alineatul (3). Statele membre se asigură că se alocă resurse suficiente echipelor lor CSIRT pentru a garanta un nivel adecvat de personal pentru ca acestea să își poată dezvolta capacitățile tehnice.	Art. 30 alin. (3) Art. 31 alin. (1) lit. g) Art. 32 alin. (1) lit. f) Art. 24 alin. (2)-(4)	Art. 30 (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. Art. 31 (1) CSIRT-urile proprii, sectoriale sau furnizorii de serviciile specifice CSIRT care deservesc entitățile esențiale sau entitățile importante au următoarele obligații: (...) 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. Art. 32	

		Art. 35 alin. (2)	(1) CSIRT-urile trebuie să îndeplinească următoarele cerințe: f) să dispună de personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor lor; Art. 24 (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 temeiul prevederilor prezentei ordonanțe de urgență, 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 şi activităţi de cercetare. Art. 35 (2) CSIRT naţional îndeplineşte cerinţele prevăzute la art. 30 alin. (3) şi art. 32 alin. (1).	
	(3) Echipelor CSIRT le revin următoarele sarcini:	Art. 33 alin. (1)	(1) CSIRT-urile au următoarele responsabilităţi:	
	a) monitorizarea şi analizarea ameninţărilor cibernetice, a vulnerabilităţilor şi a incidentelor la nivel naţional şi, la cerere, acordarea de asistenţă entităţilor esenţiale şi entităţilor importante implicate cu privire la monitorizarea în timp real sau în timp aproape real a reţelei lor şi a sistemelor lor informatice;	Art. 33 alin. (1) lit. a)	a) monitorizarea şi analiza ameninţărilor cibernetice, a vulnerabilităţilor şi a incidentelor la nivel naţional şi, la cerere, acordarea de asistenţă entităţilor esenţiale şi entităţilor importante implicate cu privire la monitorizarea în timp real sau în timp aproape real a reţelei lor şi a sistemelor lor informatice în conformitate cu necesităţile acestora;	
	b) asigurarea unor mecanisme de avertizare timpurii, alerte, anunţuri şi diseminare de informaţii către entităţile esenţiale şi entităţile importante, precum şi către autorităţile competente şi alte părţi interesate relevante cu privire la ameninţările cibernetice, vulnerabilităţi şi incidente, în timp aproape real, dacă este posibil;	Art. 33 alin. (1) lit. b)	b) asigurarea unor mecanisme de avertizare timpurii, alerte, anunţuri şi diseminare de informaţii către entităţile esenţiale şi entităţile importante, precum şi către autorităţile competente şi alte părţi interesate relevante cu privire la ameninţări cibernetice, vulnerabilităţi şi incidente în timp aproape real, dacă este posibil;	
	c) răspunsul la incidente şi acordarea de asistenţă entităţilor esenţiale şi entităţile importante implicate, atunci când este cazul	Art. 33 alin. (1) lit. c)	c) răspunsul la incidente şi acordarea de asistenţă entităţilor esenţiale şi entităţilor importante implicate, atunci când este cazul;	
	d) colectarea şi analizarea datelor criminalistice şi furnizarea de analize dinamice de risc şi de incident şi conştientizarea situaţiei în materie de securitate cibernetică	Art. 33 alin. (1) lit. d)	d) colectarea şi analiza datelor şi furnizarea de analize dinamice de risc şi de incident şi conştientizarea situaţiei în materie de securitate cibernetică;	
	e) furnizarea, la cererea unei entităţi esenţiale sau a unei entităţi importante, a unei scanări proactive a reţelelor şi a sistemelor informatice ale entităţii implicate pentru a detecta vulnerabilităţile cu un impact potenţial semnificativ;	Art. 33 alin. (1) lit. e)	Art. 33 (1) CSIRT-urile au următoarele responsabilităţi: (...) e) furnizarea, la cererea unei entităţi esenţiale sau a unei entităţi importante, a unei scanări de securitate a reţelelor şi	

		Art. 46 alin. (5)	sistemelor informatice ale entității implicate pentru a detecta vulnerabilitățile cu un impact potențial semnificativ; Art. 46 (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.	
	f) participarea la rețeaua CSIRT și furnizarea de asistență reciprocă în funcție de capacitățile și competențele lor altor membri ai rețelei, la cererea acestora;	Art. 30 alin. (5) Art. 41 alin. (1)-(2)	Art. 30 (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. 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: (...) 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;	
	g) după caz, acționarea în calitate de coordonator în scopul procesului de	Art. 36 alin. (1)	(1) DNSC, în calitate de CSIRT național, este responsabil de gestionarea procesului de divulgare	

	divulgare coordonată a vulnerabilităților menționat la articolul 12 alineatul (1);		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.	
	h) contribuirea la implementarea unor instrumente securizate de schimb de informații, în temeiul articolului 10 alineatul (3).	Art. 33 alin. (1) lit. f)	(1) CSIRT-urile au următoarele responsabilități: (...) f) participarea la implementarea unor instrumente securizate de schimb de informații, în conformitate cu art. 20.	
	Echipele CSIRT pot efectua scanări proactive și neintruzive ale rețelelor și sistemelor informatice accesibile publicului ale entităților esențiale și ale entităților importante. Asemenea scanări se efectuează pentru a detecta rețelele și sistemele informatice vulnerabile sau configurate în mod nesigur și pentru a informa entitățile în cauză. Asemenea scanări nu au niciun impact negativ asupra funcționării serviciilor entităților.	Art. 33 alin. (1) lit. e) si (2) Art. 46 alin. (5)	Art. 33 (1) CSIRT-urile au următoarele responsabilități: 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; (2) Scanările prevăzute la alin. (1) lit. e) se pot efectua si cu privire la rețelele și sistemele informatice accesibile publicului ale entităților esențiale și ale entităților importante, sunt neintruzive, se efectuează pentru a detecta rețelele și sistemele informatice vulnerabile sau configurate în mod nesigur și pentru a informa entitățile în cauză și nu aduc niciun efect negativ funcționalității serviciilor entităților în cauză. Art. 46 (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 şi proactive, bazate pe criterii obiective, nediscriminatorii, echitabile şi transparente pentru evaluarea riscurilor, cu notificarea prealabilă a entităţii în cauză şi, după caz, în cooperare cu aceasta.	
	Atunci când îndeplinesc sarcinile menţionate la primul paragraf, echipele CSIRT pot acorda prioritate anumitor sarcini pe baza unei abordări bazate pe riscuri.	Art. 46 alin. (5) Art. 47 alin. (8)	Art. 46 (5) În vederea punerii în aplicare a alin. (1) lit. a) cu privire la entităţille esenţiale şi entităţile importante, DNSC poate efectua scanări de securitate cibernetică neintruzive şi proactive, bazate pe criterii obiective, nediscriminatorii, echitabile şi transparente pentru evaluarea riscurilor, cu notificarea prealabilă a entităţii în cauză şi, după caz, în cooperare cu aceasta. Art. 47 (8) Normele de aplicare şi metodologia de prioritizare pe bază de risc a activităţilor de supraveghere, verificare şi control sunt emise prin ordin al Directorului DNSC.	
	(4) Echipele CSIRT stabilesc relaţii de cooperare cu părţile interesate relevante din sectorul privat, în vederea îndeplinirii obiectivelor prezentei directive.	Art. 30 alin. (1), (4) si (5) Art. 32 alin. (3)	Art. 30 (1) Entităţile esenţiale, entităţile importante şi autorităţile competente sectorial pot constitui echipe de răspuns la incidente de securitate cibernetică, denumite în continuare „CSIRT", proprii sau sectoriale ori pot achiziţiona servicii de specialitate de la furnizori de servicii specifice CSIRT, autorizaţi de către DNSC. (4) CSIRT-urile prevăzute la alin. (1) cooperează şi fac schimb de informaţii relevante cu comunităţile sectoriale sau trans-sectoriale formate din entităţi esenţiale şi entităţi importante, cât şi cu CSIRT-uri din state terţe, inclusiv	

			pentru a le oferi asistență în materie de securitate cibernetică. (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. Art. 32 (3) CSIRT-urile stabilesc relații de cooperare cu părțile interesate relevante în vederea îndeplinirii atribuțiilor acestora.	
	(5) Pentru a facilita cooperarea menționată la alineatul (4), echipele CSIRT promovează adoptarea și utilizarea unor practici, sisteme de clasificare și taxonomii comune sau standardizate în legătură cu:	Art. 32 alin. (4)	(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	Art. 32 alin. (4) lit. a)	a) procedurile de gestionare a incidentelor;	
	b) gestionarea crizelor; și	Art. 32 alin. (4) lit. b)	b) gestionarea crizelor;	
	c) divulgarea coordonată a vulnerabilităților în temeiul articolului 12 alineatul (1)	Art. 32 alin. (4) lit. c) Art. 36 alin. (1)	Art. 32 (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: (...) c) divulgarea coordonată a vulnerabilităților, în temeiul art. 36. 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.	
Art. 12	(1) Fiecare stat membru desemnează una dintre echipele sale CSIRT drept coordonator în scopul divulgării coordonate a vulnerabilităților. Echipa CSIRT desemnată drept coordonator acționează ca intermediar de încredere, facilitând, dacă 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. Sarcinile echipei CSIRT desemnate drept coordonator includ:	Art. 36 alin. (1)	(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.	
	a) identificarea și contactarea entităților implicate	Art. 36 alin. (2) lit. c)	(2) În îndeplinirea alin. (1), DNSC: (...) 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;	
	b) asistarea persoanelor fizice sau juridice care raportează o vulnerabilitate	Art. 36 alin. (2) lit. j)	(2) În îndeplinirea alin. (1), DNSC: (...) j) poate asista persoanele care raportează o vulnerabilitate.	
	c) negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe entități.	Art. 36 alin. (2) lit. g)	(2) În îndeplinirea alin. (1), DNSC: (...) g) negociază cu entitățile afectate calendarele de divulgare și gestionare a vulnerabilităților care afectează mai multe entități;	
	Statele membre se asigură că persoanele fizice sau juridice pot raporta, în mod anonim atunci când solicită acest lucru, o vulnerabilitate	Art. 36 alin. (1) si alin. (2) lit. b), e), f) si h)	(1) DNSC, în calitate de CSIRT național, este responsabil de gestionarea procesului de divulgare	

	echipei CSIRT desemnate drept coordonator. Echipa CSIRT desemnată drept coordonator se asigură că au loc acțiuni subsecvente susținute în ceea ce privește vulnerabilitatea raportată și asigură anonimatul persoanei fizice sau juridice care raportează vulnerabilitatea. În cazul în care o vulnerabilitate raportată ar putea avea un impact semnificativ asupra entităților în mai multe state membre, echipa CSIRT desemnată drept coordonator din fiecare stat membru în cauză cooperează, dacă este cazul, cu alte echipe CSIRT desemnate drept coordonatori în cadrul rețelei CSIRT.		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: (...) b) asigură posibilitatea anonimatului persoanei care raportează o vulnerabilitate, la solicitarea acesteia, inclusiv în contextul acțiunilor subsecvente; 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; h) atunci când o vulnerabilitate raportată ar putea avea un impact semnificativ transfrontalier, cooperează, după caz, cu CSIRT-urile desemnate din cadrul Rețelei CSIRT;	
	(2) ENISA creează și menține, după consultarea Grupului de cooperare, o bază de date europeană a vulnerabilităților. În acest scop, ENISA instituie și menține sisteme, politici și proceduri de informare adecvate și adoptă măsurile tehnice și organizatorice necesare pentru a garanta securitatea și integritatea bazei de date europene a vulnerabilităților, în special pentru a permite			Prezenta prevedere impune o obligație pentru ENISA și nu pentru statele membre, motiv pentru care nu necesită transpunere.

	entităților, indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, și furnizorilor acestora de rețele și sisteme informatice să divulge și să înregistreze, pe bază voluntară, vulnerabilitățile public cunoscute din produsele TIC sau serviciile TIC. Se oferă acces tuturor părților interesate la informațiile privind vulnerabilitățile conținute în baza de date europeană a vulnerabilităților. Baza de date include: a) informații care descriu vulnerabilitatea b) produsele TIC sau serviciile TIC afectate și gravitatea vulnerabilității în ceea ce privește circumstanțele în care aceasta poate fi exploatată c) disponibilitatea unor corecții conexe și, dacă astfel de corecții nu sunt disponibile, orientări oferite de autoritățile competente sau de echipele CSIRT adresate utilizatorilor de produse TIC și servicii TIC vulnerabile cu privire la modul în care pot fi atenuate riscurile care rezultă din vulnerabilitățile divulgate.			
Art. 13	(1) Atunci când sunt separate, autoritățile competente, punctul unic de contact și echipele CSIRT ale aceluiași stat membru cooperează între ele pentru îndeplinirea obligațiilor ce le revin în temeiul prezentei directive.	Art. 30 alin. (5) si (6)	(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.	
	(2) Statele membre se asigură că echipele lor CSIRT sau, atunci când este cazul, autoritățile lor competente primesc notificări privind incidentele semnificative în temeiul articolului 23, și incidentele, amenințările cibernetice și incidentele evitate la limită în temeiul articolului 30.	Art. 15 alin. (1), (2) si (16)	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	

		Art. 16 alin. (1)	care ar putea afecta prestarea serviciilor respective. (2) Raportarea se face prin intermediul Platformei naţionale pentru raportarea incidentelor de securitate cibernetică, denumită în continuare PNRISC, astfel cum este prevăzută la art. 20 din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative. (16) DNSC furnizează Centrului Naţional de Coordonare a Protecţiei Infrastructurilor Critice, denumit în continuare „CNCPIC", informaţii cu privire la incidentele semnificative, incidentele, ameninţările cibernetice şi incidentele evitate la limită raportate conform alin. (1) şi cu prevederile privitoare la raportarea voluntară de către entităţile identificate ca fiind entităţi critice în temeiul dispoziţiilor legale privind reziliența entităţilor critice. Art. 16 (1) Pot raporta către echipa de răspuns la incidente de securitate cibernetică naţională: a) entităţile esenţiale şi entităţile importante, cu privire la incidente, ameninţări cibernetice şi incidente evitate la limită; b) alte entităţi decât cele menţionate la lit. a), indiferent dacă intră în domeniul de aplicare al prezentei ordonanţe de urgenţă, cu privire la incidente semnificative, ameninţări cibernetice şi incidente evitate la limită.	
	(3) Statele membre se asigură că echipele sale CSIRT sau, atunci când este cazul, autorităţile sale competente informează punctele lor unice	Art. 15 alin. (1) si (2)	Art. 15 (1) Entităţile esenţiale şi entităţile importante raportează, fără întârzieri	În cadrul DNSC funcţionează echipa CSIRT naţională, este punct unic de contact şi

	de contact cu privire la notificările privind incidentele, amenințările cibernetice și incidentele evitate la limită comunicate în temeiul prezentei directive.	Art. 16 alin. (1) Art. 20 alin. (1) din Legea nr. 58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative	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. 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. Art. 20 (1) DNSC dezvoltă și asigură managementul Platformei naționale pentru raportarea incidentelor de securitate cibernetică, denumită în continuare PNRISC.	administrează platforma de raportare a incidentelor de securitate cibernetică

	(4) Pentru a garanta că sarcinile şi obligaţiile autorităţilor competente, ale punctelor unice de contact şi ale echipelor CSIRT sunt îndeplinite în mod eficient, statele membre asigură, în măsura posibilului, o cooperare adecvată între aceste organisme şi autorităţile de aplicare a legii, autorităţile pentru protecţia datelor, autorităţile naţionale în temeiul Regulamentelor (CE) nr. 300/2008 şi (UE) 2018/1139, organismele de supraveghere în temeiul Regulamentului (UE) nr. 910/2014, autorităţile competente în temeiul Regulamentului (UE) 2022/2554, autorităţile naţionale de reglementare în temeiul Directivei (UE) 2018/1972, autorităţile competente în temeiul Directivei (UE) 2022/2557, precum şi autorităţile competente în temeiul altor acte juridice sectoriale ale Uniunii, din statul membru respectiv.	Art. 30 alin. (4) si (6) Art. 37 alin. (1)-(4), (7)-(10)	Art. 30 (4) CSIRT-urile prevăzute la alin. (1) cooperează şi fac schimb de informaţii relevante cu comunităţile sectoriale sau trans-sectoriale formate din entităţi esenţiale şi entităţi importante, cât şi cu CSIRT-uri din state terţe, inclusiv pentru a le oferi asistenţă în materie de securitate cibernetică. (6) CSIRT-urile prevăzute la alin. (1) cooperează atât între ele, cât şi cu CSIRT naţional. Art. 37 (1) În vederea asigurării unui nivel comun ridicat de securitate cibernetică la nivel naţional, DNSC se consultă şi cooperează cu următoarele: a) Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, denumită în continuare „ANCOM" care este autoritate competentă sectorial în domeniul securităţii cibernetice, potrivit prevederilor prezentei ordonanţe de urgenţă, pentru sectorul „8. Infrastructură digitală": „Furnizorii de IXP (internet exchange point)", „Furnizorii de reţele publice de comunicaţii electronice" şi „Furnizorii de servicii de comunicaţii electronice accesibile publicului" din Anexa 1 şi pentru Sectorul „1. Servicii poştale şi de curierat" din Anexa 2; b) autorităţile, astfel cum acestea se identifică în temeiul 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 şi al Consiliului prin stabilirea unui cod de reţea privind normele sectoriale pentru aspectele legate de securitatea	OUG 104/2021 art. 3 alin. (4): (4) Pentru îndeplinirea responsabilităţilor sale, DNSC se consultă şi cooperează, după caz, cu: **a)** instituţiile publice prevăzute la alin. (3); **b)** Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în cazul incidentelor care au ca rezultat încălcarea securităţii datelor cu caracter personal, în condiţiile legii;**c)** Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, atunci când incidentele au ca rezultat afectarea securităţii ori funcţionării reţelelor publice de comunicaţii electronice ori când pentru administrarea unui incident sunt necesare măsuri ce intră în aria de activitate şi responsabilitate a acesteia; **d)** Oficiul Registrului National al Informaţiilor Secrete de Stat, în cazul incidentelor şi atacurilor cibernetice asupra sistemelor informatice şi de comunicaţii care vehiculează informaţii clasificate; **e)** Ministerul Afacerilor Externe, în cazul unor incidente şi atacuri cibernetice care afectează interese pe plan extern ale României; **f)** organele de urmărire penală, în condiţiile legii

			cibernetică a fluxurilor transfrontaliere de energie electrică; c) Autoritatea pentru Digitalizarea României, denumită în continuare ADR care este autoritate competentă sectorial în domeniul securității cibernetice, potrivit prevederilor prezentei ordonanțe de urgență, pentru sectorul „8. Infrastructură digitală": „Prestatorii de servicii de încredere"; d) 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	

		Art. 39	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 eficace 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. (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 ale entităților	

			care îşi desfăşoară activitatea în domeniile de competenţă ale acestora, sens în care se consultă şi cooperează cu CSIRT naţional; e) derula activităţi de evaluare a incidentelor în scopul identificării principalelor cauze, astfel încât să reducă riscul apariţiei unor astfel de incidente; f) elabora ghiduri şi recomandări în domeniul securităţii cibernetice din domeniul de competenţă pentru asigurarea unei capacităţi adecvate de identificare, evaluare şi adoptare a unor măsuri de management al riscului, răspuns la incidente şi atacuri cibernetice, de asigurare a securităţii lanţului de aprovizionare, precum şi de gestionare a situaţiilor de criză; (8) Autorităţile, astfel cum sunt stabilite la alin. (1), au următoarele atribuţii: a) transmit către DNSC, în măsura în care le deţin, informaţii şi date privind ameninţările cibernetice, inclusiv de indicatori de compromitere, tactici, tehnici şi proceduri, alerte de securitate cibernetică şi instrumente de configurare atunci când aceste schimburi de informaţii şi date vizează sporirea rezilienţei operaţionale digitale a entităţilor din domeniul de competenţă a acestora prin sensibilizarea cu privire la ameninţările cibernetice, limitarea sau împiedicarea răspândirii ameninţărilor cibernetice, sprijinirea gamei de capacităţi defensive ale entităţilor, tehnicile de detectare a ameninţărilor, strategiile de atenuare sau etapele proceselor de răspuns şi de recuperare; b) emit ordine comune, împreună cu DNSC, în domeniul securităţii 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 alin. (1) și (4)-(9), art. 47 alin. (1)-(7), art. 48-50, art. 51 alin. (1) și art. 57. (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, precum și ale regulamentelor Uniunii Europene din domeniul securității cibernetice și ale actelor de punere în aplicare a dispozițiilor Directivei (UE) 2022/2555 care vizează entitățile din sectorul lor de competență potrivit prezentei ordonanțe de urgență, în cazul în care competențele de supraveghere, control și sancționare ale Regulamentelor, respectiv ale actelor de punere în aplicare, nu au fost acordate altei autorități. 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.	
	(5) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive și autoritățile lor competente în temeiul Directivei (UE) 2022/2557 cooperează și fac schimb periodic de informații pentru identificarea entităților critice, cu privire la riscurile, amenințările cibernetice și incidentele, precum și la riscurile, amenințările și incidentele de altă natură decât cibernetică care afectează entitățile esențiale identificate ca fiind critice în temeiul Directivei (UE) 2022/2557, precum și cu privire la măsurile luate ca răspuns la astfel de riscuri, amenințări și incidente. Statele membre se asigură, de asemenea, că autoritățile lor competente în temeiul prezentei directive și autoritățile lor competente în temeiul Regulamentului (UE) nr. 910/2014, al Regulamentului (UE) 2022/2554 și al Directivei (UE) 2018/1972 fac schimb de informații relevante în mod periodic, inclusiv în ceea ce privește incidentele și amenințările cibernetice relevante.	Art. 37 alin. (2)- (3) si (12)	Art. 37 (2) În vederea asigurării unui nivel comun ridicat de securitate cibernetică la nivel național, DNSC se coordonează cu CNCPIC și face schimb de informații periodic 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 acestea. (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:	

		Art. 51	a) BNR şi ASF transmit în timp util către DNSC informaţii privind incidentele majore legate de TIC şi ameninţările cibernetice semnificative, raportate de către entităţile cărora li se aplică cerinţele Regulamentului DORA, iar DNSC transmite către BNR şi ASF informaţii privind incidentele majore şi ameninţările cibernetice, raportate de către entităţile esenţiale sau importante cărora li se aplică prezenta ordonanţă de urgenţă şi care au fost desemnate conform Regulamentului DORA drept furnizori terţi esenţiali de servicii TIC; b) BNR şi ASF pot solicita orice tip de consultanţă şi asistenţă tehnică relevantă din partea DNSC, în limita capacităţilor şi resurselor DNSC şi pot stabili acorduri de cooperare pentru a permite crearea unor mecanisme de coordonare eficace şi rapide. (12) Autorităţile competente sectorial îşi pot exercita atribuţiile de supraveghere şi control prevăzute de prezenta ordonanţă de urgenţă inclusiv la solicitarea motivată a CNCPIC, pentru entităţile identificate critice conform dispoziţiilor legale privind reziliența entităţilor critice. Art. 51 (1) DNSC sau, după caz, autoritatea competentă sectorial informează CNCPIC atunci când îşi exercită competenţele de supraveghere şi control asupra unei entităţi esenţiale identificate drept entitate critică în conformitate cu dispoziţiile legale privind reziliența entităţilor critice. (2) CNCPIC poate solicita DNSC să îşi exercite competenţele de supraveghere şi control asupra unei entităţi esenţiale	

			identificate drept entitate critică în conformitate cu dispozițiile legale privind reziliența entităților critice.	
	(6) Statele membre simplifică raportarea prin mijloace tehnice pentru notificările menționate la articolele 23 și 30.	Art. 15 alin. (1) si (2)	(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.	Lege 58/2023, Capitolul IV Managementul incidentelor și reziliența în spațiul cibernetic, Secțiunea 1 Managementul incidentelor de securitate cibernetică: Articolul 20 (1) DNSC dezvoltă și asigură managementul Platformei naționale pentru raportarea incidentelor de securitate cibernetică, denumită în continuare PNRISC. (2) Autoritățile prevăzute la art. 10 au acces la PNRISC, pentru îndeplinirea responsabilităților care le revin. (3) Procesarea informațiilor din PNRISC se realizează cu respectarea politicilor de confidențialitate și transparență stabilite și implementate de DNSC
Art. 14	(1) Pentru a sprijini și a facilita cooperarea strategică și schimbul de informații între statele membre, precum și pentru a consolida încrederea, se instituie un Grup de cooperare			Nu este necesara transpunerea.
	(2) Grupul de cooperare își îndeplinește sarcinile pe baza programelor bienale de lucru menționate la alineatul (7).			Nu este necesara transpunerea. Nu face referire la o obligație a statelor membre, este adresat Comisiei Europene
	(3) Grupul de cooperare este format din reprezentanți ai statelor membre, ai Comisiei și ai ENISA. Serviciul European de Acțiune Externă participă la activitățile Grupului de cooperare în calitate de observator. Autoritățile europene de supraveghere (AES) și autoritățile competente în temeiul Regulamentului (UE) 2022/2554 pot participa la activitățile Grupului de cooperare în conformitate cu articolul 47 alineatul (1) din regulamentul respectiv.	Art. 40 alin. (2) lit. a) Art. 42	Art. 40 (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, acolo unde este	

			cazul, cu Comisia Europeană, ENISA, Grupul de cooperare și Rețeaua CSIRT; 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.	
	După caz, Grupul de cooperare poate invita să participe la lucrările sale Parlamentul European și reprezentanți ai părților interesate relevante.			Nu este necesara transpunerea. Prezenta prevedere face referire la funcționarea Grupului de Cooperare.
	Comisia asigură secretariatul.			Nu este necesara transpunerea. Prezenta prevedere face referire la funcționarea Grupului de Cooperare fiind o obligație a Comisiei Europene.
	(4) Grupului de cooperare îi revin următoarele sarcini: a) furnizarea de orientări autorităților competente în legătură cu transpunerea și punerea în aplicare a prezentei directive;			Nu este necesara transpunerea. Prezenta prevedere face referire la funcționarea Grupului de Cooperare fiind o obligație a Comisiei Europene.
	b) furnizarea de orientări autorităților competente în legătură cu elaborarea și punerea în aplicare a politicilor privind divulgarea coordonată a vulnerabilităților, astfel cum se menționează la articolul 7 alineatul (2) litera (c);			
	c) schimbul de bune practici și de informații în legătură cu punerea în aplicare a prezentei directive, inclusiv în ceea ce privește amenințările cibernetice, incidentele, vulnerabilitățile, incidentele evitate la limită, inițiativele de sensibilizare, cursurile de formare, exercițiile și competențele, consolidarea capacităților, standardele și specificațiile tehnice, precum și identificarea entităților esențiale și a entităților importante			

	în temeiul articolului 2 alineatul (2) literele (b)-(e);			
	d) schimbul de opinii şi cooperarea cu Comisia cu privire la iniţiativele emergente de politică în materie de securitate cibernetică, precum şi coerenţa generală a cerinţelor de securitate cibernetică specifice fiecărui sector;			
	e) schimbul de opinii şi cooperarea cu Comisia cu privire la proiectele de acte delegate sau de punere în aplicare adoptate în temeiul prezentei directive			
	f) schimbul de bune practici şi de informaţii cu instituţiile, organele, oficiile şi agenţiile relevante ale Uniunii;			
	g) schimbul de opinii cu privire la punerea în aplicare a actelor juridice sectoriale ale Uniunii care conţin dispoziţii privind securitatea cibernetică;			
	h) atunci când este cazul, discutarea rapoartelor privind evaluarea inter pares menţionate la articolul 19 alineatul (9) şi stabilirea de concluzii şi recomandări;			
	i) efectuarea unor evaluări coordonate ale riscurilor de securitate la nivelul lanţurilor de aprovizionare critice, în conformitate cu articolul 22 alineatul (1);			
	j) discutarea cazurilor de asistenţă reciprocă, inclusiv a experienţelor şi rezultatelor acţiunilor comune de supraveghere transfrontaliere, astfel cum se menţionează la articolul 37;			
	k) la cererea unuia sau a mai multor state membre în cauză, discutarea cererilor specifice de asistenţă reciprocă astfel cum se menţionează la articolul 37;			
	l) furnizarea de orientări strategice reţelei CSIRT şi EU-CyCLONe cu privire la aspecte emergente specifice;			
	m) schimbul de opinii cu privire la politica privind acţiunile ulterioare incidentelor de securitate cibernetică de mare amploare şi			

	crizelor, pe baza lecțiilor învățate din rețeaua CSIRT și EU-CyCLONe;			
	n) contribuția la capacitățile în materie de securitate cibernetică în întreaga Uniune prin facilitarea schimbului de funcționari naționali prin intermediul unui program de consolidare a capacităților care implică personal din cadrul autorităților competente sau al echipelor CSIRT;			
	o) organizarea de reuniuni comune periodice cu părțile interesate relevante din sectorul privat din întreaga Uniune pentru a discuta activitățile pe care le desfășoară Grupul de cooperare și pentru a colecta informații cu privire la provocările emergente în materie de politici;			
	p) discutarea activității desfășurate în legătură cu exercițiile de securitate cibernetică, inclusiv a activității desfășurate de ENISA;			
	q) stabilirea metodologiei și a aspectelor organizatorice ale evaluărilor inter pares menționate la articolul 19 alineatul (1), precum și definirea metodologiei de autoevaluare pentru statele membre în conformitate cu articolul 19 alineatul (5), cu sprijinul Comisiei și al ENISA, și, în cooperare cu Comisia și cu ENISA, elaborarea codurilor de conduită care să stea la baza metodelor de lucru ale experților în materie de securitate cibernetică desemnați în conformitate cu articolul 19 alineatul (6)			
	r) pregătirea de rapoarte în scopul revizuirii menționate la articolul 40 privind experiența obținută la nivel strategic și din evaluările inter pares;			
	s) discutarea și efectuarea periodică a unei evaluări a situației amenințărilor sau incidentelor cibernetice, cum ar fi ransomware.			
	Grupul de cooperare prezintă rapoartele menționate la primul paragraf litera (r) Comisiei, Parlamentului European și Consiliului.			Nu este necesara transpunerea. Prezenta prevedere face referire la funcționarea Grupului de Cooperare fiind o obligație în sarcina acestuia.

	(5) Statele membre asigură cooperarea eficace, eficientă şi sigură a reprezentanţilor lor în Grupul de cooperare.	Art. 25 alin. (1) lit. e)	Art. 25 - (1) DNSC, în exercitarea calităţii de autoritate competentă responsabilă cu securitatea cibernetică şi cu sarcinile de supraveghere şi asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică, are următoarele atribuţii: (...) e) participă, prin reprezentanţi, la formatele de cooperare la nivel european;	
	(6) Grupul de cooperare poate solicita reţelei CSIRT un raport tehnic pe anumite teme.			Nu este necesara transpunerea. Prezenta prevedere face referire la funcţionarea Grupului de Cooperare fiind o obligaţie în sarcina acestuia.
	(7) Până la 1 februarie 2024 şi, ulterior, o dată la doi ani, Grupul de cooperare stabileşte un program de lucru cu privire la acţiunile care urmează să fie întreprinse pentru punerea în aplicare a obiectivelor şi a sarcinilor sale.			Nu este necesara transpunerea. Prezenta prevedere face referire la funcţionarea Grupului de Cooperare fiind o obligaţie în sarcina acestuia.
	(8) Comisia poate adopta acte de punere în aplicare prin care se stabilesc acordurile procedurale necesare pentru funcţionarea Grupului de cooperare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 39 alineatul (2). Comisia face schimb de opinii şi cooperează cu Grupul de cooperare în ceea ce priveşte proiectele de acte de punere în aplicare menţionate la primul paragraf de la prezentul alineat, în conformitate cu alineatul (4) litera (e).			Nu este necesara transpunerea. Prevedere ce abilitează Comisia să adopte acte de punere în aplicare.
	(9) Grupul de cooperare se reuneşte periodic, şi în toate cazurile cel puţin o dată pe an, cu Grupul privind reziliența entităţilor critice instituit în temeiul Directivei (UE) 2022/2557 pentru a promova şi facilita cooperarea strategică şi schimbul de informaţii.			Prevedere referitoare la funcţionarea Grupului de cooperare, care nu necesită transpunere.

Art. 15	(1) Pentru a contribui la dezvoltarea încrederii şi pentru a promova cooperarea operaţională rapidă şi eficace între statele membre, se stabileşte o reţea a echipelor naţionale CSIRT.			Nu este necesară transpunerea.
	(2) Reţeaua echipelor CSIRT este formată din reprezentanţi ai echipelor CSIRT desemnate sau instituite în temeiul articolului 10 şi din Centrul de răspuns la incidente de securitate cibernetică pentru instituţiile, organele şi agenţiile Uniunii (CERT-UE). Comisia participă la reţeaua CSIRT în calitate de observator. ENISA asigură secretariatul şi acordă asistenţă în mod activ pentru cooperarea între echipele CSIRT	Art. 24 alin. (2) Art. 41 alin. (1)	Art. 24 (2) DNSC îndeplineşte funcţia de echipă de răspuns la incidente de securitate cibernetică naţională, denumită în continuare „CSIRT naţional", în temeiul dispoziţiilor OUG nr. 104/2021 privind Înfiinţarea Directoratului Naţional de Securitate Cibernetică. Art. 41 (1) DNSC, în calitate de CSIRT naţional, participă la Reţeaua CSIRT în scop operaţional.	
	(3) Reţelei CSIRT îi revin următoarele sarcini:			Nu este necesară transpunerea.
	a) schimbul de informaţii privind capacităţile echipelor CSIRT			
	b) facilitarea partajării, transferului şi schimbului de tehnologie şi măsuri, politici, instrumente, procese, bune practici şi cadre relevante între echipele CSIRT			
	c) schimbul de informaţii relevante privind incidentele, incidentele evitate la limită, ameninţările cibernetice, riscurile şi vulnerabilităţile			
	d) schimbul de informaţii în ceea ce priveşte publicaţiile şi recomandările în materie de securitate cibernetică;			

	e) asigurarea interoperabilității în ceea ce privește specificațiile și protocoalele referitoare la schimbul de informații;			
	f) la cererea unui membru al rețelei CSIRT care ar putea fi afectat de un incident, schimbul de informații și discutarea informațiilor cu privire la incidentul respectiv și la amenințările cibernetice, riscurile și vulnerabilitățile conexe;			
	g) la cererea unui membru al rețelei CSIRT, discutarea și, după caz, punerea în aplicare a unui răspuns coordonat la un incident care a fost identificat în jurisdicția statului membru respectiv			
	h) furnizarea de asistență statelor membre în abordarea incidentelor transfrontaliere în temeiul prezentei directive;			
	i) cooperarea, schimbul de bune practici și furnizarea de asistență echipelor CSIRT desemnate drept coordonatori în temeiul articolului 12 alineatul (1) în ceea ce privește gestionarea divulgării coordonate a vulnerabilităților care ar putea avea un impact semnificativ asupra entităților din mai multe state membre;			
	j) discutarea și identificarea de noi forme de cooperare operațională, inclusiv în legătură cu: i. categoriile de amenințări cibernetice și incidente; ii. alertele timpurii; iii. asistența reciprocă; iv. principiile și modalitățile de coordonare, ca răspuns la riscuri și incidente transfrontaliere; v. contribuția la planul național de răspuns la incidente de securitate cibernetică de mare amploare și crize menționat la articolul 9 alineatul (4), la solicitarea unui stat membru;			
	k) informarea Grupului de cooperare cu privire la activitățile sale și cu privire la noi forme de cooperare operațională discutate în			

	temeiul literei (j) şi, după caz, solicitarea de orientări în acest sens;			
	l) bilanţul exerciţiilor de securitate cibernetică, inclusiv al celor organizate de ENISA			
	m) la cererea unei anumite echipe CSIRT, discutarea capacităţilor şi a nivelului de pregătire al echipei CSIRT respective;			
	n) cooperarea şi schimbul de informaţii cu centrele de operaţiuni de securitate la nivel regional şi la nivelul Uniunii pentru a îmbunătăţi conştientizarea comună a situaţiei cu privire la incidentele şi ameninţările cibernetice din întreaga Uniune;			
	o) atunci când este cazul, discutarea rapoartelor privind evaluarea inter pares menţionate la articolul 19 alineatul (9)			
	p) oferirea de orientări pentru a facilita convergenţa practicilor operaţionale în ceea ce priveşte aplicarea dispoziţiilor prezentului articol referitoare la cooperarea operaţională			
	(4) Până la 17 ianuarie 2025 şi, ulterior, o dată la doi ani, reţeaua CSIRT evaluează, în scopul revizuirii menţionate la articolul 40, progresele înregistrate în ceea ce priveşte cooperarea operaţională şi adoptă un raport. Raportul formulează, în special, concluzii şi recomandări pe baza rezultatelor evaluărilor inter pares menţionate la articolul 19, care sunt efectuate în legătură cu echipele naţionale CSIRT. Raportul respectiv se transmite Grupului de cooperare.			Nu este necesară transpunerea. Prevedere ce se aplică reţelei CSIRT. DNSC în calitate de membru al reţelei, prin echipa sa CSIRT va contribui la îndeplinirea acestor cerinţe
	(5) Reţeaua CSIRT îşi adoptă regulamentul de procedură.			Prevedere ce nu necesită transpunere.
	(6) Reţeaua CSIRT şi EU-CyCLONe convin asupra modalităţilor procedurale şi cooperează pe baza acestora.			Nu este necesară transpunerea. Prevedere în sarcina reţelei CSIRT şi EU-CyCLONe.
Art. 16	(1) EU-CyCLONe este instituită pentru a sprijini gestionarea coordonată, la nivel operaţional, a incidentelor de securitate cibernetică de mare amploare şi a crizelor şi pentru a asigura schimbul periodic de informaţii relevante între statele membre şi instituţiile, organele, oficiile şi agenţiile Uniunii.			Nu este necesară transpunerea.

	(2) EU-CyCLONe este compusă din reprezentanți ai autorităților de gestionare a crizelor cibernetice din statele membre, precum și, în cazurile în care un incident de securitate cibernetică de mare amploare potențial sau în curs de desfășurare are sau este probabil să aibă un impact semnificativ asupra serviciilor și activităților care intră în domeniul de aplicare al prezentei directive, reprezentanți ai Comisiei. În celelalte cazuri, Comisia participă la activitățile EU-CyCLONe în calitate de observator	Art. 28 alin. (1) Art. 29 alin. (4) Art. 43	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. Art. 29 (4) În termen de trei luni de la intrarea în vigoare a prezentei ordonanțe de urgență, punctul unic de contact național notifică Comisiei Europene și EU-CyCLONe calitatea DNSC de autoritate națională de gestionare a crizelor cibernetice, precum și orice modificări ulterioare ale acestei calități. 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.	
	ENISA asigură secretariatul EU-CyCLONe și sprijină schimbul securizat de informații și, de asemenea, furnizează instrumentele necesare pentru sprijinirea cooperării dintre statele			Prevedere ce stabilește o obligație pentru ENISA, care nu necesită transpunere

	membre, asigurând schimbul securizat de informații.			
	După caz, EU-CyCLONe poate invita să participe la lucrările sale, în calitate de observatori, reprezentanți ai părților interesate relevante			Prevedere referitoare la funcționarea EU-CyCLONe, care nu necesită transpunere
	(3) EU-CyCLONe are următoarele sarcini:			Nu este necesară transpunerea.
	a) consolidarea nivelului de pregătire pentru gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor;			
	b) dezvoltarea unei conștientizări comune a situației în cazul incidentelor de securitate cibernetică de mare amploare și al crizelor;			
	c) evaluarea consecințelor și a impactului incidentelor de securitate cibernetică de mare amploare și crizelor relevante și propunerea unor posibile măsuri de atenuare;			
	d) coordonarea gestionării incidentelor de securitate cibernetică de mare amploare și a crizelor și sprijinirea procesului decizional la nivel politic în legătură cu astfel de incidente și crize;			
	e) discutarea, la solicitarea unui stat membru în cauză, a planurilor naționale de răspuns la incidente de securitate cibernetică de mare amploare și crize menționate la articolul 9 alineatul (4).			
	(4) EU-CyCLONe își adoptă regulamentul de procedură.			Prevedere în sarcina EU-CyCLONe, care nu necesită transpunere.
	(5) EU-CyCLONe prezintă periodic rapoarte Grupului de cooperare cu privire la gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor, precum și la tendințe, concentrându-se în special pe impactul acestora asupra entităților esențiale și a entităților importante.			Prevedere în sarcina EU-CyCLONe, care nu necesită transpunere.
	(6) EU-CyCLONe cooperează cu rețeaua CSIRT pe baza modalităților procedurale convenite prevăzute la articolul 15 alineatul (6).			Prevedere în sarcina EU-CyCLONe, care nu necesită transpunere.
	(7) Până la 17 iulie 2024 și, ulterior, la fiecare 18 luni, EU-CyCLONe prezintă un raport			Prevedere în sarcina EU-CyCLONe, care nu necesită transpunere.

	Parlamentului European şi Consiliului în care îşi evaluează activitatea.			
Art. 17	După caz, Uniunea poate să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaţionale cu ţări terţe sau organizaţii internaţionale, care să permită şi să organizeze participarea acestora la anumite activităţi ale Grupului de cooperare, ale reţelei CSIRT, precum şi ale EU-CyCLONe. Aceste acorduri respectă dreptul Uniunii în materie de protecţie a datelor.			Nu este necesară transpunerea. Prevedere privind funcţionarea Grupului de Coopereare, reţelei CSIRT şi EU-CyCLONe
Art. 18	(1) ENISA adoptă, în cooperare cu Comisia şi Grupul de cooperare, un raport bienal privind situaţia în materie de securitate cibernetică în Uniune şi înaintează şi prezintă respectivul raport Parlamentului European. Raportul este, printre altele, pus la dispoziţie într-un format citibil automat şi include următoarele: a) o evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, ţinând seama de situaţia ameninţărilor cibernetice; b) o evaluare a dezvoltării capacităţilor în materie de securitate cibernetică în sectorul public şi cel privat în întreaga Uniune; c) o evaluare a nivelului general de sensibilizare cu privire la securitatea cibernetică şi igiena cibernetică în rândul cetăţenilor şi entităţilor, inclusiv al întreprinderilor mici şi mijlocii; d) o evaluare globală a rezultatelor evaluărilor inter pares menţionate la articolul 19; e) o evaluare globală a nivelului de maturitate a capacităţilor şi a resurselor în materie de securitate cibernetică în întreaga Uniune, inclusiv a celor de la nivel sectorial, precum şi a gradului de aliniere a strategiilor naţionale de securitate cibernetică ale statelor membre. (2) Raportul include recomandări de politică specifice pentru a aborda deficienţele şi a îmbunătăţi nivelul de securitate cibernetică în			Nu este necesara transpunerea. Prevedere în sarcina ENISA, a Grupului de cooperare şi a Comisiei.

	întreaga Uniune şi un rezumat al constatărilor pentru perioada respectivă incluse în rapoartele UE privind situaţia tehnică în materie de securitate cibernetică cu privire la incidente şi ameninţări cibernetice, pregătite de ENISA în conformitate cu articolul 7 alineatul (6) din Regulamentul (UE) 2019/881. (3) ENISA, în cooperare cu Comisia, Grupul de cooperare şi reţeaua CSIRT, elaborează metodologia, inclusiv variabilele relevante, cum ar fi indicatori cantitativi şi calitativi, pentru evaluarea globală menţionată la alineatul (1) litera (e).			
Art. 19	(1) Grupul de cooperare stabileşte, până la 17 ianuarie 2025, cu sprijinul Comisiei şi al ENISA şi, după caz, al reţelei CSIRT, metodologia şi aspectele organizatorice ale evaluărilor inter pares pentru a învăţa din experienţele comune, a consolida încrederea reciprocă, a atinge un nivel comun ridicat de securitate cibernetică, precum şi a consolida capacităţile şi politicile de securitate cibernetică ale statelor membre necesare pentru punerea în aplicare a prezentei directive. Participarea la evaluările inter pares se face pe bază voluntară. Evaluările inter pares sunt efectuate de experţi în materie de securitate cibernetică. Experţii în materie de securitate cibernetică sunt desemnaţi de cel puţin două state membre, diferite de statul membru care face obiectul evaluării. Evaluările inter pares acoperă cel puţin unul din următoarele elemente: a) nivelul punerii în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică şi a obligaţiilor de raportare menţionate la articolele 21 şi 23; b) nivelul capacităţilor, inclusiv resursele financiare, tehnice şi umane disponibile, precum şi eficacitatea exercitării sarcinilor autorităţilor competente; c) capacităţile operaţionale ale echipelor CSIRT;			Nu este necesară transpunerea art. 19 alin. (1) teza 1 – obligaţie ce revine Grupului de cooperare, cu sprijinul Comisiei şi al ENISA şi, după caz, al Reţelei CSIRT.

	d) nivelul de punere în aplicare a asistenței reciproce menționate la articolul 37; e) nivelul de punere în aplicare a acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la articolul 29 f) aspecte specifice de natură transfrontalieră sau transsectorială. (2) Metodologia menționată la alineatul (1) include criterii obiective, nediscriminatorii, echitabile și transparente pe baza cărora statele membre desemnează experți în domeniul securității cibernetice eligibili pentru efectuarea evaluărilor inter pares. ENISA și Comisia participă în calitate de observatori la evaluările inter pares (3) Statele membre pot identifica aspecte specifice, astfel cum sunt menționate la alineatul (1) litera (f), pentru o evaluare inter pares (4) Înainte de a începe o evaluare inter pares, astfel cum este menționată la alineatul (1), statele membre informează statele membre participante cu privire la domeniul de aplicare al acesteia, inclusiv aspectele specifice identificate în temeiul alineatului (3). (5) Înainte de începerea evaluării inter pares, statele membre pot efectua o autoevaluare a aspectelor analizate și furniza autoevaluarea respectivă experților în materie de securitate cibernetică desemnați. Grupul de cooperare, cu sprijinul Comisiei și al ENISA, stabilește metodologia pentru autoevaluarea statelor membre. (6) Evaluările inter pares implică vizite fizice sau virtuale și schimburi de informații ex situ. În conformitate cu principiul bunei cooperări, statul membru supus evaluării inter pares le furnizează experților în materie de securitate cibernetică desemnați informațiile necesare pentru evaluare, fără a aduce atingere dreptului Uniunii sau dreptului intern privind protecția informațiilor confidențiale sau clasificate și protejării funcțiilor esențiale ale statului, cum ar fi			

	securitatea națională. Grupul de cooperare, în colaborare cu Comisia și ENISA, elaborează coduri de conduită adecvate care stau la baza metodelor de lucru ale experților în materie de securitate cibernetică desemnați. Orice informație obținută prin intermediul evaluării inter pares este utilizată exclusiv în acest scop. Experții în materie de securitate cibernetică care participă la evaluarea inter pares nu divulgă terților nicio informație sensibilă sau confidențială obținută în cursul evaluării inter pares respective. (7) Odată ce au făcut obiectul unei evaluări inter pares, aceleași aspecte evaluate într-un stat membru nu fac obiectul unei noi evaluări inter pares în statul membru respectiv timp de doi ani de la încheierea evaluării inter pares, cu excepția cazului în care statul membru decide altfel sau se convine astfel la propunerea Grupului de cooperare. (8) Statele membre 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. Statul membru supus evaluării inter pares se poate opune desemnării anumitor experți în materie de securitate cibernetică din motive justificate corespunzător, comunicate statului membru care i-a desemnat. (9) Experții în materie de securitate cibernetică care participă la evaluări inter pares elaborează rapoarte cu privire la constatările și concluziile evaluărilor inter pares. Statele membre care fac obiectul unei evaluări inter pares pot prezenta observații cu privire la proiectele de rapoarte care le privesc, iar aceste observații se anexează la rapoarte. Rapoartele includ recomandări care să faciliteze îmbunătățirea aspectelor acoperite de evaluarea inter pares. Rapoartele sunt transmise Grupului de cooperare și rețelei CSIRT atunci când este cazul. Un stat membru			

	care face obiectul unei evaluări inter pares poate decide să pună la dispoziția publicului raportul său sau o versiune ocultată a acestuia.			
Art. 20	(1) Statele membre se asigură că organele de conducere ale entităților esențiale și ale entităților importante aprobă măsurile de gestionare a riscurilor în materie de securitate cibernetică luate de entitățile respective pentru a se conforma articolului 21, supraveghează punerea în aplicare a acestuia și pot fi trase la răspundere pentru încălcarea de către entități a respectivului articol. Aplicarea prezentului alineat nu aduce atingere dreptului intern în ceea ce privește normele referitoare la răspundere aplicabile instituțiilor publice, precum și răspunderea funcționarilor publici și a funcționarilor aleși sau numiți.	Art. 14 alin. (1)	(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 și, după caz, a dispozițiilor ordinului prevăzut la art. 37 alin. (8) lit. b), 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) Statele membre se asigură că membrii organelor de conducere din cadrul entităților esențiale și al entităților importante au obligația de a urma o formare pentru a dobândi suficiente cunoștințe și competențe pentru a putea identifica riscurile și a evalua practicile de gestionare a riscurilor în materie de securitate cibernetică și impactul acestora asupra serviciilor pe care le furnizează entitatea, și încurajează entitățile esențiale și entitățile importante să ofere o formare similară tuturor angajaților în mod regulat.	Art. 14 alin. (2)	(2) Membrii organelor de conducere ale entităților esențiale și ale entităților importante urmează cursuri de formare profesională acreditate 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. Entitățile esențiale și importante asigură formarea profesională întregului personal în vederea asigurării unui nivel suficient de cunoștințe și competențe.	
Art. 21	(1) Statele membre se asigură că entitățile esențiale și entitățile importante iau măsuri tehnice, operaționale și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care entitățile respective le utilizează pentru operațiunile lor sau pentru a furniza servicii și pentru a preveni sau reduce la minimum impactul incidentelor asupra	Art. 11 alin. (1)	(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,	

	beneficiarilor serviciilor lor şi asupra altor servicii.		precum şi pentru a elimina sau, după caz, a reduce la minim efectele incidentelor asupra destinatarilor serviciilor lor şi asupra altor servicii.	
	Ţinând seama de cele mai avansate standarde în domeniu şi, atunci când este cazul, de standardele europene şi internaţionale relevante, precum şi de costul punerii în aplicare, măsurile menţionate la primul paragraf asigură un nivel de securitate a reţelelor şi a sistemelor informatice corespunzător riscurilor prezentate. Atunci când se evaluează proporţionalitatea acestor măsuri, se ţine seama în mod corespunzător de gradul de expunere a entităţii la riscuri, de dimensiunea entităţii şi de probabilitatea producerii incidentelor, precum şi de gravitatea acestora, inclusiv de impactul lor societal şi economic.	Art. 9 Art. 10 alin. (1) şi (2) Art. 11 alin. (1) (2), (3) şi (10)	Art. 9 O entitate este considerată esenţială sau importantă, dacă: a) entitatea este singurul furnizor al unui serviciu care este esenţial pentru susţinerea unor activităţi societale şi economice critice; b) perturbarea serviciului furnizat de entitate ar putea avea un impact semnificativ asupra siguranţei publice, a securităţii publice sau a sănătăţii 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 importanţei sale specifice la nivel naţional 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 funcţie de: a) impactul asupra drepturilor şi libertăţilor fundamentale; b) impactul asupra economiei naţionale; c) impactul asupra sănătăţii şi vieţii persoanelor; d) impactul financiar; e) impactul asupra apărării, ordinii publice şi securităţii naţionale;	

			f) impactul trans-sectorial sau transfrontalier. (2) Criteriile prevăzute la alin. (1), pragurile corespunzătoare acestora şi metodologia de evaluare a nivelului de risc al entităţilor se stabilesc prin ordin al Directorului DNSC. Art. 11 (1) Entităţile esenţiale şi entităţile importante iau măsuri tehnice, operaţionale şi organizatorice proporţionale şi adecvate pentru a identifica, evalua şi gestiona riscurile aferente securităţii reţelelor şi a sistemelor informatice pe care acestea le utilizează în desfăşurarea activităţilor lor sau furnizarea serviciilor lor, precum şi pentru a elimina sau, după caz, a reduce efectele incidentelor asupra destinatarilor serviciilor lor şi asupra altor servicii. (2) Măsurile prevăzute la alin. (1) trebuie să asigure un nivel de securitate cibernetică adecvat nivelului de risc al entităţii, ţinând seama de stadiul actual al tehnologiei şi, după caz, de cele mai relevante standarde şi bune practici naţionale, europene şi internaţionale, cât şi de costurile de punere în aplicare a acestor măsuri. (3) Nivelul de risc al entităţii se evaluează conform metodologiei de evaluare a nivelului de risc cuprinse în ordinul Directorului DNSC prevăzut la art. 10 alin. (2). (10) Atunci când este evaluată proporţionalitatea măsurilor de gestionare a riscurilor în conformitate cu alin. (1), se ţine seama în mod corespunzător de amploarea expunerii la riscuri a entităţii şi 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.	
	(2) Măsurile menționate la alineatul (1) se bazează pe o abordare multirisc care vizează protejarea rețelelor și a sistemelor informatice, precum și a mediului fizic al acestor sisteme împotriva incidentelor, și includ cel puțin următoarele:	Art. 11 alin. (4) Art. 12 alin. (1) si (2) Art. 13	Art. 11 (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. 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) Fără a aduce atingere dispozițiilor art. 37 alin. (8) lit. b) și alin. (17), 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. Art. 13 Măsurile prevăzute la art. 11 alin. (1) cuprind cel puțin următoarele:	
	a) politici referitoare la analiza riscurilor și securitatea sistemelor informatice	Art. 13 lit. a)	a) politicile și procedurile referitoare la analiza riscurilor și la securitatea sistemelor informatice și revizuirea periodică a acestora;	
	b) gestionarea incidentelor;	Art. 13 lit. g)	g) gestionarea incidentelor;	

	c) continuitatea activității, de exemplu gestionarea copiilor de rezervă și recuperarea în caz de dezastru, precum și gestionarea crizelor	Art. 13 lit. h)	h) continuitatea activității, inclusiv gestionarea copiilor de rezervă, redresarea în caz de dezastru și managementul crizelor;	
	d) securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile dintre fiecare entitate și prestatorii sau furnizorii săi direcți de servicii;	Art. 13 lit. d)	d) securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitatea relației dintre entitate și prestatorii și furnizorii săi direcți;	
	e) securitatea în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice, inclusiv gestionarea vulnerabilităților și divulgarea acestora;	Art. 13 lit. e)	e) securitatea achiziției, dezvoltării, întreținerii și casării rețelelor și sistemelor informatice, inclusiv gestionarea și divulgarea vulnerabilităților;	
	f) politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor în materie de securitate cibernetică;	Art. 13 lit. b)	b) politicile și procedurile de evaluare a eficacității măsurilor de gestionare a riscurilor de securitate cibernetică;	
	g) practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice;	Art. 13 lit. i)	i) practicile de bază în materie de igienă cibernetică și formarea în domeniul securității cibernetice;	
	h) politici și proceduri privind utilizarea criptografiei și, după caz, a criptării	Art. 13 lit. c)	c) politicile și procedurile referitoare la utilizarea criptografiei și, după caz, a criptării;	
	i) securitatea resurselor umane, politicile de control al accesului și gestionarea activelor;	Art. 13 lit. f)	f) securitatea resurselor umane, politicile de control al accesului și gestionarea activelor;	
	j) utilizarea de soluții de autentificare multifactor sau de autentificare continuă, de comunicații securizate voce, video și text și de sisteme securizate de comunicații de urgență în cadrul entității, după caz	Art. 13 lit. j)	j) utilizarea, în interiorul entității, a soluțiilor de autentificare multi-factor sau de autentificare continuă, a comunicațiilor securizate vocale, video și text și a sistemelor de comunicații de urgență securizate, după caz.	
	(3) Statele membre se asigură că, atunci când analizează care măsuri menționate la alineatul (2) litera (d) de la prezentul articol sunt adecvate, entitățile iau în considerare vulnerabilitățile specifice fiecărui prestator și furnizor direct de servicii, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale prestatorilor și furnizorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare. Statele membre se asigură, de asemenea, că, atunci când analizează	Art. 11 alin. (8)	(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;	

	care măsuri menționate la litera respectivă sunt adecvate, entitățile au obligația de a ține seama de rezultatele evaluărilor coordonate ale riscurilor de securitate la nivelul lanțurilor de aprovizionare critice efectuate în conformitate cu articolul 22 alineatul (1)		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.	
	(4) Statele membre se asigură că o entitate care constată că nu respectă măsurile prevăzute la alineatul (2) ia, fără întârzieri nejustificate, toate măsurile corective necesare, adecvate și proporționale.	Art. 12 alin. (3)	(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) sau, după caz, pe cele prevăzute în ordinul de la art. 37 alin. (8) lit. b), acestea aplică, fără întârzieri nejustificate, măsurile corective necesare.	
	(5) Până la 17 octombrie 2024, Comisia adoptă acte de punere în aplicare de stabilire a cerințelor tehnice și metodologice ale măsurilor menționate la alineatul (2) în ceea ce privește furnizorii de servicii DNS, registrele de nume TLD, 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, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere. Comisia poate adopta acte de punere în aplicare de stabilire a cerințelor tehnice și metodologice, precum și a cerințelor sectoriale, după caz, ale măsurilor menționate la alineatul (2) în ceea ce privește entitățile esențiale și entitățile importante, altele decât cele menționate la primul paragraf de la prezentul alineat. Atunci când pregătește actele de punere în aplicare menționate la primul și al doilea paragraf de la prezentul alineat, Comisia urmează, în cea mai mare măsură posibilă, standardele europene și internaționale, precum și specificațiile tehnice relevante. Comisia face			Nu este necesara transpunerea. Prevedere ce abilitează Comisia să adopte acte de punere în aplicare.

	schimb de opinii şi cooperează cu Grupul de cooperare şi ENISA privind proiectele de acte de punere în aplicare, în conformitate cu articolul 14 alineatul (4) litera (e). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 39 alineatul (2).			
Art. 22	(1) Grupul de cooperare, în cooperare cu Comisia şi ENISA, poate efectua evaluări coordonate ale riscurilor în materie de securitate ale anumitor servicii TIC, sisteme TIC sau lanţuri de aprovizionare cu produse TIC critice, ţinând seama de factorii de risc de natură tehnică şi, după caz, care nu sunt de natură tehnică. (2) Comisia, după consultarea Grupului de cooperare şi a ENISA şi, atunci când este necesar, a părţilor interesate relevante, identifică serviciile TIC, sistemele TIC sau produsele TIC critice specifice care pot face obiectul evaluării coordonate a riscurilor de securitate menţionate la alineatul (1)			Nu este necesară transpunerea. Vizează posibilitatea Grupului de coordonare, a Comisiei şi a ENISA de a efectua evaluări coordonate ale riscurilor în materie de securitate cibernetică.
Art. 23	(1) Fiecare stat membru se asigură că entităţile esenţiale şi entităţile importante notifică, fără întârzieri nejustificate, echipei CSIRT sau, după caz, autorităţii sale competente, în conformitate cu alineatul (4), orice incident care are un impact semnificativ asupra prestării serviciilor lor, astfel cum se menţionează la alineatul (3) (incident semnificativ). Dacă este cazul, entităţile în cauză notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor incidentele semnificative care ar putea afecta în mod negativ prestarea serviciilor respective. Fiecare stat membru se asigură că entităţile respective raportează, inter alia, orice informaţie care îi permite echipei CSIRT sau, după caz, autorităţii competente să constate orice impact transfrontalier al incidentului. Simpla notificare nu expune entitatea notificatoare unei răspunderi sporite.	Art. 15 alin. (1) si (3)	(1) Entităţile esenţiale şi entităţile importante raportează, fără întârzieri nejustificate, echipei de răspuns la incidente de securitate cibernetică naţionale orice incident care are un impact semnificativ asupra prestării serviciilor lor (incident semnificativ) şi, dacă este cazul, entităţile în cauză notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor, incidentele semnificative care ar putea afecta prestarea serviciilor respective. (3) Entităţile esenţiale şi entităţile importante raportează orice informaţie care îi permite echipei de răspuns la incidente de securitate cibernetică naţionale să constate un impact transfrontalier al incidentului. Simpla raportare nu expune entitatea unei răspunderi sporite.	

	În cazul în care entitățile în cauză notifică autorității competente un incident semnificativ în temeiul primului paragraf, statul membru se asigură că autoritatea competentă înaintează notificarea echipei CSIRT la primirea acesteia.	Art. 15 alin. (2)	(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.	În cadrul DNSC funcționează CSIRT național, care asigura si calitatea de autoritate competenta in sensul art. 8 din directiva, iar raportarea se face prin PNRISC, care este administrată de către DNSC conform Legii 58/2023
	În cazul unui incident semnificativ transfrontalier sau transsectorial, statele membre se asigură că punctele lor unice de contact primesc în timp util informațiile relevante notificate în conformitate cu alineatul (4).	Art. 15 alin. (4)	(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).	În cadrul DNSC funcționează punctul national de contact si CSIRT național
	(2) Dacă este cazul, statele membre se asigură că 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. Dacă este cazul, entitățile informează, de asemenea, destinatarii în cauză despre amenințarea semnificativă propriu-zisă.	Art. 15 alin. (5)	(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.	
	(3) Un incident este considerat semnificativ dacă:	Art. 15 alin. (6)	(6) Un incident este considerat semnificativ sau impactul unui incident este considerat semnificativ dacă:	
	a) a provocat sau poate provoca perturbări operaționale grave ale serviciilor sau pierderi financiare pentru entitatea în cauză;	Art. 15 alin. (6) lit. a)	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 morale considerabile.	Art. 15 alin. (6) lit. b)	b) a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau non-materiale considerabile.	
	(4) Statele membre se asigură că, în scopul notificării în temeiul alineatului (1), entitățile în cauză transmit echipei CSIRT sau, după caz, autorității competente:	Art. 15 alin. (7)	(7) În scopul notificării în temeiul alin. (1), entitățile în cauză transmit echipei de răspuns la incidente de securitate cibernetică naționale:	

	a) fără întârzieri nejustificate şi, în orice caz, în termen de 24 de ore de la data la care au luat cunoştinţă de incidentul semnificativ, o avertizare timpurie care, după caz, indică dacă există suspiciuni că incidentul semnificativ este cauzat de acţiuni ilegale sau răuvoitoare sau ar putea avea un impact transfrontalier;	Art. 15 alin. (7) lit. a)	a) fără întârzieri nejustificate şi, în orice caz, în termen de 24 de ore de la data la care au luat cunoştinţă de incidentul semnificativ, o avertizare timpurie care, după caz, indică dacă există suspiciuni că incidentul este cauzat de acţiuni ilicite sau răuvoitoare sau că ar putea avea un impact transfrontalier;	
	b) fără întârzieri nejustificate şi, în orice caz, în termen de 72 de ore din momentul în care au luat cunoştinţă de incidentul semnificativ, o notificare a incidentului, care, după caz, actualizează informaţiile menţionate la litera (a) şi prezintă o evaluare iniţială a incidentului semnificativ, inclusiv a gravităţii şi a impactului acestuia, precum şi a indicatorilor de compromitere, dacă sunt disponibili;	Art. 15 alin. (7) lit. b)	b) fără întârzieri nejustificate şi, în orice caz, în termen de 72 de ore din momentul în care au luat cunoştinţă de incidentul semnificativ, o raportare a incidentului, care, după caz, actualizează informaţiile menţionate la lit. a) şi prezintă o evaluare iniţială a incidentului semnificativ, inclusiv a gravităţii şi a impactului acestuia, precum şi a indicatorilor de compromitere, dacă sunt disponibili;	
	c) la cererea unei echipe CSIRT sau, după caz, a autorităţii competente, un raport intermediar privind actualizarea relevantă a situaţiei	Art. 15 alin. (7) lit. c)	c) un raport intermediar privind actualizarea relevantă a situaţiei, la cererea echipei de răspuns la incidente de securitate cibernetică naţionale;	
	d) un raport final, în termen de cel mult o lună de la transmiterea notificării incidentului în temeiul literei (b), care să includă următoarele elemente: i. o descriere detaliată a incidentului, inclusiv a gravităţii şi a impactului acestuia; ii. tipul de ameninţare sau de cauză principală care probabil că a declanşat incidentul; iii. măsurile de atenuare aplicate şi în curs; iv. dacă este cazul, impactul transfrontalier al incidentului;	Art. 15 alin. (7) lit. d)	d) un raport final, în termen de cel mult o lună de la transmiterea notificării incidentului în temeiul lit. b), care să includă cel puţin următoarele elemente: 1. o descriere detaliată a incidentului, inclusiv a gravităţii şi a impactului acestuia; 2. tipul de ameninţare sau de cauză principală care probabil că a declanşat incidentul; 3. măsurile de atenuare aplicate şi în curs; 4. dacă este cazul, impactul transfrontalier al incidentului.	
	e) în cazul unui incident în desfăşurare la momentul prezentării raportului final menţionat la litera (d), statele membre se	Art. 15 alin. (7) lit. e)	e) în cazul unui incident în desfăşurare la momentul prezentării raportului menţionat la lit. d), entităţile în cauză	

	asigură că entitățile în cauză prezintă la momentul respectiv un raport privind progresele înregistrate şi un raport final în termen de o lună de la gestionarea incidentului.		prezintă un raport privind progresele înregistrate şi un raport final în termen de o lună de la gestionarea incidentului.	
	Prin derogare de la primul paragraf litera (b), un prestator de servicii de încredere notifică, în ceea ce priveşte incidentele semnificative care afectează prestarea serviciilor sale de încredere, echipa CSIRT sau, după caz, autoritatea competentă, fără întârzieri nejustificate şi, în orice caz, în termen de 24 de ore de la data la care a luat cunoştinţă de incidentul semnificativ.	Art. 15 alin. (8)	(8) Prin excepție de la alin. (7) lit. b), un prestator de servicii de încredere notifică, în ceea ce priveşte incidentele semnificative care afectează prestarea serviciilor sale de încredere, echipei de răspuns la incidente de securitate cibernetică naționale, fără întârzieri nejustificate şi, în orice caz, în termen de 24 de ore de la data la care a luat cunoştinţă de incidentul semnificativ.	
	(5) Echipa CSIRT sau autoritatea competentă furnizează, fără întârzieri nejustificate şi, atunci când este posibil, în termen de 24 de ore de la primirea alertei timpurii menționate la alineatul (4) litera (a), un răspuns entității notificatoare, inclusiv un feedback inițial cu privire la incidentul semnificativ şi, la cererea entității, orientări sau instrucțiuni operaționale privind punerea în aplicare a unor eventuale măsuri de atenuare. În cazul în care echipa CSIRT nu este destinatarul inițial al notificării menționate la alineatul (1), orientările sunt furnizate de autoritatea competentă în colaborare cu echipa CSIRT. Echipa CSIRT furnizează sprijin tehnic suplimentar în cazul în care entitatea în cauză solicită acest lucru. În cazul în care se suspectează că incidentul este de natură penală, echipa CSIRT sau autoritatea competentă furnizează, de asemenea, orientări privind raportarea incidentului către autoritățile de aplicare a legii.	Art. 15 alin. (9) si (10)	(9) Echipa de răspuns la incidente de securitate cibernetică națională furnizează, fără întârzieri nejustificate şi, 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 şi, 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 furnizează 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 naționale furnizează, de asemenea, orientări privind sesizarea incidentului către organele de urmărire penală.	Este redundantă teza mediană a alin. (5) deoarece dnsc îndeplineşte toate funcțiile ce decurg din directivă (csirt național, spoc, autoritate competentă)
	(6) După caz, şi în special dacă incidentul semnificativ implică două sau mai multe state membre, echipa CSIRT, autoritatea competentă sau punctul unic de contact informează, fără	Art. 15 alin. (11) şi (12)	(11) După caz, şi în special dacă incidentul semnificativ implică două sau mai multe state, DNSC informează, fără întârzieri nejustificate, celelalte	

	întârzieri nejustificate, celelalte state membre afectate şi ENISA cu privire la incidentul semnificativ. Aceste informaţii includ tipul de informaţii primite în conformitate cu alineatul (4). Astfel, echipa CSIRT, autoritatea competentă sau punctul unic de contact, în conformitate cu dreptul Uniunii sau dreptul intern, protejează interesele de securitate şi comerciale ale entităţii, precum şi confidenţialitatea informaţiilor furnizate.		state afectate şi Agenţia Uniunii Europene pentru Securitate Cibernetică, denumită în continuare „ENISA", cu privire la incidentul semnificativ. Aceste informaţii includ tipul de informaţii primite conform alin. (7). (12) În cazul alin. (11), DNSC, în conformitate cu legislaţia naţională şi normele Uniunii Europene, protejează interesele de securitate şi pe cele comerciale ale entităţii, precum informaţiile privilegiate, datele legate de afacere sau cele corporate şi asigură confidenţialitatea informaţiilor furnizate.	
	(7) În cazul în care sensibilizarea 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, echipa CSIRT a unui stat membru sau, după caz, autoritatea sa competentă, şi, după caz, echipele CSIRT sau autorităţile competente din alte state membre în cauză pot, după consultarea entităţii în cauză, să informeze publicul cu privire la incidentul semnificativ sau să solicite entităţii să facă acest lucru.	Art. 15 alin. (13)	(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 autorităţile omoloage din alte state în cauză pot, după consultarea entităţii respective, să informeze publicul cu privire la incidentul semnificativ sau să solicite entităţii să facă acest lucru.	
	(8) La cererea echipei CSIRT sau a autorităţii competente, punctul unic de contact înaintează notificările primite în temeiul alineatului (1) punctelor unice de contact din celelalte state membre afectate.	Art. 15 alin. (14)	(14) Punctul unic de contact naţional, înaintează, după caz, raportările primite conform alin. (1) punctelor unice de contact din celelalte state membre afectate.	
	(9) Punctul unic de contact transmite ENISA o dată la trei luni un raport de sinteză care include date anonimizate şi agregate privind incidentele semnificative, incidentele, ameninţările cibernetice semnificative şi incidentele evitate la limită notificate în conformitate cu alineatul (1) de la prezentul articol şi cu articolul 30. Pentru a contribui la furnizarea de informaţii comparabile, ENISA poate adopta orientări	Art. 15 alin. (15)	(15) Punctul unic de contact naţional transmite către ENISA, o dată la trei luni, un raport de sinteză care include date anonimizate agregate privind incidentele semnificative, incidentele, ameninţările cibernetice şi incidentele evitate la limită raportate conform alin. (1) şi cu cele privind raportarea voluntară.	Nu este necesara transpunerea art. 23 alin. (9) tezele 2 si 3. Prevederi ce abilitează ENISA să adopte orientări tehnice, respectiv obligatii de informare in sarcina ENISA.

	tehnice cu privire la parametrii informațiilor care trebuie incluse în raportul de sinteză. ENISA informează Grupul de cooperare și rețeaua CSIRT cu privire la constatările sale referitoare la notificările primite o dată la șase luni.			
	(10) Echipele CSIRT sau, după caz, autoritățile competente furnizează autorităților competente în temeiul Directivei (UE) 2022/2557 informații cu privire la incidentele semnificative, incidentele, amenințările cibernetice și incidentele evitate la limită notificate în conformitate cu alineatul (1) de la prezentul articol și cu articolul 30 de către entitățile identificate ca fiind entități critice în temeiul Directivei (UE) 2022/2557.	Art. 15 alin. (16)	(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 dispozițiilor legale privind reziliența entităților critice.	
	(11) Comisia poate adopta acte de punere în aplicare pentru a preciza mai în detaliu tipul de informații, formatul și procedura referitoare la o notificare transmisă în temeiul alineatului (1) de la prezentul articol și al articolului 30 și la o comunicare transmisă în temeiul alineatului (2) de la prezentul articol. Până la 17 octombrie 2024, Comisia adoptă, în ceea ce privește furnizorii de servicii DNS, registrele de nume TLD, 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, acte de punere în aplicare pentru a preciza mai în detaliu cazurile în care un incident este considerat a fi semnificativ, astfel cum se menționează la alineatul (3). Comisia poate adopta astfel de acte de punere în aplicare și pentru alte entități esențiale și entități importante.			Nu este necesara transpunerea. Prevedere ce abilitează Comisia să adopte acte de punere în aplicare.

	Comisia face schimb de opinii şi cooperează cu Grupul de cooperare privind proiectele de acte de punere în aplicare menţionate la primul şi al doilea paragraf de la prezentul alineat, în conformitate cu articolul 14 alineatul (4) litera (e). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menţionată la articolul 39 alineatul (2).			
Art. 24	(1) Pentru a demonstra conformitatea cu anumite cerinţe de la articolul 21, statele membre le pot solicita entităţilor esenţiale şi entităţilor importante să utilizeze anumite produse TIC, servicii TIC şi procese TIC, dezvoltate de entităţi esenţiale sau de entităţi importante ori achiziţionate de la părţi terţe, care sunt certificate în cadrul sistemelor europene de certificare a securităţii cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881. De asemenea, statele membre încurajează entităţile esenţiale şi entităţile importante să utilizeze servicii de încredere calificate.	Art. 25 alin. (1)	(1) DNSC, în exercitarea calităţii de autoritate competentă responsabilă cu securitatea cibernetică şi cu sarcinile de supraveghere şi asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică, are următoarele atribuţii: (...) m) încurajează utilizarea de către entităţile esenţiale şi importante a produselor TIC, serviciilor TIC şi proceselor TIC ce corespund cerinţelor de standardizare şi certificare în domeniul securităţii cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881 şi a serviciilor de încredere calificate, cu respectarea standardelor şi a specificaţiilor tehnice europene şi internaţionale relevante pentru securitatea reţelelor şi a sistemelor informatice;	

	(2) Comisia este împuternicită să adopte acte delegate, în conformitate cu articolul 38, pentru a completa prezenta directivă prin specificarea categoriilor de entități esențiale și de entități importante care au obligația de a utiliza anumite produse TIC, servicii TIC și procese TIC certificate sau de a obține un certificat în cadrul unui sistem european de certificare a securității cibernetice adoptat în temeiul articolului 49 din Regulamentul (UE) 2019/881. Respectivele acte delegate se adoptă atunci când se identifică niveluri insuficiente de securitate cibernetică și includ o perioadă de punere în aplicare. Înainte de a adopta astfel de acte delegate, Comisia efectuează o evaluare a impactului și desfășoară consultări în conformitate cu articolul 56 din Regulamentul (UE) 2019/881. (3) În cazurile în care nu este disponibil niciun sistem european adecvat de certificare a securității cibernetice în sensul alineatului (2) de la prezentul articol, Comisia poate solicita ENISA să pregătească o propunere de sistem în temeiul articolului 48 alineatul (2) din Regulamentul (UE) 2019/881, după consultarea Grupului de cooperare și a Grupului european pentru certificarea securității cibernetice.			Nu este necesară transpunerea. Prevedere care împuternicește Comisia Europeană să adopte acte pentru a completa prezenta directivă.
Art. 25	(1) Pentru promovarea punerii în aplicare convergente a articolului 21 alineatele (1) și (2), statele membre, fără a impune un anumit tip de tehnologie sau a discrimina în favoarea utilizării acestuia, încurajează utilizarea standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice.	Art. 25 alin. (1)	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: 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;	
	(2) ENISA, în cooperare cu statele membre și, după caz, după consultarea părților interesate relevante, elaborează avize și orientări în ceea ce privește domeniile tehnice care ar trebui să fie examinate în legătură cu alineatul (1), precum și în ceea ce privește standardele deja existente, inclusiv standardele naționale, care ar permite reglementarea respectivelor domenii.	Art. 40 alin. (1)	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.	
Art. 26	(1) Entitățile care intră în domeniul de aplicare al prezentei directive sunt considerate ca fiind sub jurisdicția statului membru în care sunt stabilite, cu următoarele excepții:	Art. 7 alin. (1)	(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.	
	a) furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului, care se consideră că intră sub jurisdicția statului membru în care își prestează serviciile;	Art. 7 alin. (2)	(2) Prin excepție de la alin. (1), furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice destinate publicului intră în domeniul de aplicare al prezentei ordonanțe de urgență atunci când prestează servicii pe teritoriul României, indiferent de locul de înființare sau de înregistrare.	
	b) 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, care se consideră că se află sub jurisdicția statului membru în care își au sediul principal în Uniune în temeiul alineatului (2);	Art. 7 alin. (3)	(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.	
	c) entitățile administrației publice, care se consideră că intră sub jurisdicția statului membru care le-a instituit.	Art. 7 alin. (4)	(4) Entitățile administrației publice străine sunt în jurisdicția statului care le-a instituit.	
	(2) În sensul prezentei directive, se consideră că o entitate, astfel cum este menționată la alineatul (1) litera (b), își are sediul principal din Uniune în statul membru în care se iau în mod predominant deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică. Dacă un astfel de stat membru nu poate fi stabilit sau dacă astfel de decizii nu sunt luate în Uniune, sediul principal este considerat a fi în statul membru în care se desfășoară operațiunile de securitate cibernetică. Dacă un astfel de stat membru nu poate fi stabilit, sediul principal este considerat a fi în statul membru în care entitatea în cauză își are sediul cu cel mai mare număr de angajați din Uniune.	Art. 7 alin. (5)	(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) sau dacă astfel de decizii nu sunt luate în Uniunea Europeană, 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.	
	(3) În cazul în care o entitate, astfel cum este menționată la alineatul (1) litera (b), nu este stabilită în Uniune, dar oferă servicii în Uniune, aceasta desemnează un reprezentant în Uniune. Reprezentantul se stabilește în unul dintre statele membre în care se oferă serviciile. O astfel de entitate se consideră a fi sub jurisdicția statului membru în care este stabilit reprezentantul. În absența unui reprezentant în Uniune desemnat în temeiul prezentului alineat, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității pentru încălcarea prezentei directive.	Art. 7 alin. (6) si (7)	(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. În acest caz, entitatea se consideră a fi sub jurisdicția statului membru în care este stabilit reprezentantul. (7) Atunci când entitatea 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, inclusiv în cazul în care	

			entitatea nu a desemnat un reprezentant conform alin. (6).	
	(4) Desemnarea unui reprezentant de către o entitate, astfel cum este menționată la alineatul (1) litera (b), nu aduce atingere acțiunilor în justiție care ar putea fi inițiate împotriva entității înseși.	Art. 7 alin. (3), (6) si (7)	(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. (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. În acest caz, entitatea se consideră a fi sub jurisdicția statului membru în care este stabilit reprezentantul. (7) Atunci când entitatea 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, inclusiv în cazul în care entitatea nu a desemnat un reprezentant conform alin. (6).	
	(5) Statele membre care au primit o cerere de asistență reciprocă în legătură cu o entitate, astfel cum este menționată la alineatul (1) litera	Art. 45	(1) Atunci când o entitate înregistrată în România ca entitate esențială sau importantă furnizează servicii în mai	

	(b), pot, în limitele cererii respective, să ia măsuri adecvate de supraveghere şi de asigurare a respectării legii în ceea ce priveşte entitatea în cauză care furnizează servicii sau care are o reţea şi un sistem informatic pe teritoriul lor.		multe state membre sau furnizează servicii în unul sau mai multe state membre iar reţeaua şi sistemele sale informatice sunt situate în unul sau mai multe alte state membre, DNSC cooperează cu celelalte autorităţi competente omoloage de la nivelul Uniunii Europene şi îşi oferă asistenţă reciprocă. (2) În situaţia alin. (1), DNSC poate solicita autorităţilor competente omoloage de la nivelul Uniunii Europene să exercite atribuţii de supraveghere şi control şi, 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 şi România, sau furnizează servicii în unul sau mai multe state membre iar reţeaua şi sistemele sale informatice sunt situate în unul sau mai multe alte state membre, printre care şi România, DNSC cooperează cu celelalte autorităţi competente omoloage de la nivelul Uniunii Europene şi îşi oferă asistenţă reciprocă. (4) În situaţia alin. (3), DNSC poate exercita atribuţii de supraveghere şi control la solicitarea expresă a autorităţilor competente omoloage de la nivelul Uniunii Europene.	
Art. 27	(1) ENISA creează şi păstrează un registru al furnizorilor de servicii DNS, registrelor de nume TLD, al entităţilor care prestează servicii de înregistrare a numelor de domenii, al furnizorilor de servicii de cloud computing, al furnizorilor de servicii de centre de date, al furnizorilor de reţele de furnizare de conţinut, al furnizorilor de servicii gestionate, al furnizorilor de servicii de securitate gestionate, precum şi al furnizorilor de			Nu este necesara transpunerea. Prevedere ce stabileşte o obligaţie pentru ENISA.

	piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, pe baza informațiilor primite de la punctele unice de contact în conformitate cu alineatul (4). La cerere, ENISA permite accesul autorităților competente la registrul respectiv, asigurându-se în același timp că confidențialitatea informațiilor este protejată, după caz			
	(2) Până la 17 ianuarie 2025, statele membre solicită entităților menționate la alineatul (1) să transmită autorităților competente următoarele informații:	Art. 18 alin. (1) - (3)	(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 entității;		a) denumirea;	
	b) sectorul, subsectorul relevant și tipul de entitate menționate în anexa I sau II, după caz;		f) sectorul, subsectorul și tipul de entitate, astfel cum acestea se încadrează în anexa 1 sau în anexa 2;	
	c) adresa sediului principal al entității și a celorlalte sedii legale ale sale din Uniune sau, dacă nu este stabilită în Uniune, adresa reprezentantului său desemnat în temeiul articolului 26 alineatul (3)		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; e) persoana desemnată în calitate de reprezentant al entității, adresa și datele de contact ale acesteia, dacă entitatea nu este stabilită în Uniunea Europeană;	
	d) datele de contact actualizate, inclusiv adresele de e-mail și numerele de telefon ale entității și, după caz, ale reprezentantului său		b) adresa sediului social principal și datele de contact actualizate, inclusiv	

	desemnat în temeiul articolului 26 alineatul (3);		adresele de e-mail şi numerele de telefon; e) persoana desemnată în calitate de reprezentant al entităţii, adresa şi datele de contact ale acesteia, dacă entitatea nu este stabilită în Uniunea Europeană;	
	e) statele membre în care entitatea furnizează servicii; şi		g) statele membre în care prestează servicii, după caz;	
	f) gamele de adrese IP ale entităţii.		h) intervalele de adrese IP publice ale entităţii, în cazul furnizorilor de servicii DNS, registrelor de nume TLD, entităţilor care furnizează servicii de înregistrare a numelor de domenii, furnizorilor de servicii de cloud computing, operatorilor de reţele de livrare de conţinut, furnizorilor de servicii de centre de date, furnizorilor de servicii gestionate, furnizorilor de servicii de securitate gestionate şi furnizorilor de servicii digitale;	
	(3) Statele membre se asigură că entităţile menţionate la alineatul (1) notifică autorităţii competente fără întârziere şi, în orice caz, în termen de trei luni de la data modificării, orice modificare a informaţiilor pe care le-au transmis în temeiul alineatului (2).	Art. 18 alin. (8)	(8) Entităţile prevăzute la alin. (2) comunică DNSC modificările aduse informaţiilor prevăzute la alin. (3), astfel: a) pentru informaţiile prevăzute la alin. (3) lit. a)-d), lit. f) şi lit. j), fără întârzieri nejustificate şi în orice caz în termen de cel mult 2 săptămâni de la data modificării; b) pentru informaţiile prevăzute la alin. (3) lit. e) şi lit. g)-i), fără întârzieri nejustificate şi în orice caz în termen de cel mult trei luni de la data modificării.	
	(4) După ce primeşte informaţiile menţionate la alineatele (2) şi (3), cu excepţia celor menţionate la alineatul (2) litera (f), punctul unic de contact al statului membru în cauză le înaintează către ENISA, fără întârzieri nejustificate.	Art. 18 alin. (10)	(10) Punctul unic de contact naţional transmite în legătură cu furnizorii de servicii DNS, registrele de nume TLD, entităţile care furnizează servicii de înregistrare a numelor de domenii, furnizorii de servicii de cloud computing, operatorii de reţele de livrare de conţinut, furnizorii de servicii de centre de date, furnizorilor de	

			servicii gestionate, furnizorii de servicii de securitate gestionate şi furnizorii de servicii digitale, informaţiile prevăzute la alin. (3) către ENISA, după primirea acestora, cu excepţia informaţiilor cuprinse în alin. (3) lit. i) şi lit. j) până cel târziu la 17 ianuarie 2025 şi ori de câte ori intervin modificări în legătură cu acestea. Punctul unic de contact revizuieşte informaţiile prevăzute în mod regulat şi cel puţin o dată la doi ani. Până la 17 aprilie 2025 şi la cererea Comisiei Europene, punctul unic de contact naţional notifică Comisiei Europene denumirile entităţilor esenţiale şi ale entităţilor importante identificate conform art. 9.	
	(5) După caz, informaţiile menţionate la alineatele (2) şi (3) de la prezentul articol se transmit prin mecanismul naţional menţionat la articolul 3 alineatul (4) al patrulea paragraf.	Art. 18 alin. (1) - (3)	(1) DNSC păstrează un registru al entităţilor esenţiale şi al entităţilor importante identificate. (2) Entităţile care desfăşoară activitate în sectoarele din anexele 1 şi 2, notifică DNSC în vederea înregistrării în cel mult 30 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă sau în termen de cel mult 30 zile de la data la care prevederile prezentei ordonanţe de urgenţă le sunt aplicabile, atunci când, conform art. 5 şi art. 6, se încadrează ca entităţi esenţiale sau entităţi importante. (3) Notificarea de la alin. (2), constă în furnizarea către DNSC a următoarelor tipuri de informaţii: a) denumirea; b) adresa sediului social principal şi datele de contact actualizate, inclusiv adresele de e-mail şi numerele de telefon; c) adresele celorlalte sedii sociale din Uniunea Europeană, după caz;	

			d) mijloacele permanente de contact şi persoana din cadrul entităţii însărcinată cu monitorizarea mijloacelor de contact; e) persoana desemnată în calitate de reprezentant al entităţii, adresa şi datele de contact ale acesteia, dacă entitatea nu este stabilită în Uniunea Europeană; f) sectorul, subsectorul şi 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 entităţii, în cazul furnizorilor de servicii DNS, registrelor de nume TLD, entităţilor care furnizează servicii de înregistrare a numelor de domenii, furnizorilor de servicii de cloud computing, operatorilor de reţele de livrare de conţinut, furnizorilor de servicii de centre de date, furnizorilor de servicii gestionate, furnizorilor de servicii de securitate gestionate şi furnizorilor de servicii digitale; i) intervalele de adrese IP publice ale entităţii, pentru alte entităţi decât cele prevăzute la lit. h), după caz; j) informaţii necesare şi suficiente din care să rezulte îndeplinirea condiţiilor pentru identificarea drept entitate esenţială sau entitate importantă conform art. 5 şi respectiv art. 6.	
Art. 28	(1) Pentru a contribui la securitatea, stabilitatea şi reziliența DNS, statele membre solicită ca registrele de nume TLD şi entităţile care prestează servicii de înregistrare a numelor de domenii să colecteze şi să menţină date exacte şi complete privind înregistrarea numelor de domenii într-o bază de date dedicată, cu diligența necesară, în conformitate cu dreptul	Art. 19 alin. (1)	(1) Pentru a contribui la securitatea, stabilitatea şi reziliența sistemelor de nume de domenii, registrele de nume TLD şi entităţile care furnizează servicii de înregistrare a numelor de domenii colecteaza si mentin, cu diligenta necesara, date exacte şi complete de înregistrare a numelor de domenii într-o bază de date dedicată, în	

	Uniunii în materie de protecție a datelor cu caracter personal.		conformitate cu dreptul Uniunii privind protecția datelor.	
	(2) În sensul alineatului (1), statele membre solicită ca baza de date cu datele de înregistrare a numelor de domenii să conțină informațiile necesare pentru identificarea și contactarea titularilor numelor de domenii și a punctelor de contact care administrează numele de domenii în cadrul TLD-urilor. Informațiile includ:	Art. 19 alin. (2)	Art. 19 (2) Baza de date prevazuta la 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;		a) numele de domeniu;	
	b) data înregistrării;		b) data înregistrării;	
	c) numele, adresa de e-mail și numărul de telefon de contact ale solicitantului înregistrării;		c) numele, adresa de e-mail și numărul de telefon ale solicitantului înregistrării;	
	d) adresa de e-mail și numărul de telefon de contact ale punctului de contact care administrează numele de domeniu în cazul în care acestea sunt diferite de cele 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) Statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să dispună de politici și proceduri, inclusiv proceduri de verificare, care să asigure că bazele de date menționate la alineatul (1) conțin informații exacte și complete. Statele membre solicită ca aceste politici și proceduri să fie puse la dispoziția publicului	Art. 19 alin. (3)	(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 baza de date menționata la alin. (1) conține informații exacte și complete și pun la dispoziția publicului aceste politici și proceduri.	
	(4) Statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să pună la dispoziția publicului, fără întârzieri nejustificate după înregistrarea unui nume de domeniu, datele de înregistrare a numelui de domeniu care nu sunt date cu caracter personal.	Art. 19 alin. (4)	(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) Statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să ofere acces la datele de înregistrare a numelor de domenii specifice în baza unor cereri legale și justificate	Art. 19 alin. (8) si (9)	(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	

	în mod corespunzător ale solicitanților de acces legitimi, în conformitate cu dreptul Uniunii în materie de protecție a datelor. Statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să răspundă fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la primirea cererilor de acces. Statele membre solicită ca politicile și procedurile de divulgare a unor astfel de date să fie puse la dispoziția publicului.		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.	
	(6) Respectarea obligațiilor prevăzute la alineatele (1)-(5) nu trebuie să ducă la o suprapunere în colectarea datelor de înregistrare a numelor de domenii. În acest scop, statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să coopereze între ele.	Art. 19 alin. (10)	(10) Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii cooperează între ele, inclusiv pentru a evita suprapunerile în colectarea datelor de înregistrare a numelor de domenii, în contextul indeplinirii obligatilor prevazute la alin. (1) - (9).	
Art. 29	(1) Statele membre se asigură că entitățile care intră în domeniul de aplicare al prezentei directive și, după caz, alte entități care nu intră în domeniul de aplicare al prezentei directive pot face schimb reciproc de informații relevante în materie de securitate cibernetică, pe bază voluntară, inclusiv de informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice, în cazul în care un astfel de schimb de informații:	Art. 20 alin. (1) - (3)	(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 cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice. (3) Schimbul de informații se realizează în următoarele scopuri:	
	a) vizează prevenirea și detectarea incidentelor, răspunsul la incidente sau redresarea în urma acestora sau atenuarea impactului lor;		a) prevenirea și detectarea incidentelor, răspunsul la incidente sau redresarea în urma acestora sau atenuarea impactului lor;	

	b) sporeşte nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la ameninţările cibernetice, prin limitarea sau împiedicarea posibilităţii răspândirii unor asemenea ameninţări, sprijinirea gamei de capacităţi defensive, remedierea şi divulgarea vulnerabilităţilor, detectarea ameninţărilor, tehnicile de limitare şi prevenire a ameninţărilor, strategiile de atenuare sau etapele proceselor de răspuns şi de recuperare sau promovarea colaborării dintre entităţile publice şi private în domeniul cercetării ameninţărilor cibernetice.		b) sporirea nivelului de securitate cibernetică, în special prin sensibilizarea cu privire la ameninţările cibernetice, prin limitarea sau împiedicarea posibilităţii răspândirii unor asemenea ameninţări, sprijinirea gamei de capacităţi defensive, remedierea şi divulgarea vulnerabilităţilor, detectarea ameninţărilor, tehnicile de limitare şi prevenire a ameninţărilor, strategiile de atenuare sau etapele proceselor de răspuns şi de recuperare sau promovarea colaborării dintre entităţile publice şi private în domeniul cercetării ameninţărilor cibernetice.	
	(2) Statele membre se asigură că schimbul de informaţii are loc în cadrul unor comunităţi ale entităţilor esenţiale şi ale entităţilor importante şi, după caz, ale prestatorilor sau furnizorilor lor de servicii. Un astfel de schimb este pus în aplicare prin acorduri privind schimbul de informaţii în materie de securitate cibernetică, în considerarea caracterului potenţial sensibil al informaţiilor partajate.	Art. 20 alin. (2)	(2) Schimbul de informaţii prevăzut la alin. (1) se realizează în cadrul unor comunităţi ale entităţilor esenţiale şi ale entităţilor importante şi, după caz, ale prestatorilor sau furnizorilor lor de servicii, prin intermediul unor acorduri privind schimbul de informaţii în materie de securitate cibernetică.	Norma imperativă a fost introdusă, în cadrul textului de lege nefiind necesar a introduce şi explicaţia pentru caracterul imperativ.
	(3) Statele membre facilitează instituirea acordurilor privind schimbul de informaţii în materie de securitate cibernetică menţionate la alineatul (2) de la prezentul articol. Astfel de acorduri pot specifica elemente operaţionale, inclusiv utilizarea platformelor TIC dedicate şi a instrumentelor de automatizare, conţinutul şi condiţiile acordurilor privind schimbul de informaţii. Atunci când stabilesc detaliile implicării autorităţilor publice în astfel de acorduri, statele membre pot impune condiţii cu privire la informaţiile puse la dispoziţie de autorităţile competente sau de echipele CSIRT. Statele membre oferă asistenţă pentru aplicarea unor astfel de acorduri în conformitate cu politicile lor menţionate la articolul 7 alineatul (2) litera (h).	Art. 20 alin. (4) si (5) Art. 4 lit. d) şi art. 16 alin. (3) din OUG 104 din 22 septembrie 2021 privind înfiinţarea Directoratului	Art. 20 (4) Acordurile privind schimbul de informaţii în materie de securitate cibernetică cuprind şi informaţii cu privire la elemente operaţionale, inclusiv utilizarea platformelor TIC dedicate şi a instrumentelor de automatizare, conţinutul şi condiţiile acordurilor privind schimbul de informaţii şi se notifică DNSC atât încheierea, cât şi retragerea din cadrul acestora. (5) DNSC poate sprijini entităţile interesate în încheierea unui acord privind schimbul de informaţii în materie de securitate cibernetică şi poate solicita limitarea schimbului de	Aceasta este o teză care să sprijine SM în transpunerea prevederii referitoare la acordurile privind schimbul de informaţii, iar România a introdus posibilitatea DNSC de a solicita limitarea informaţiilor care fac obiectul schimbului de informaţii.

		Național de Securitate Cibernetică	informații atunci când acestea fac referire la informațiile puse la dispoziție de autorități competente sau de echipele de răspuns la incidente de securitate cibernetică. Art. 4 Principalele obiective ale DNSC sunt: d) crearea și operarea unei platforme naționale de colaborare care să permită schimbul de informații între constituenți, instituții ale statului, mediul academic și mediul privat în domeniul incidentelor, vulnerabilităților și crizelor de natură cibernetică; Art. 16 (3) Pentru asigurarea unei capacități adecvate de identificare, evaluare și adoptare a unor măsuri de management al riscului și/sau de răspuns la incidente și atacuri cibernetice, DNSC dezvoltă schimburi de informații și transfer de expertiză cu instituțiile și autoritățile cu responsabilități în domeniu, promovează și susține cooperarea între sectorul public și cel privat, precum și cooperarea cu mediile neguvernamentale și comunitatea academică.	
	(4) Statele membre se asigură că entitățile esențiale și entitățile importante informează autoritățile competente cu privire la participarea lor la acordurile privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2), odată cu încheierea unor astfel de acorduri sau, după caz, cu retragerea din astfel de acorduri, după ce retragerea intră în vigoare.	Art. 20 alin. (4)	(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) ENISA oferă asistență pentru instituirea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) prin schimbul de bune practici și oferind orientări.			Prevedere ce impune o obligație pentru ENISA, care nu necesită transpunere.
Art. 30	(1) Statele membre se asigură că, pe lângă obligația de notificare prevăzută la articolul 23, notificările pot fi transmise echipelor CSIRT sau, după caz, autorităților competente, în mod voluntar, de către:	Art. 16 alin. (1)	(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;		a) entitățile esențiale și entitățile importante, cu privire la incidente, amenințări cibernetice și incidente evitate la limită;	
	b) alte entități decât cele menționate la litera (a), indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, cu privire la incidente semnificative, amenințări cibernetice și incidente evitate la limită.		b) alte entități decât cele menționate la lit. a), indiferent dacă intră sau nu în domeniul de aplicare al prezentei ordonanțe de urgență, cu privire la incidente semnificative, amenințări cibernetice și incidente evitate la limită.	
	(2) Statele membre prelucrează notificările menționate la alineatul (1) de la prezentul articol în conformitate cu procedura prevăzută la articolul 23. Statele membre pot trata notificările obligatorii cu prioritate față de notificările voluntare.	Art. 16 alin. (2) si (3)	(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.	
	Dacă este necesar, echipele CSIRT și, după caz, autoritățile competente furnizează punctelor unice de contact informațiile despre notificările primite în temeiul prezentului articol, asigurând totodată confidențialitatea și protecția adecvată a informațiilor furnizate de entitatea notificatoare. Fără a aduce atingere prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, raportarea voluntară nu impune entității notificatoare nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis notificarea.	Art. 16 alin. (4)	(4) Raportarea voluntară nu impune entității notificatoare nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis raportarea.	Legea penală are caracter special și este redundantă precizarea expresă a sintagmei.
Art. 31	(1) Statele membre se asigură că autoritățile lor competente supraveghează în mod eficace și iau	Art. 25 alin. (1) lit. b) - h)	Art. 25 (1) DNSC, în exercitarea calității de autoritate competentă responsabilă cu	

	măsurile necesare pentru a asigura respectarea prezentei directive.	Art. 26 alin. (1) Art. 37 alin. (10) si (12) Art. 61 alin. (2)	securitatea cibernetică şi cu sarcinile de supraveghere şi asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică, are următoarele atribuţii: (...) b) emite norme şi cerinţe în domeniul de aplicare al prezentei ordonanţe de urgenţă prin ordine şi decizii ale Directorului DNSC; c) elaborează şi actualizează ghiduri, recomandări şi bune practici în domeniul de aplicare al prezentei ordonanţe de urgenţă; d) administrează şi gestionează resursele pentru punerea în aplicarea a prezentei ordonanţe de urgenţă; e) participă, prin reprezentanţi, la formatele de cooperare la nivel european; f) supraveghează, verifică şi controlează respectarea prevederilor prezentei ordonanţe de urgenţă; g) primeşte sesizări cu privire la neîndeplinirea obligaţiilor de către entităţile esenţiale şi importante; h) cooperează cu autorităţile competente din celelalte state şi oferă asistenţă acestora, prin schimbul de informaţii, transmiterea de solicitări şi sesizări, efectuarea controlului ori luarea de măsuri de supraveghere şi remediere a deficienţelor constatate, în cazul entităţilor care fac obiectul prezentei ordonanţe de urgenţă; Art. 26 (1) DNSC, în exercitarea atribuţiilor de supraveghere şi control, în cazul neîndeplinirii de către entităţile esenţiale şi entităţile importante a obligaţiilor ce le revin conform dispoziţiilor prezentei ordonanţe de urgenţă, 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. Art. 37 (10) Autoritățile competente sectorial sunt, de asemenea, împuternicite să asigure supravegherea, controlul și sancționarea în aplicarea prevederilor prezentei ordonanțe de urgență, precum și ale regulamentelor Uniunii Europene din domeniul securității cibernetice și ale actelor de punere în aplicare a dispozițiilor Directivei (UE) 2022/2555 care vizează entitățile din sectorul lor de competență potrivit prezentei ordonanțe de urgență, în cazul în care competențele de supraveghere, control și sancționare ale Regulamentelor, respectiv ale actelor de punere în aplicare, nu au fost acordate altei autorități. (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 legale privind reziliența entităților critice. Art. 61 (2) Constatarea contravențiilor prevăzute la art. 60 alin. (1) lit. a)-n), ee), ff), jj)-oo) se realizează de către DNSC sau de către personalul de	

			control al autorităților competente sectorial conform art. 37 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). Constatarea contravențiilor prevăzute la art. 60 alin. (1) lit. o)-dd), gg)-ii) se realizează de către DNSC, aplicarea sancțiunii realizându-se prin decizie a Directorului DNSC.	
	(2) Statele membre pot permite autorităților lor competente să acorde prioritate sarcinilor de supraveghere. O asemenea prioritizare are la bază o abordare bazată pe riscuri. În acest scop, atunci când își exercită sarcinile de supraveghere prevăzute la articolele 32 și 33, autoritățile competente pot stabili metodologii de supraveghere care să permită tratarea cu prioritate a acestor sarcini, urmând o abordare bazată pe riscuri.	Art. 47 alin. (8)	(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.	
	(3) Autoritățile competente lucrează în strânsă cooperare cu autoritățile de supraveghere în temeiul Regulamentului (UE) 2016/679 în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, fără a aduce atingere competențelor și sarcinilor autorităților de supraveghere în temeiul regulamentului respectiv.	Art. 37 alin. (4) Art. 62 alin. (1)	Art. 37 (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. Art. 62 (1) DNSC informează, fără întârzieri nejustificate, 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.	
	(4) Fără a aduce atingere cadrelor legislative și instituționale naționale, statele membre se asigură că, în ceea ce privește supravegherea respectării prezentei directive de către entitățile administrației publice și aplicarea de măsuri de asigurare a respectării legii în cazul încălcării prezentei directive, autoritățile competente au competențele corespunzătoare pentru a îndeplini astfel de sarcini cu independență operațională în raport cu entitățile administrației publice care sunt supravegheate. Statele membre pot decide impunerea unor măsuri adecvate, proporționale și efective de supraveghere și de asigurare a respectării legii în ceea ce privește respectivele entități, în conformitate cu cadrele legislative și instituționale naționale.	Art. 24 alin. (1) Art. 26 alin. (1) Art. 37 alin. (10) si (12) Art. 46	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. 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. Art. 37 (10) Autoritățile competente sectorial sunt, de asemenea, împuternicite să asigure supravegherea, controlul și sancționarea în aplicarea prevederilor prezentei ordonanțe de urgență, precum și ale regulamentelor Uniunii Europene din domeniul securității cibernetice și ale actelor de punere în aplicare a dispozițiilor Directivei (UE) 2022/2555 care vizează entitățile din sectorul lor de competență potrivit prezentei ordonanțe de urgență, în cazul în care	

			competențele de supraveghere, control și sancționare ale Regulamentelor, respectiv ale actelor de punere în aplicare, nu au fost acordate altei autorități. (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 legale privind reziliența entităților critice.	
		Art. 61 alin. (2)	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 şi 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 şi control sau în următoarele cazuri, fără a fi limitate la acestea: a) unui incident semnificativ; b) indiciilor temeinice cu privire la încălcarea dispoziţiilor prezentei ordonanţe de urgenţă de către o entitate. (3) Activitatea de supraveghere şi control se realizează de către DNSC inclusiv la solicitarea motivată a CNCPIC pentru entităţile identificate critice conform dispoziţiilor legale privind reziliența entităţilor critice. (4) În cazul entităţilor 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 entităţille esenţiale şi entităţile importante, DNSC poate efectua scanări de securitate cibernetică neintruzive şi proactive, bazate pe criterii obiective, nediscriminatorii, echitabile şi transparente pentru evaluarea riscurilor, cu notificarea prealabilă a entităţii în cauză şi, după caz, în cooperare cu aceasta. (6) În vederea punerii în aplicare a alin. (2), DNSC poate solicita accesul la date, echipamente hardware şi software, precum şi informaţii de la	

			personalul entităților în vederea îndeplinirii sarcinilor de supraveghere şi control. (7) Cu ocazia desfăşurării auditului de securitate cibernetică în condiţiile prevăzute la art. 11 alin. (5) sau, după caz, alin. (6), se realizează o evaluare sistematică a tuturor politicilor, procedurilor şi măsurilor de protecţie implementate la nivelul unor reţele şi sisteme informatice, în vederea identificării disfuncţionalităţilor şi vulnerabilităţilor şi 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 şi, după caz, autorităţii competente sectorial, rezultatele acestuia. (9) Costurile generate de auditul de securitate cibernetică, inclusiv cel ad-hoc, sunt suportate de către entitatea auditată. Art. 61 (2) Constatarea contravenţiilor prevăzute la art. 60 alin. (1) lit. a)-n), ee), ff), jj)-oo) se realizează de către DNSC sau de către personalul de control al autorităţilor competente sectorial conform art. 37 alin. (1), pentru entităţile esenţiale sau importante, după caz, care îşi desfăşoară activitatea în domeniul de competenţă al acestor autorităţi, aplicarea sancţiunii realizându-se, în cazul autorităţilor competente sectorial, prin decizie a conducerii acestora, cu aplicarea în mod corespunzător a alin. (3)-(8). Constatarea contravenţiilor prevăzute la art. 60 alin. (1) lit. o)-dd), gg)-ii) se realizează de către DNSC,	

			aplicarea sancțiunii realizându-se prin decizie a Directorului DNSC.	
Art. 32	(1) Statele membre se asigură că măsurile de supraveghere sau de asigurare a respectării legii impuse entităților esențiale în ceea ce privește obligațiile prevăzute în prezenta directivă sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte.	Art. 24 alin. (3) Art. 25 alin. (1) lit. a)-d), f)-h) si l) Art. 50 alin. (1)	Art. 24 (3) În vederea îndeplinirii atribuțiilor ce îi revin în temeiul prevederilor prezentei ordonanțe de urgență, 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. 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; 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 aplicarea a prezentei ordonanțe de urgență; 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; l) asigură ducerea la îndeplinire a obligațiilor de raportare a incidentelor de către entitățile esențiale și importante în condițiile 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) Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile esențiale, au competența de a supune entitățile respective cel puțin:			
	a) unor inspecții la fața locului și unei supravegheri ex situ, inclusiv unor verificări aleatorii, realizate de profesioniști cu formare corespunzătoare;	Art. 24 alin. (3) si (4) lit. d)	Art. 24 (3) În vederea îndeplinirii atribuțiilor ce îi revin în temeiul prevederilor prezentei ordonanțe de urgență, 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.	

		Art. 46 alin. (1) lit. a) Art. 50 alin. (3)	(4) Pentru aplicarea alin. (3), din bugetul DNSC se asigură, cu respectarea prevederilor legale, următoarele categorii de cheltuieli: (...) d) cursuri de formare şi perfecţionare precum şi certificări ale personalului propriu; Art. 46 (1) În scopul asigurării respectării dispoziţiilor prezentei ordonanţe de urgenţă, precum şi a actelor normative subsecvente de către entităţi, DNSC, poate: a) derula activităţi de supraveghere, verificare şi control efectuate de persoane desemnate în acest sens prin decizie a Directorului DNSC; Art. 50 (3) Organele de conducere ale entităţii răspund pentru permiterea accesului personalului, desemnat în acest sens de către DNSC, în spaţiile supuse controlului, cât şi asupra datelor şi informaţiilor necesare controlului.	
	b) unor audituri de securitate periodice şi specifice efectuate de un organism independent sau de o autoritate competentă;	Art. 11 alin. (5) si (6) Art. 57 alin. (1) lit. a) si (7)	Art. 11 (5) Entităţile esenţiale şi entităţile importante sunt obligate să se supună efectuării unui audit de securitate cibernetică în condiţiile şi cu periodicitatea stabilite prin ordinul Directorului DNSC prevăzut la art. 12 alin. (1), în funcţie de nivelul de risc prevăzut la alin. (3). (6) Atunci când există autoritatea cu competenţe sectoriale, condiţiile şi periodicitatea auditului de securitate prevăzute la alin. (5) vor fi stabilite prin ordin comun în condiţiile art. 37 alin. (8) lit. b), în funcţie de nivelul de risc prevăzut la alin. (3).	

		Art. 58 alin. (1)	Art. 57 (1) Auditul de securitate cibernetică poate fi: a) periodic, care se desfăşoară cu regularitate, conform ordinului de la art. 12 alin. (1); (7) Cu ocazia desfăşurării auditului de securitate cibernetică periodic, se realizează o evaluare sistematică a tuturor politicilor, procedurilor şi măsurilor de protecţie implementate la nivelul unor reţele şi sisteme informatice, în vederea identificării disfuncţionalităţilor şi vulnerabilităţilor şi recomandării măsurilor de remediere a acestora. Art. 58 (1) Auditul de securitate cibernetică se realizează de către auditorii de securitate cibernetică ce deţin atestat valabil eliberat de către DNSC, cu excepţia auditului de securitate cibernetică realizat la nivelul instituţiilor cu responsabilităţi în domeniul apărării, ordinii publice şi securităţii naţionale, precum şi pentru serviciile puse la dispoziţie de către acestea.	
	c) unor audituri ad-hoc, inclusiv în cazurile justificate de un incident semnificativ sau de o încălcare a prezentei directive de către entitatea esențială;	Art. 46 alin. (1) lit. b) Art. 48 alin. (2) lit. a)	Art. 46 (1) În scopul asigurării respectării dispoziţiilor prezentei ordonanţe de urgenţă, precum şi a actelor normative subsecvente de către entităţi, DNSC, poate: (...) b) dispune efectuarea de audituri de securitate ad-hoc, realizate de un auditor de securitate cibernetică atestat; Art. 48	Aceasta este interpretarea României în ceea ce priveşte aplicabilitatea normelor directivei pentru cadrul legislativ naţional cu privire la auditul ad-hoc, ţinând cont de faptul că specificul legislaţiei naţionale nu permite unele dispoziţii cu caracter obligatoriu în lipsa caracterului coercitiv al statului pentru acestea.

		Art. 57 alin. (1) lit. b), (2) si (3)	(2) DNSC poate dispune, după caz, următoarele: a) adoptarea unor măsuri atunci când acestea sunt necesare pentru a preveni sau remedia un incident, precum şi termene limită pentru punerea în aplicare a acestor măsuri, inclusiv a unui audit ad-hoc; Art. 57 (1) Auditul de securitate cibernetică poate fi: (...) b) ad-hoc, în baza deciziei Directorului DNSC conform alin. (2). (2) Auditul de securitate cibernetică ad-hoc are caracter excepţional şi reprezintă acea activitate de auditare efectuată de un auditor atestat conform dispoziţiilor prezentei ordonanţe de urgenţă, cu privire la o entitate esenţială sau o entitate importantă, la solicitarea motivată a DNSC, ca urmare a: a) unui incident semnificativ; b) o schimbare cu impact semnificativ la nivelul reţelelor şi sistemelor informatice, dar nu mai târziu de 180 de zile de la apariţia acesteia; c) indiciilor temeinice cu privire la încălcarea dispoziţiilor prezentei ordonanţe de urgenţă de către o entitate esenţială. (3) Atunci când se dispune un audit ad-hoc, DNSC comunică entităţii atât motivele, cât şi obiectivele auditului.	
	d) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile şi transparente de evaluare a riscurilor, după caz cu cooperarea entităţii în cauză	Art. 46 alin. (5)	(5) În vederea punerii în aplicare a alin. (1) lit. a) cu privire la entităţile esenţiale şi entităţile importante, DNSC poate efectua scanări de securitate cibernetică neintruzive şi proactive, bazate pe criterii obiective, nediscriminatorii, echitabile şi	

			transparente pentru evaluarea riscurilor, cu notificarea prealabilă a entității în cauză și, după caz, în cooperare cu aceasta.	
	e) unor cereri de 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 trimite informații autorităților competente în temeiul articolului 27;	Art. 46 alin. (1) lit. c)	(1) În scopul asigurării respectării dispozițiilor prezentei ordonanțe de urgență, precum și a actelor normative subsecvente de către entități, DNSC, poate: (...) 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;	
	f) unor cereri de acces la date, la documente și la orice informații necesare pentru îndeplinirea sarcinilor lor de supraveghere;	Art. 46 alin. (1) lit. d)	(1) În scopul asigurării respectării dispozițiilor prezentei ordonanțe de urgență, precum și a actelor normative subsecvente de către entități, DNSC, poate: (...) d) solicita acces la date, la documente și la orice informații necesare pentru îndeplinirea sarcinilor de supraveghere;	
	g) unor cereri de dovezi privind punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și mijloacele de probă care stau la baza acestora.	Art. 46 alin. (1) lit. e)	(1) În scopul asigurării respectării dispozițiilor prezentei ordonanțe de urgență, precum și a actelor normative subsecvente de către entități, DNSC, poate: (...) 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.	
	Auditurile de securitate specifice, menționate la primul paragraf litera (b), se bazează pe evaluări ale riscurilor efectuate de autoritatea competentă	Art. 11 alin (1) - (6)	(1) Entitățile esențiale și entitățile importante iau măsuri tehnice, operaționale și organizatorice	

	sau de entitatea auditată sau pe alte informații disponibile legate de riscuri.		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).	
	Rezultatele oricărui audit de securitate specific se pun la dispoziția autorității competente. Costurile unui astfel de audit de securitate specific efectuat de un organism independent sunt plătite de entitatea auditată, în afara cazurilor justificate corespunzător, atunci când autoritatea competentă decide altfel.	Art. 46 alin. (8) si (9)	(8) În termen de cel mult 5 zile de la finalizarea oricărui audit de securitate cibernetică, entitatea auditată transmite către DNSC și, după caz, autorității competente sectorial, rezultatele acestuia. (9) Costurile generate de auditul de securitate cibernetică, inclusiv cel ad-hoc, sunt suportate de către entitatea auditată.	
	(3) Atunci când își exercită competențele în temeiul alineatului (2) literele (e), (f) sau (g), autoritățile competente precizează scopul solicitării și informațiile solicitate.	Art. 47 alin. (1)	(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.	
	(4) Statele membre se asigură că, atunci când își exercită competențele de asigurare a respectării legii în ceea ce privește entitățile esențiale, autoritățile lor competente au competența cel puțin:			
	a) de a emite avertismente cu privire la încălcări ale prezentei directive de către entitățile în cauză;	Art. 48 alin. (1) lit. a)	(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) de a adopta instrucțiuni obligatorii, inclusiv în ceea ce privește măsurile necesare pentru a preveni sau remedia un incident, precum și termene-limită pentru punerea în aplicare a acestor măsuri și pentru a raporta cu privire la punerea lor în aplicare, sau un ordin prin	Art. 48 alin. (2) lit. a)	Art. 48 (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	

	care le solicită entităților în cauză să remedieze deficiențele identificate sau încălcările prezentei directive;	Art. 47 alin. (3) și (7)	termene limită pentru punerea în aplicare a acestor măsuri, inclusiv a unui audit ad-hoc; Art. 47 (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. (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.	
	c) de a dispune ca entitățile în cauză să înceteze conduita prin care încalcă prezenta directivă și să se abțină de la repetarea conduitei respective;	Art. 48 alin. (2) lit. c) Art. 50 alin. (2)	Art. 48 (2) DNSC poate dispune, după caz, următoarele: (...) c) încetarea conduitei entităților prin care încalcă dispozițiile prezentei ordonanțe de urgență; Art. 50 (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. 11-14 sau obligațiile de raportare prevăzute la art. 15; 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).	
	d) de a dispune ca entitățile în cauză să asigure că măsurile lor de gestionare a riscurilor în materie de securitate cibernetică respectă dispozițiile de la articolul 21 sau să îndeplinească obligațiile de raportare prevăzute la articolul 23, într-un anumit mod și într-o anumită perioadă;	Art. 48 alin. (2) lit. f)	(2) DNSC poate dispune, după caz, următoarele: (...) 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;	
	e) de a dispune ca entitățile în cauză să informeze persoanele fizice sau juridice cu privire la care furnizează servicii sau desfășoară activități care sunt potențial afectate de o amenințare cibernetică semnificativă cu privire la caracterul amenințării, precum și cu privire la toate măsurile de protecție sau de remediere pe care le-ar putea lua persoanele fizice sau juridice în cauză ca răspuns la amenințarea respectivă	Art. 48 alin. (4)	(4) DNSC poate dispune entităților să informeze, într-un termen anume determinat, persoanele cărora le prestează un serviciu sau cu care desfășoară activități, 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.	
	f) de a dispune ca entitățile în cauză să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil;	Art. 48 alin. (2) lit. d)	(2) DNSC poate dispune, după caz, următoarele: (...)	

			d) punerea în aplicare a recomandărilor formulate ca urmare a unui audit de securitate;	
	g) de a desemna un ofițer de monitorizare cu sarcini bine definite pe o perioadă determinată de timp pentru a supraveghea respectarea de către entitățile în cauză a articolelor 21 și 23	Art. 48 alin. (2) lit. e)	(2) DNSC poate dispune, după caz, următoarele: (...) 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;	
	h) de a dispune ca entitățile în cauză să facă publice într-un mod specific aspectele legate de încălcări ale prezentei directive;	Art. 48 alin. (2) lit. g)	(2) DNSC poate dispune, după caz, următoarele: (...) g) ca încălcările dispozițiilor prezentei ordonanțe de urgență să fie făcute publice de către entitatea responsabilă.	
	i) de a aplica sau a solicita aplicarea de către organismele sau instanțele relevante, în conformitate cu dreptul intern, a unei amenzi administrative în temeiul articolului 34, în plus față de oricare dintre măsurile menționate la literele (a)-(h) de la prezentul alineat.	Art. 48 alin. (1) lit. b)	(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: (...) b) amendă contravențională.	
	(5) În cazul în care măsurile de asigurare a respectării legii adoptate în temeiul alineatului (4) literele (a)-(d) și (f) sunt ineficiente, statele membre se asigură că autoritățile lor competente au competența de a stabili un termen în care entității esențiale i se solicită să ia măsurile necesare pentru remedierea deficiențelor sau să respecte cerințele autorităților respective. În cazul în care acțiunea solicitată nu este întreprinsă în termenul stabilit, statele membre se asigură că autoritățile lor competente au competența:	Art. 49 alin. (1)	(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) de a suspenda temporar sau de a solicita unui organism de certificare sau de autorizare sau unei instanțe, în conformitate cu dreptul intern, suspendarea temporară a unei certificări sau a unei autorizații privind o		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	

	parte sau toate serviciile relevante furnizate sau activitățile relevante desfășurate de entitatea esențială;		sau pentru toate serviciile relevante furnizate sau pentru activitățile relevante desfășurate de entitatea respectivă;	
	b) de a solicita impunerea de către organismele sau instanțele relevante, în conformitate cu dreptul intern, a unei interdicții temporare de a exercita funcții de conducere în cadrul entității respective împotriva oricărei persoane fizice care exercită responsabilități de conducere la nivel de director executiv sau de reprezentant legal în entitatea esențială.		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.	
	Suspendările sau interdicțiile temporare impuse în temeiul prezentului alineat se aplică numai până în momentul în care entitatea în cauză ia măsurile necesare în vederea remedierii deficiențelor sau a respectării cerințelor impuse de autoritatea competentă pentru care au fost aplicate aceste măsuri de asigurare a respectării legii. Impunerea unor astfel de suspendări sau interdicții temporare face obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu carta, inclusiv dreptul la o cale de atac eficace și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare.	Art. 49 alin. (2) Art. 1 alin. (1) și (2) din Legea 554 din 2 decembrie 2004 contenciosului administrativ	Art. 49 (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. (1) Orice persoană care se consideră vătămată într-un drept al său ori într-un interes legitim, de către o autoritate publică, printr-un act administrativ sau prin nesoluționarea în termenul legal a unei cereri, se poate adresa instanței de contencios administrativ competente, pentru anularea actului, recunoașterea dreptului pretins sau a interesului legitim și repararea pagubei ce i-a fost cauzată. Interesul legitim poate fi atât privat, cât și public. (2) Se poate adresa instanței de contencios administrativ și persoana vătămată într-un drept al său sau într-un interes legitim printr-un act administrativ cu caracter individual, adresat altui subiect de drept.	
	Măsurile de asigurare a respectării legii prevăzute la prezentul alineat nu se aplică	Art. 49 alin. (3)	(3) Măsurile prevăzute la alin. (1) nu se aplică entităților din administrația publică care intră în domeniul de	

	entităților administrației publice care intră în domeniul de aplicare al prezentei directive.		aplicare al prezentei ordonanțe de urgență.	
	(6) Statele membre se asigură că orice persoană fizică responsabilă de o entitate esențială sau care acționează în calitate de reprezentant legal al unei entități esențiale pe baza competenței de a o reprezenta, a autorității de a lua decizii în numele acesteia sau a autorității de a exercita controlul asupra acesteia are competența de a se asigura că aceasta respectă prezenta directivă. Statele membre se asigură că aceste persoane fizice pot fi trase la răspundere pentru încălcarea obligațiilor care le revin de a asigura respectarea prezentei directive.	Art. 14 Art. 50 Art. 60	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 și, după caz, a dispozițiilor ordinului prevăzut la art. 37 alin. (8) lit. b), 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. Art. 50 (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. (4) Adunarea generală a acționarilor nu este organ de conducere a entităților esențiale și importante în înțelesul prezentei ordonanțe de urgență. Art. 60 (1) Următoarele fapte constituie contravenții dacă nu au fost săvârșite în astfel de condiții încât să fie considerate infracțiuni potrivit legii: (...) 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);	
	În ceea ce privește entitățile administrației publice, prezentul alineat nu aduce atingere dreptului intern în ceea ce privește răspunderea funcționarilor publici și a funcționarilor aleși sau numiți.	Art. 14 alin. (1)	(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 și, după caz, a dispozițiilor ordinului prevăzut la art. 37 alin. (8) lit. b), 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.	
	(7) Atunci când iau oricare dintre măsurile de asigurare a respectării legii menționate la alineatul (4) sau (5), autoritățile competente respectă dreptul la apărare, iau în considerare circumstanțele fiecărui caz în parte și țin seama în mod corespunzător cel puțin de:	Art. 50 alin. (1)	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;	Constituția României republicată: Articolul 24 (1) Dreptul la apărare este garantat. (2) În tot cursul procesului, părțile au dreptul să fie asistate de un avocat, ales sau numit din oficiu.

		Art. 61 alin. (8)	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. Art. 61 (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.	
	a) gravitatea încălcării și importanța dispozițiilor încălcate, următoarele fiind considerate, printre altele, încălcări grave în orice situație: i.încălcări repetate; ii.o neîndeplinire a obligației de notificare sau de remediere a incidentelor semnificative; iii.o neremediere a deficiențelor în urma instrucțiunilor obligatorii din partea autorităților competente; iv.obstrucționarea auditurilor sau a activităților de monitorizare dispuse de autoritatea	Art. 50 alin. (2)	(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;	

	competentă în urma constatării unei încălcări; v. furnizarea de informații false sau vădit denaturate în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate cibernetică sau obligațiile de raportare prevăzute la articolele 21 și 23;		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. 11-14 sau obligațiile de raportare prevăzute la art. 15; 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).	
	b) durata încălcării	Art. 50 alin. (1) lit. a)	(1) Stabilirea măsurilor prevăzute la art. 48-49 se face cu evaluarea a cel puțin: a) durata faptei;	
	c) orice încălcare anterioară relevantă comisă de entitatea în cauză;	Art. 50 alin. (1) lit. b)	(1) Stabilirea măsurilor prevăzute la art. 48-49 se face cu evaluarea a cel puțin: (...) b) existența unei abateri anterioare relevante;	
	d) orice prejudicii materiale sau morale cauzate, inclusiv pierderile financiare sau economice, efectele asupra altor servicii și numărul de utilizatori afectați;	Art. 50 alin. (1) lit. c)	(1) Stabilirea măsurilor prevăzute la art. 48-49 se face cu evaluarea a cel puțin: (...) c) prejudiciile materiale sau non-materiale cauzate prin faptă;	
	e) orice intenție sau neglijență din partea autorului încălcării;	Art. 21 alin. 3 din OG 2 din 12 iulie 2001 privind regimul juridic al contravențiilor	(3) Sancțiunea se aplică în limitele prevăzute de actul normativ și trebuie să fie proporțională cu gradul de pericol social al faptei săvârșite, ținându-se seama de împrejurările în care a fost săvârșită fapta, de modul și mijloacele de săvârșire a acesteia, de scopul urmărit, de urmarea produsă, precum și de circumstanțele personale ale contravenientului și de celelalte date înscrise în procesul-verbal.	
	f) orice măsuri luate de entitate pentru a preveni sau a atenua prejudiciile materiale sau morale;	Art. 50 alin. (1) lit. d)	(1) Stabilirea măsurilor prevăzute la art. 48-49 se face cu evaluarea a cel puțin: (...)	

			d) măsurile adoptate de entitate în vederea prevenirii sau remedierii efectelor faptei;	
	g) orice aderare la coduri de conduită aprobate sau la mecanisme de certificare aprobate;	Art. 50 alin. (1) lit. e)	(1) Stabilirea măsurilor prevăzute la art. 48-49 se face cu evaluarea a cel puțin: (...) e) conduita entității în raport cu mecanismele de certificare la care a aderat sau codurile de conduită asumate;	
	h) măsura în care persoanele fizice sau juridice declarate responsabile cooperează cu autoritățile competente.	Art. 50 alin. (1) lit. f)	(1) Stabilirea măsurilor prevăzute la art. 48-49 se face cu evaluarea a cel puțin: (...) f) conduita persoanelor responsabile în raport cu autoritățile competente.	
	(8) Autoritățile competente prezintă o motivare detaliată a măsurilor lor de asigurare a respectării legii. Înainte de a adopta astfel de măsuri, autoritățile competente notifică entităților în cauză constatările lor preliminare. De asemenea, acestea acordă entităților respective un termen rezonabil să prezinte observații, cu excepția cazurilor justificate în mod corespunzător, când ar fi împiedicată o acțiune imediată pentru a preveni sau răspunde la incidente.	Art. 47 alin. (3) - (4)	(3) În cazul în care prin nota de constatare 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.	
	(9) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive informează autoritățile competente relevante din același stat membru în temeiul Directivei (UE) 2022/2557 atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea de către o	Art. 51	(1) DNSC sau, după caz, autoritatea competentă sectorial informează CNCPIC atunci când își exercită competențele de supraveghere și control asupra unei entități esențiale identificate drept entitate critică în	

	entitate identificată ca fiind entitate critică în temeiul Directivei (UE) 2022/2557 a prezentei directive. După caz, autoritățile competente în temeiul Directivei (UE) 2022/2557 pot solicita autorităților competente în temeiul prezentei directive să își exercite competențele de supraveghere și de asigurare a respectării legii în legătură cu o entitate care este identificată ca fiind entitate critică în temeiul Directivei (UE) 2022/2557.		conformitate cu dispozițiile legale privind reziliența entităților critice. (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 legale privind reziliența entităților critice.	
	(10) Statele membre se asigură că autoritățile lor competente în temeiul prezentei directive cooperează cu autoritățile competente relevante din statul membru în cauză în temeiul Regulamentului (UE) 2022/2554. În special, statele membre se asigură că autoritățile lor competente în temeiul prezentei directive informează Forumul de supraveghere instituit în temeiul articolului 32 alineatul (1) din Regulamentul (UE) 2022/2554 atunci când își exercită competențele de supraveghere și de asigurare a respectării legii menite să asigure respectarea prezentei directive de către o entitate esențială, care este desemnată ca fiind un furnizor terț de servicii TIC critice în temeiul articolului 31 din Regulamentul (UE) 2022/ 2554.	Art. 37 alin. (3)	(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 eficace şi rapide.	
Art. 33	(1) Atunci când li se furnizează dovezi, indicii sau informaţii că o entitate importantă nu ar respecta prezenta directivă, în special articolele 21 şi 23, statele membre se asigură că autorităţile competente iau măsuri, dacă este necesar, prin intermediul unor măsuri de supraveghere ex post. Statele membre se asigură că aceste măsuri sunt efective, proporţionale şi cu efect de descurajare, ţinând seama de circumstanţele fiecărui caz în parte.	Art. 46 alin. (2) si (4) Art. 21 alin. 3 din OG 2 din 12 iulie 2001 privind regimul juridic al contravenţiilor	(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 şi control sau în următoarele cazuri, fără a fi limitate la acestea: a) unui incident semnificativ; b) indiciilor temeinice cu privire la încălcarea dispoziţiilor prezentei ordonanţe de urgenţă de către o entitate. (4) În cazul entităţilor importante, supravegherea conform alin. (1) lit. a) se realizează doar pentru punerea în aplicare a art. 48 alin. (2) lit. b)-g). (3) Sancţiunea se aplică în limitele prevăzute de actul normativ şi trebuie să fie proporţională cu gradul de pericol social al faptei săvârşite, ţinându-se seama de împrejurările în care a fost săvârşită fapta, de modul şi mijloacele de săvârşire a acesteia, de scopul urmărit, de urmarea produsă, precum şi de circumstanţele personale ale contravenientului şi de celelalte date înscrise în procesul-verbal.	
	(2) Statele membre se asigură că autorităţile competente, atunci când îşi exercită sarcinile de supraveghere în ceea ce priveşte entităţile importante, au competenţa de a supune entităţile respective cel puţin:			
	a) unor inspecţii la faţa locului şi unei supravegheri ex situ ex post realizate de profesionişti cu formare corespunzătoare;	Art. 24 alin. (3) si (4)	Art. 24 (3) În vederea îndeplinirii atribuţiilor ce îi revin în temeiul prevederilor prezentei ordonanţe de urgenţă, DNSC se asigură că deţine personal suficient şi competent şi că dispune de resurse	

		Art. 46 alin. (1) lit. a) si (4) Art. 48 alin. (2) lit. b) - g) Art. 50 alin. (3)	adecvate pentru a-şi îndeplini în mod eficace şi eficient atribuţiile. (4) Pentru aplicarea alin. (3), din bugetul DNSC se asigură, cu respectarea prevederilor legale, următoarele categorii de cheltuieli: (...) d) cursuri de formare şi perfecţionare precum şi certificări ale personalului propriu; Art. 46 (1) În scopul asigurării respectării dispoziţiilor prezentei ordonanţe de urgenţă, precum şi a actelor normative subsecvente de către entităţi, DNSC, poate: a) derula activităţi de supraveghere, verificare şi control efectuate de persoane desemnate în acest sens prin decizie a Directorului DNSC; (4) În cazul entităţilor importante, supravegherea conform alin. (1) lit. a) se realizează doar pentru punerea în aplicare a art. 48 alin. (2) lit. b)-g). Art. 48 (2) DNSC poate dispune, după caz, următoarele: (...) b) remedierea deficienţelor identificate în aplicarea lit. a); c) încetarea conduitei entităţilor prin care încalcă dispoziţiile prezentei ordonanţe de urgenţă; 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 esenţială în cauză a dispoziţiilor art. 11-14;	

			f) respectarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică prevăzute la art. 11-14 şi a obligaţiilor de raportare prevăzute la art. 15, într-o anumită modalitate şi într-un interval de timp; g) ca încălcările dispoziţiilor prezentei ordonanţe de urgenţă să fie făcute publice de către entitatea responsabilă. Art. 50 (3) Organele de conducere ale entităţii răspund pentru permiterea accesului personalului, desemnat în acest sens de către DNSC, în spaţiile supuse controlului, cât şi asupra datelor şi informaţiilor necesare controlului.	
	b) unor audituri de securitate specifice efectuate de un organism independent sau de o autoritate competentă;	Art. 11 alin. (5) si (6) Art. 46 alin. (1) Art. 57 alin. (1) lit. a) si (7)	Art. 11 (5) Entităţile esenţiale şi entităţile importante sunt obligate să se supună efectuării unui audit de securitate cibernetică în condiţiile şi cu periodicitatea stabilite prin ordinul Directorului DNSC prevăzut la art. 12 alin. (1), în funcţie de nivelul de risc prevăzut la alin. (3). (6) Atunci când există autoritatea cu competenţe sectoriale, condiţiile şi periodicitatea auditului de securitate prevăzute la alin. (5) vor fi stabilite prin ordin comun în condiţiile art. 37 alin. (8) lit. b), în funcţie de nivelul de risc prevăzut la alin. (3). Art. 46 (1) În scopul asigurării respectării dispoziţiilor prezentei ordonanţe de urgenţă, precum şi a actelor normative subsecvente de către entităţi, DNSC, poate: (...)	Oportunitatea şi necesitatea introducerii acestor prevederi şi cu privire la entităţile importante ţine de atributul iniţiatorului care este singurul în măsură să poată aprecia realităţile societale în domeniul securităţii cibernetice româneşti pe acest subiec, ţinând seama şi de bune practici şi de lecţii învăţate nis 1.

		Art. 58 alin. (1)	b) dispune efectuarea de audituri de securitate ad-hoc, realizate de un auditor de securitate cibernetică atestat; Art. 57 (1) Auditul de securitate cibernetică poate fi: a) periodic, care se desfăşoară cu regularitate, conform ordinului de la art. 11 alin. (5) sau, după caz, alin. (6); (7) Cu ocazia desfăşurării auditului de securitate cibernetică periodic, se realizează o evaluare sistematică a tuturor politicilor, procedurilor şi măsurilor de protecţie implementate la nivelul unor reţele şi sisteme informatice, în vederea identificării disfuncţionalităţilor şi vulnerabilităţilor şi recomandării măsurilor de remediere a acestora. Art. 58 (1) Auditul de securitate cibernetică se realizează de către auditorii de securitate cibernetică ce deţin atestat valabil eliberat de către DNSC, cu excepţia auditului de securitate cibernetică realizat la nivelul instituţiilor cu responsabilităţi în domeniul apărării, ordinii publice şi securităţii naţionale, precum şi pentru serviciile puse la dispoziţie de către acestea.	
	c) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile şi transparente de evaluare a riscurilor, după caz cu cooperarea entităţii în cauză;	Art. 46 alin. (5)	(5) În vederea punerii în aplicare a alin. (1) lit. a) cu privire la entităţile esenţiale şi entităţile importante, DNSC poate efectua scanări de securitate cibernetică neintruzive şi proactive, bazate pe criterii obiective, nediscriminatorii, echitabile şi transparente pentru evaluarea riscurilor, cu notificarea prealabilă a entităţii în	

			cauză şi, după caz, în cooperare cu aceasta.	
	d) unor cereri de informaţii necesare pentru a evalua, ex post, măsurile de gestionare a riscurilor în materie de securitate cibernetică adoptate de entitatea în cauză, inclusiv politicile de securitate cibernetică documentate, precum şi respectarea obligaţiei de a transmite informaţii autorităţilor competente în temeiul articolului 27;	Art. 46 alin. (1) lit. c)	(1) În scopul asigurării respectării dispoziţiilor prezentei ordonanţe de urgenţă, precum şi a actelor normative subsecvente de către entităţi, DNSC, poate: (...) c) solicita informaţii 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 şi respectarea obligaţiei de a transmite informaţii către DNSC în temeiul art. 18;	
	e) unor cereri de acces la date, la documente şi la informaţii necesare pentru îndeplinirea sarcinilor lor de supraveghere;	Art. 46 alin. (1) lit. d)	(1) În scopul asigurării respectării dispoziţiilor prezentei ordonanţe de urgenţă, precum şi a actelor normative subsecvente de către entităţi, DNSC, poate: (...) d) solicita acces la date, la documente şi la orice informaţii necesare pentru îndeplinirea sarcinilor lor de supraveghere;	
	f) unor cereri de dovezi privind punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat şi mijloacele de probă care stau la baza acestora.	Art. 46 alin. (1) lit. e)	(1) În scopul asigurării respectării dispoziţiilor prezentei ordonanţe de urgenţă, precum şi a actelor normative subsecvente de către entităţi, DNSC, poate: (...) e) solicita date, documente şi orice informaţii 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 şi mijloacele de probă care stau la baza acestora.	
	Auditurile de securitate specifice, menţionate la primul paragraf litera (b), se bazează pe evaluări ale riscurilor efectuate de autoritatea competentă	Art. 11 alin. (1) - (6)	(1) Entităţile esenţiale şi entităţile importante iau măsuri tehnice, operaţionale şi organizatorice proporţionale şi adecvate pentru a	

	sau de entitatea auditată sau pe alte informații disponibile legate de riscuri.		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).	
	Rezultatele oricărui audit de securitate specific se pun la dispoziția autorității competente. Costurile unui astfel de audit de securitate specific efectuat de un organism independent sunt plătite de entitatea auditată, în afara cazurilor justificate corespunzător, atunci când autoritatea competentă decide altfel.	Art. 46 alin. (8) si (9)	(8) În termen de cel mult 5 zile de la finalizarea oricărui audit de securitate cibernetică, entitatea auditată transmite către DNSC și, după caz, autorității competente sectorial, rezultatele acestuia. (9) Costurile generate de auditul de securitate cibernetică, inclusiv cel ad-hoc, sunt suportate de către entitatea auditată.	
	(3) Atunci când își exercită competențele în temeiul alineatului (2) literele (d), (e) sau (f), autoritățile competente precizează scopul solicitării și informațiile solicitate.	Art. 47 alin. (1)	(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.	
	(4) Statele membre se asigură că, atunci când își exercită sarcinile de asigurare a respectării legii în ceea ce privește entitățile importante, autoritățile competente au competența cel puțin:			
	a) de a emite avertismente cu privire la încălcări ale prezentei directive de către entitățile în cauză;	Art. 48 alin. (1) lit. a)	(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) de a adopta instrucțiuni obligatorii sau un ordin prin care le solicită entităților în cauză să remedieze deficiențele identificate sau încălcarea prezentei directive;	Art. 48 alin. (2) lit. a)	(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;	
	c) de a dispune ca entitățile în cauză să înceteze conduita prin care încalcă prezenta directivă și să se abțină de la repetarea conduitei respective;	Art. 48 alin. (2) lit. c)	(2) DNSC poate dispune, după caz, următoarele: (...) c) încetarea conduitei entităților prin care încalcă dispozițiile prezentei ordonanțe de urgență;	
	d) de a dispune ca entitățile în cauză să asigure că măsurile lor de gestionare a riscurilor în materie de securitate cibernetică respectă dispozițiile de la articolul 21 sau să îndeplinească obligațiile de raportare prevăzute la articolul 23, într-un anumit mod și într-o anumită perioadă;	Art. 48 alin. (2) lit. f)	(2) DNSC poate dispune, după caz, următoarele: (...) 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;	
	e) de a dispune ca entitățile în cauză să informeze persoanele fizice sau juridice cu privire la care furnizează servicii sau desfășoară activități care sunt potențial afectate de o amenințare cibernetică semnificativă cu privire la caracterul amenințării, precum și cu privire la toate măsurile de protecție sau de remediere pe care le-ar putea lua persoanele fizice sau juridice în cauză ca răspuns la amenințarea respectivă;	Art. 48 alin. (4)	(4) DNSC poate dispune entităților să informeze, într-un termen anume determinat, persoanele cărora le prestează un serviciu sau cu care desfășoară activități, 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.	
	f) de a dispune ca entitățile în cauză să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil	Art. 48 alin. (2) lit. d) Art. 57 alin. (8)	Art. 48 (2) DNSC poate dispune, după caz, următoarele: (...) d) punerea în aplicare a recomandărilor formulate ca urmare a unui audit de securitate; Art. 57 (8) În cel mult 15 zile lucrătoare de la data primirii raportului de audit, entitățile sunt obligate să întocmească și să transmită către DNSC și, după caz, autorității competente sectorial, în	

			baza recomandărilor emise de către auditor, planul de măsuri pentru remedierea tuturor deficienţelor constatate şi termenele asumate pentru implementarea acestora.	
	g) de a dispune ca entităţile în cauză să facă publice într-un mod specific aspectele legate de încălcările prezentei directive;	Art. 48 alin. (2) lit. g)	(2) DNSC poate dispune, după caz, următoarele: (...) g) ca încălcările dispoziţiilor prezentei ordonanţe de urgenţă să fie făcute publice de către entitatea responsabilă.	
	h) de a aplica sau a solicita aplicarea de către organismele sau instanţele relevante, în conformitate cu dreptul intern, a unei amenzi administrative în temeiul articolului 34, în plus faţă de oricare dintre măsurile menţionate la literele (a)-(g) de la prezentul alineat.	Art. 48 alin. (1) lit. b)	(1) În vederea îndeplinirii atribuţiilor care îi revin, precum şi pentru asigurarea respectării dispoziţiilor prezentei ordonanţe de urgenţă de către entităţi, DNSC aplică următoarele sancţiuni: (...) b) amendă contravenţională.	
	(5) Articolul 32 alineatele (6), (7) şi (8) se aplică, mutatis mutandis, măsurilor de supraveghere şi de asigurare a respectării legii prevăzute în prezentul articol pentru entităţile importante.	Art. 7 alin. (6) si (7) Art. 14 alin. (1) Art. 50 alin. (1) si (2)	Art. 7 (6) Atunci când, în situaţia 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 îşi prestează serviciile. În acest caz, entitatea se consideră a fi sub jurisdicţia statului membru în care este stabilit reprezentantul. (7) Atunci când entitatea prestează servicii pe teritoriul României, DNSC poate introduce acţiuni în justiţie conform prevederilor legale împotriva entităţii în cauză pentru nerespectarea prevederilor prezentei ordonanţe de urgenţă, inclusiv în cazul în care entitatea nu a desemnat un reprezentant conform alin. (6). Art. 14 (1) Organele de conducere ale entităţilor esenţiale şi ale entităţilor	

		Art. 47 alin. (2) si (3)	importante aprobă măsurile de gestionare a riscurilor de securitate cibernetică pe care le iau în vederea respectării art. 11-13 şi, după caz, a dispoziţiilor ordinului prevăzut la art. 37 alin. (8) lit. b), supraveghează punerea acestora în aplicare şi sunt responsabile de încălcările acestor dispoziţii, fără a aduce atingere dispoziţiilor legale privind răspunderea instituţiilor publice, a funcţionarilor publici şi a celor aleşi sau numiţi. Art. 50 (1) Stabilirea măsurilor prevăzute la art. 48-49 se face cu evaluarea a cel puţin: a) durata faptei; b) existenţa 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 entităţii în raport cu mecanismele de certificare la care a aderat sau codurile de conduită asumate; f) conduita persoanelor responsabile în raport cu autorităţile competente. (2) Următoarele fapte constituie încălcări grave: a) încălcări repetate; b) neîndeplinirea obligaţiei de notificare sau de remediere a incidentelor semnificative; c) neîndeplinirea obligaţiei de remediere a deficienţelor constatate de către autorităţile competente; d) obstrucţionarea auditurilor sau a activităţii de monitorizare dispuse de DNSC în urma constatărilor; e) furnizarea de informaţii false sau vădit denaturate în ceea ce priveşte	

			măsurile de gestionare a riscurilor în materie de securitate cibernetică prevăzute la art. 12 şi art. 13 sau obligaţiile de raportare prevăzute la art. 17; f) îngrădirea accesului personalului desemnat în acest sens de către DNSC în spaţiile supuse controlului, cât şi asupra datelor şi informaţiilor necesare controlului; g) nerespectarea dispoziţiilor DNSC emise în temeiul art. 48 alin. (2). Art. 47 (2) Constatările urmare a îndeplinirii activităţilor de supraveghere, verificare şi control prevăzute la art. 46 alin. (1) sunt consemnate de personalul de control desemnat în nota de constatare. (3) În cazul în care prin nota de constatare prevăzută la alin. (2) sunt reţinute fapte care ar putea constitui una dintre contravenţiile prevăzute la art. 60, nota de constatare se comunică entităţii în cauză pentru a transmite un punct de vedere cu privire la deficienţele constatate, solicitându-se, dacă este cazul, un plan de măsuri pentru remedierea acestora.	
	(6) Statele membre se asigură că autorităţile lor competente în temeiul prezentei directive cooperează cu autorităţile competente relevante din statul membru în cauză în temeiul Regulamentului (UE) 2022/2554. În special, statele membre se asigură că autorităţile lor competente în temeiul prezentei directive informează Forumul de supraveghere instituit în temeiul articolului 32 alineatul (1) din Regulamentul (UE) 2022/2554 atunci când îşi exercită competenţele de supraveghere şi de asigurare a respectării legii menite să asigure respectarea prezentei directive de către o entitate	Art. 37 alin. (3)	(3) DNSC cooperează şi colaborează cu Banca Naţională a României, denumită în continuare „BNR" şi Autoritatea de Supraveghere Financiară, denumită în continuare „ASF", pentru evaluarea şi gestionarea riscurilor cibernetice, identificarea vulnerabilităţilor şi implementarea măsurilor de protecţie adecvate entităţilor esenţiale şi entităţilor importante din domeniul bancar şi al infrastructurilor pieţei financiare, astfel:	

	importantă, care este desemnată ca fiind un furnizor terț de servicii TIC critice în temeiul articolului 31 din Regulamentul (UE) 2022/2554		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 eficace și rapide.	
Art. 34	(1) Statele membre se asigură că amenzile administrative aplicate entităților esențiale și entităților importante în temeiul prezentului articol în ceea ce privește încălcările prezentei directive sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte.	Art. 48 alin. (1) lit. b) Art. 50 alin. (1) si (2)	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: (...) b) amendă contravențională. 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. 11-14 sau obligațiile de raportare prevăzute la art. 15; 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).	
	(2) Amenzile administrative sunt aplicate în plus față de oricare dintre măsurile menționate la articolul 32 alineatul (4) literele (a)-(h), la articolul 32 alineatul (5) și la articolul 33 alineatul (4) literele (a)-(g).	Art. 48 alin. (1) lit. b) și alin. (2)	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: (...) b) amendă contravențională. (2) DNSC poate dispune, după caz, următoarele:	

		Art. 49	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. 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.	
	(3) Atunci când se ia decizia de a aplica o amendă administrativă și se decide cuantumul acesteia în fiecare caz în parte, se acordă atenția cuvenită cel puțin elementelor prevăzute la articolul 32 alineatul (7).	Art. 50 alin. (1) si (2)	(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. 11-14 sau obligațiile de raportare prevăzute la art. 15; 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).	
	(4) Statele membre se asigură că, atunci când încalcă articolul 21 sau articolul 23, entitățile esențiale sunt supuse, în conformitate cu alineatele (2) și (3) din prezentul articol, unor amenzi administrative având o limită superioară de cel puțin 10 000 000 EUR sau o limită superioară de cel puțin 2 % din cifra de afaceri mondială totală anuală, înregistrată în exercițiul financiar precedent, a întreprinderii căreia îi aparține entitatea esențială, luându-se în considerare valoarea cea mai mare dintre acestea.	Art. 60 alin. (1), (2) lit. b) si (3)	(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 în condițiile stabilite conform art. 11 alin. (5) sau, după caz, alin. (6) și în termenul indicat; c) nerespectarea de către entitățile esențiale și importante a obligației de a transmite datele solicitate conform art.	

			11 alin. (7) în termenul şi în condiţiile stabilite în cerere; d) nerespectarea de către entităţile esenţiale şi importante a obligaţiei de a transmite datele solicitate conform art. 11 alin. (9) în termenul şi în condiţiile stabilite în cerere; e) nerespectarea de către entităţile esenţiale şi importante a obligaţiei de a realiza şi transmite autoevaluarea nivelului de maturitate conform art. 12 alin. (4); f) nerespectarea de către entităţile esenţiale a obligaţiei de a întocmi şi transmite planul de măsuri pentru remedierea deficienţelor conform art. 12 alin. (5), în termen de 30 de zile de la realizarea autoevaluării; (2) Prin derogare de la dispoziţiile art. 8 alin. (2) lit. a) din Ordonanţa Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, cu modificările şi completările ulterioare, sancţiunile sunt: (...) b) pentru entităţile esenţiale până la 10 000 000 euro în echivalentul în lei sau cel mult 2% din cifra de afaceri netă, luându-se în considerare valoarea cea mai mare dintre acestea, în situaţia alin. (1) lit. a)-m), dd), jj) şi mm); (3) Cifra de afaceri netă prevăzută la alin. (2) este cea înregistrată de către entitatea importantă sau esenţială în ultimul exerciţiu financiar.	
	(5) Statele membre se asigură că, atunci când încalcă articolul 21 sau articolul 23, entităţile importante sunt supuse, în conformitate cu alineatele (2) şi (3) din prezentul articol, unor amenzi administrative având o limită superioară de cel puţin 7 000 000 EUR sau având o limită superioară de cel puţin 1,4 % din cifra de afaceri mondială totală anuală, înregistrată în exerciţiul	Art. 60 alin. (1), alin. (2) lit. a) si (3)	(1) Următoarele fapte constituie contravenţii dacă nu au fost săvârşite în astfel de condiţii încât să fie considerate infracţiuni potrivit legii: g) nerespectarea de către organele de conducere ale entităţilor esenţiale şi importante a obligaţiei de supraveghere a punerii în aplicare a măsurilor de	

	financiar precedent, a întreprinderii căreia îi aparţine entitatea importantă, luându-se în considerare valoarea cea mai mare dintre acestea.		gestionare a riscurilor conform art. 14 alin. (1); h) nerespectarea de către membrii organelor de conducere ale entităţilor esenţiale şi importante a obligaţiei de a urma cursuri de formare profesională conform cu art. 14 alin. (2); i) nerespectarea de către organele de conducere ale entităţilor esenţiale şi importante a obligaţiei de stabilire a mijloacelor permanente de contact conform art. 14 alin. (3); j) nerespectarea de către organele de conducere ale entităţilor esenţiale şi importante a obligaţiei de alocare a resurselor conform art. 14 alin. (3); k) nerespectarea de către organele de conducere ale entităţilor esenţiale şi importante a obligaţiei de desemnare a responsabililor cu securitatea reţelelor şi sistemelor informatice conform art. 14 alin. (3); l) nerespectarea de către entităţile esenţiale şi importante a obligaţiei de raportare în temeiul art. 15 alin. (1) cu respectarea termenelor şi condiţiilor stabilite conform art. 15; (2) Prin derogare de la dispoziţiile art. 8 alin. (2) lit. a) din Ordonanţa Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, cu modificările şi completările ulterioare, sancţiunile sunt: a) pentru entităţile importante până la 7 000 000 euro în echivalentul în lei sau cel mult 1,4% din cifra de afaceri netă, luându-se în considerare valoarea cea mai mare dintre acestea, în situaţia alin. (1) lit. a)-d), f)-m), dd), jj) şi mm); (3) Cifra de afaceri netă prevăzută la alin. (2) este cea înregistrată de către entitatea importantă sau esenţială în ultimul exerciţiu financiar.	

	(6) Statele membre pot prevedea competența de a aplica penalități cu titlu cominatoriu pentru a obliga o entitate esențială sau o entitate importantă să înceteze o încălcare a prezentei directive în conformitate cu o decizie prealabilă a autorității competente.			Nu s-a apreciat necesară transpunerea.
	(7) Fără a aduce atingere competențelor autorităților competente menționate la articolele 32 și 33, fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi aplicate amenzi administrative entităților administrației publice cărora le revin obligațiile prevăzute în prezenta directivă. (8) În cazul în care sistemul juridic al unui stat membru nu prevede amenzi administrative, statul membru respectiv se asigură că prezentul articol este aplicat astfel încât amenda să fie inițiată de autoritatea competentă și aplicată de instanțele naționale competente, garantându-se, în același timp, faptul că aceste căi de atac sunt eficiente și că au un efect echivalent cu cel al amenzilor administrative aplicate de autoritățile competente. În orice caz, amenzile aplicate sunt efective, proporționale și cu efect de descurajare. Statele membre informează Comisia cu privire la dispozițiile de drept intern pe care le adoptă în temeiul prezentului alineat până la 17 octombrie 2024, precum și, fără întârziere, cu privire la orice act legislativ de modificare sau orice modificare ulterioară a acestora.	Art. 46	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	Regimul sancționator se aplică și în cazul entităților din administrația publică ce fac obiectul prezentei ordonanțe.

		Art. 48	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 legale privind reziliența entităților critice. (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 entitățille 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 în condițiile prevăzute la art. 11 alin. (5) sau, după caz, alin. (6), se realizează o evaluare	

		Art. 49	sistematică a tuturor politicilor, procedurilor şi măsurilor de protecţie implementate la nivelul unor reţele şi sisteme informatice, în vederea identificării disfuncţionalităţilor şi vulnerabilităţilor şi 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 şi, după caz, autorităţii competente sectorial, rezultatele acestuia. (9) Costurile generate de auditul de securitate cibernetică, inclusiv cel ad-hoc, sunt suportate de către entitatea auditată.	
		Art. 61	Art. 48 (1) În vederea îndeplinirii atribuţiilor care îi revin, precum şi pentru asigurarea respectării dispoziţiilor prezentei ordonanţe de urgenţă de către entităţi, DNSC aplică următoarele sancţiuni: a) avertisment; b) amendă contravenţională. (2) DNSC poate dispune, după caz, următoarele: a) adoptarea unor măsuri atunci când acestea sunt necesare pentru a preveni sau remedia un incident, precum şi termene limită pentru punerea în aplicare a acestor măsuri, inclusiv a unui audit ad-hoc; b) remedierea deficienţelor identificate în aplicarea lit. a); c) încetarea conduitei entităţilor prin care încalcă dispoziţiile prezentei ordonanţe de urgenţă; 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 sau cu care desfășoară activități, 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. 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) lit. a)-n), ee), ff), jj)-oo) se realizează de către DNSC sau de către personalul de	

			control al autorităților competente sectorial conform art. 37 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). Constatarea contravențiilor prevăzute la art. 60 alin. (1) lit. o)-dd), gg)-ii) se realizează de către DNSC, aplicarea sancțiunii realizându-se prin decizie a Directorului DNSC. (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 acţiuni sau inacţiuni, care prezintă, fiecare în parte, conţinutul aceleiaşi contravenţii, prescripţia începe să curgă de la data constatării sau de la data încetării ultimului act ori fapt săvârşit, dacă acest moment intervine anterior constatării. (5) Contravenientului i se comunică şi înştiinţarea de plată, care conţine menţiunea privind obligativitatea achitării amenzii în termen de 30 de zile de la data comunicării actului. (6) Decizia de constatare a contravenţiei şi de aplicare a sancţiunii prevăzută la alin. (2) şi (3), neatacată în termenul prevăzut la alin. (8), precum şi hotărârea judecătorească definitivă prin care s-a soluţionat acţiunea în contencios administrativ constituie titlu executoriu, fără vreo altă formalitate. Acţiunea în contencios administrativ în condiţiile prevăzute la alin. (8) suspendă executarea numai în ceea ce priveşte achitarea amenzii, până la pronunţarea de către instanţa de judecată a unei hotărâri definitive. (7) Sumele provenite din amenzile aplicate în conformitate cu dispoziţiile prezentului articol se fac venit integral la bugetul de stat. Executarea se realizează în conformitate cu dispoziţiile legale privind executarea silită a creanţelor fiscale. În vederea punerii în executare a sancţiunii, DNSC şi autorităţile competente sectorial prevăzute la art. 37, comunică, din oficiu, organelor de specialitate ale Agenţiei Naţionale de Administrare Fiscală, decizia de constatare a contravenţiei şi de aplicare a sancţiunii prevăzută la alin. (2) sau (3), neatacată în termenul prevăzut la alin. (8), după	

			expirarea termenului prevăzut în înştiinţarea de plată sau după rămânerea definitivă a hotărârii judecătoreşti prin care s-a soluţionat acţiunea în contencios administrativ. (8) Prin derogare de la dispoziţiile art. 7 din Legea contenciosului administrativ nr. 554/2004, cu modificările şi completările ulterioare şi de la dispoziţiile art. 32 alin. (1) din OG nr. 2/2001, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, actele administrative, deciziile şi deciziile de constatare a contravenţiei şi de aplicare a sancţiunii adoptate potrivit dispoziţiilor prezentei ordonanţe de urgenţă pot fi atacate în contencios administrativ la Curtea de Apel Bucureşti, fără parcurgerea procedurii prealabile, în termen de 30 de zile de la comunicarea acestora.	

Art. 35	(1) În cazul în care, în cursul supravegherii sau al asigurării respectării legii, autoritățile competente iau cunoștință de faptul că încălcarea de către o entitate esențială sau de către o entitate importantă a obligațiilor prevăzute la articolele 21 și 23 din prezenta directivă poate atrage după sine o încălcare a securității datelor cu caracter personal, astfel cum este definită la articolul 4 alineatul (12) din Regulamentul (UE) 2016/679, care trebuie notificată în temeiul articolului 33 din regulamentul respectiv, acestea informează fără întârzieri nejustificate autoritățile de supraveghere menționate la articolele 55 sau 56 din regulamentul respectiv. (2) În cazul în care autoritățile de supraveghere menționate la articolele 55 sau 56 din Regulamentul (UE) 2016/679 aplică o amendă administrativă în temeiul articolului 58 alineatul (2) litera (i) din regulamentul respectiv, autoritățile competente nu aplică o amendă administrativă în conformitate cu articolul 34 din prezenta directivă pentru o încălcare menționată la alineatul (1) din prezentul articol rezultată în urma aceluiași comportament care a făcut obiectul amenzii administrative în temeiul articolului 58 alineatul (2) litera (i) din Regulamentul (UE) 2016/679. Cu toate acestea, autoritățile competente pot aplica măsurile de asigurare a respectării legii prevăzute la articolul 32 alineatul (4) literele (a)- (h), la articolul 32 alineatul (5) și la articolul 33 alineatul (4) literele (a)-(g) din prezenta directivă. (3) În cazul în care autoritatea de supraveghere competentă în temeiul Regulamentului (UE) 2016/679 este stabilită într-un alt stat membru decât autoritatea competentă, autoritatea competentă informează autoritatea de supraveghere stabilită în statul său membru cu privire la potențiala încălcare a securității datelor menționată la alineatul (1).	Art. 37 alin. (4) Art. 62	Art. 37 (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. Art. 62 (1) DNSC informează, fără întârzieri nejustificate, 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 domeniul protecției datelor cu caracter personal cu privire la care s-a efectuat sau se efectuează o investigație 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.	ANSPDCP este autoritatea națională în domeniu și desemnată să aplice Regulamentul (UE) 2016/679, astfel încât menționarea acestora este redundantă. Cu privire la aplicarea prezentei și aplicarea Regulamentului (UE) 2016/679 complementar, precizăm faptul că regimul sancționator permite aplicarea unor accesorii doar pe lângă o sancțiune principală, astfel încât nu pot fi cumulate sancțiunea aplicată de către ANSPDCP concurent cu o sancțiune aplicată de orice altă autoritate pentru aceeași faptă. Cu toate acestea, măsurile ce trebuie aplicate imediat de către o entitate în vederea gestionării unui incident, spre exemplu, nu au caracter sancționator și pot fi aplicate indiferent de aceasta.

Art. 36	Statele membre adoptă normele privind sancțiunile care se aplică în cazul nerespectării măsurilor naționale adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a asigura aplicarea acestora. Sancțiunile trebuie să fie efective, proporționale și cu efect de descurajare. Statele membre notifică aceste norme și aceste măsuri Comisiei până la 17 ianuarie 2025 și notifică acesteia, fără întârziere, orice modificare ulterioară a acestora.	Art. 48 alin. (1) - (3) Art. 49 alin. (1) si (3) Art. 60	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). 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. (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. 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 în condițiile stabilite conform art. 11 alin. (5) sau, după caz, alin. (6) și în termenul indicat; c) nerespectarea de către entitățile esențiale și importante a obligației de a transmite datele solicitate conform art. 11 alin. (7) în termenul și în condițiile stabilite în cerere; d) nerespectarea de către entitățile esențiale și importante a obligației de a transmite datele solicitate conform art. 11 alin. (9) în termenul și în condițiile stabilite în cerere; e) nerespectarea de către entitățile esențiale și importante a obligației de a realiza și transmite autoevaluarea nivelului de maturitate conform art. 12 alin. (4); 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 realizarea autoevaluării; 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); l) nerespectarea de către entitățile esențiale și importante a obligației de raportare în temeiul art. 15 alin. (1) cu respectarea termenelor și condițiilor stabilite conform art. 15; m) nerespectarea de către entitățile esențiale și importante a obligației de notificare a destinatarilor serviciilor cu respectarea termenelor și condițiilor stabilite conform art. 15 alin. (1); n) nerespectarea de către entitățile esențiale și importante a obligației de raportare a informațiilor cu respectarea termenelor și condițiilor stabilite conform art. 15 alin. (3); 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, luându-se în considerare valoarea cea mai mare dintre acestea, în situația alin. (1) lit. a)-d), f)-m), dd), jj) și mm); b) pentru entitățile esențiale până la 10 000 000 euro în echivalentul în lei sau cel mult 2% din cifra de afaceri netă, luându-se în considerare valoarea cea mai mare dintre acestea, în situația alin. (1) lit. a)-m), dd), jj) și mm); c) pentru entitățile importante de la 1 000 lei la 300 000 lei, în cazul alin. (1) lit. n)-t), ee)-ff), kk)-ll) și nn)-oo);	

			d) pentru entitățile esențiale de la 1 500 lei la 500 000 lei, în cazul alin. (1) lit. n)-t), ee)-ff), kk)-ll) şi nn)-oo); e) de la 1 000 lei la 100 000 lei, în cazul alin. (1) lit. u)-z), aa)-cc) şi 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 şi pentru persoanele juridice care nu au înregistrat cifra de afaceri în exercițiul financiar anterior sancționării, amenda prevăzută la alin. (2) se stabileşte în cuantum de minimum unu şi 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 şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare. (7) Prin derogare de la prevederile art. 16 alin. (1) şi ale art. 28 alin. (1) din Ordonanța Guvernului nr. 2/2001, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, şi ale art. 22 alin. (2) din Legea nr. 203/2018 privind măsuri de eficientizare a achitării amenzilor	

			contravenţionale, cu modificările ulterioare, în cazul sancţiunilor aplicate pentru săvârşirea contravenţiilor prevăzute la alin. (1), contravenientul poate achita, în termen de cel mult 15 zile de la data înmânării sau comunicării actului de constatare a contravenţiei şi de aplicare a sancţiunii, jumătate din cuantumul amenzii aplicate, agentul constatator făcând menţiune despre această posibilitate în procesul-verbal, respectiv în decizia prin care se aplică sancţiunea.	
Art. 37	(1) Dacă o entitate furnizează servicii în mai multe state membre sau furnizează servicii în unul sau mai multe state membre iar reţeaua şi sistemele sale informatice sunt situate în unul sau mai multe alte state membre, autorităţile competente ale statelor membre în cauză cooperează şi îşi oferă asistenţă reciprocă, după caz. Această cooperare implică cel puţin următoarele: a) autorităţile competente care aplică măsuri de supraveghere sau de asigurare a respectării legii într-un stat membru informează şi consultă, prin intermediul punctului unic de contact, autorităţile competente din celelalte state membre în cauză cu privire la măsurile de supraveghere şi de asigurare a respectării legii luate; b) o autoritate competentă poate solicita unei alte autorităţi competente să ia măsuri de supraveghere sau de asigurare a respectării legii; c) la primirea unei cereri motivate din partea altei autorităţi competente, o autoritate competentă acordă asistenţă reciprocă celeilalte autorităţi competente proporţional cu resursele sale, astfel încât măsurile de supraveghere sau de asigurare a respectării legii să poată fi puse în aplicare într-un mod eficace, eficient şi consecvent.	Art. 45 Art. 40 alin. (1)-(2) lit. a)	Art. 45 (1) Atunci când o entitate înregistrată în România ca entitate esenţială sau importantă furnizează servicii în mai multe state membre sau furnizează servicii în unul sau mai multe state membre iar reţeaua şi sistemele sale informatice sunt situate în unul sau mai multe alte state membre, DNSC cooperează cu celelalte autorităţi competente omoloage de la nivelul Uniunii Europene şi îşi oferă asistenţă reciprocă. (2) În situaţia alin. (1), DNSC poate solicita autorităţilor competente omoloage de la nivelul Uniunii Europene să exercite atribuţii de supraveghere şi control şi, 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 şi România, sau furnizează servicii în unul sau mai multe state membre iar reţeaua şi sistemele sale informatice sunt situate în unul sau mai multe alte state membre, printre care şi România, DNSC cooperează cu celelalte autorităţi competente	

	Asistența reciprocă menționată la primul paragraf litera (c) poate acoperi cererile de informații și măsurile de supraveghere, inclusiv cererile de efectuare a unor inspecții la fața locului, a unei supravegheri ex situ sau a unor audituri de securitate specifice. O autoritate competentă căreia i se adresează o cerere de asistență nu refuză cererea respectivă, cu excepția cazului în care se stabilește că nu are competența de a furniza asistența solicitată, asistența solicitată nu este proporțională cu sarcinile de supraveghere ale autorității competente sau cererea privește informații sau implică activități care, dacă ar fi divulgate sau desfășurate, ar fi contrare intereselor esențiale ale statului membru respectiv în materie de securitate națională, siguranță publică sau apărare. Înainte de a refuza o astfel de cerere, autoritatea competentă consultă celelalte autorități competente în cauză, precum și, la cererea unuia dintre statele membre în cauză, Comisia și ENISA. (2) Dacă este cazul și de comun acord, autorități competente din diferite state membre pot desfășura acțiuni comune de supraveghere.	Art. 25 alin. (1) lit. h)	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. 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, acolo unde este cazul, cu Comisia Europeană, ENISA, Grupul de cooperare și Rețeaua CSIRT; 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: 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;	
Art. 38	(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol. (2) Competența de a adopta acte delegate menționată la articolul 24 alineatul (2) se conferă Comisiei pe o perioadă de cinci ani de la 16 ianuarie 2023. (3) Delegarea de competențe menționată la articolul 24 alineatul (2) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în Jurnalul Oficial al Uniunii Europene sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare. (4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare. (5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului. (6) Un act delegat adoptat în temeiul articolului 24 alineatul (2) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu, sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.			Nu este necesara transpunerea. Prevedere ce abilitează Comisia să adopte acte delegate.

Art. 39	(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011. (2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011. (3) În cazul în care avizul comitetului urmează să fie obținut prin procedură scrisă, respectiva procedură se încheie fără rezultat atunci când, în termenul stabilit pentru emiterea avizului, președintele comitetului decide în acest sens sau un membru al comitetului solicită acest lucru.			Nu este necesară transpunerea. Prevedere aplicabilă Comisiei Europene.
Art. 40	Până la 17 octombrie 2027 și, ulterior, la fiecare 36 de luni, Comisia revizuiește funcționarea prezentei directive și prezintă un raport Parlamentului European și Consiliului. Raportul evaluează în special relevanța dimensiunii entităților vizate și sectoarele, subsectoarele și tipurile de entități menționate în anexele I și II pentru funcționarea economiei și a societății în ceea ce privește securitatea cibernetică. În acest scop și în vederea intensificării cooperării strategice și operaționale, Comisia ține cont de rapoartele Grupului de cooperare și ale rețelei CSIRT privind experiența obținută la nivel strategic și operațional. Raportul este însoțit, după caz, de o propunere legislativă.			Nu este necesară transpunerea. Prevedere aplicabilă Comisiei Europene.
Art. 41	(1) Până la 17 octombrie 2024, statele membre adoptă și publică măsurile necesare pentru a se conforma prezentei directive. Statele membre informează de îndată Comisia cu privire la aceasta. Statele membre aplică măsurile respective de la 18 octombrie 2024 (2) Atunci când statele membre adoptă măsurile menționate la alineatul (1), acestea conțin o trimitere la prezenta		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), publicată în Jurnalul Oficial al Uniunii	

	directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a unei astfel de trimiteri.		Europene (JOUE) nr. L333/80 din 27 decembrie 2022.	
Art. 42	În Regulamentul (UE) nr. 910/2014, articolul 19 se elimină de la 18 octombrie 2024	Art. 6 alin. (2) Anexa 1 pct. 8 Infrastructură digitală - Prestatorii de servicii de încredere	Art. 6 (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: c) prestatorii de servicii de încredere.	Prezenta transpunere asigură măsurile de securitate cibernetică și pentru prestatorii de servicii de încredere, acestora aplicându-li-se prezenta ordonanță ca entități esențiale/importante.
Art. 43	În Directiva (UE) 2018/1972, articolele 40 și 41 se elimină de la 18 octombrie 2024.	Art. 66 lit. b)	La data intrării în vigoare a prezentei ordonanțe de urgență, se abrogă: (...) b) art. 4 alin. (1) pct. 54^1 și 54^2, 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;	
Art. 44	Directiva (UE) 2016/1148 se abrogă de la 18 octombrie 2024. Trimiterile la directiva abrogată se interpretează ca trimiteri la prezenta directivă și se citesc în conformitate cu tabelul de corespondență din anexa III.	Art. 66 lit. a)	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.	

Art. 45	Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene.			Nu este necesara transpunerea
Art. 46	Prezenta directivă se adresează statelor membre.			Nu este necesara transpunerea
Anexa I				
1. Energie a) Electricitate	Întreprinderile din domeniul energiei electrice, astfel cum sunt definite la articolul 2 punctul 57 din Directiva (UE) 2019/944 a Parlamentului European şi a Consiliului(1), care îndeplinesc funcţia de „furnizare", astfel cum este definită la articolul 2 punctul 12 din directiva respectivă		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 şi a gazelor naturale, care îndeplinesc funcţia de „furnizare de energie electrică", astfel cum este definită la art. 3 pct. 46 din Legea nr. 123/2012 a energiei electrice şi a gazelor naturale	
	Operatorii de distribuţie, astfel cum sunt definiţi la articolul 2 punctul 29 din Directiva (UE) 2019/944		Operatorii de distribuţie, astfel cum sunt definiţi la art. 3 pct. 70 din Legea nr. 123/2012 a energiei electrice şi a gazelor naturale	
	Operatorii de transport şi de sistem, astfel cum sunt definiţi la articolul 2 punctul 35 din Directiva (UE) 2019/944		Operatorii de transport şi de sistem, astfel cum sunt definiţi la art. 3 pct. 71 din Legea nr. 123/2012 a energiei electrice şi a gazelor naturale	
	Producătorii, astfel cum sunt definiţi la articolul 2 punctul 38 din Directiva (UE) 2019/944		Producătorii, astfel cum sunt definiţi ca "producători de energie electrică" la art. 3 pct. 92 din Legea nr. 123/2012 a energiei electrice şi a gazelor naturale	
	• Operatorii pieţei de energie electrică desemnaţi, astfel cum sunt definiţi la articolul 2 punctul 8 din Regulamentul (UE) 2019/943 al Parlamentului European şi al Consiliului(2) • Participanţii la piaţă, astfel cum sunt definiţi la articolul 2 punctul 25 din Regulamentul (UE) 2019/943, care furnizează serviciile de agregare, consum dispecerizabil sau stocare de energie, astfel cum sunt definite la articolul 2 punctele 18, 20 şi 59 din Directiva (UE) 2019/944 • Operatorii unui punct de reîncărcare care sunt responsabili cu gestionarea şi exploatarea unui punct de reîncărcare care furnizează un serviciu de reîncărcare utilizatorilor finali,		• Operatorii desemnaţi ai pieţei de energie electrică, astfel cum sunt definiţi la art. 3 pct. 68 din Legea nr. 123/2012 a energiei electrice şi a gazelor naturale • Participanţii la piaţă, astfel cum sunt definiţi la art. 3 pct. 79 din Legea nr. 123/2012 a energiei electrice şi a gazelor naturale, care furnizează serviciile de agregare, consum dispecerizabil sau stocare de energie, astfel cum sunt definite la art. 3 pct. 6, 29 şi respectiv 121 din aceeaşi lege.	

	inclusiv în numele şi în contul unui furnizor de servicii de mobilitate		• Operatorii unui punct de reîncărcare, astfel cum este definit la art. 3 pct. 96 din Legea nr. 123/2012 a energiei electrice şi a gazelor naturale, care sunt responsabili cu gestionarea şi exploatarea unui punct de reîncărcare care furnizează un serviciu de reîncărcare clienţilor finali, astfel cum sunt definiţi la art. 3 pct. 20 din aceeaşi lege, inclusiv în numele şi în contul unui furnizor de servicii de mobilitate, astfel cum aceştia sunt definiţi la Articolul 3 pct. 36 din Regulamentul (UE) 2023/1804 al Parlamentului European şi al Consiliului din 13 septembrie 2023 privind instalarea infrastructurii pentru combustibili alternativi şi de abrogare a Directivei 2014/94/UE • Operatori economici, concesionarii şi dezvoltatorul centralei electrice eoliene offshore prevăzuţi de Legea nr. 121/2024 privind energia eoliană offshore	
1. Energie b) Încălzire centralizată şi răcire centralizată	Operatorii de încălzire centralizată sau răcire centralizată, astfel cum este definită la articolul 2 punctul 19 din Directiva (UE) 2018/2001 a Parlamentului European şi a Consiliului(3)		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 şi completările ulterioare	
1. Energie c) Petrol	Operatorii de conducte de transport al petrolului		Operatorii de conducte de transport al petrolului, astfel cum sunt definiţi ca „transportatori" la art. 2 pct. 42 din Legea nr. 238 din 7 iunie 2004 a petrolului, cu modificările şi completările ulterioare	

	Operatorii instalațiilor de producție, de rafinare și de tratare a petrolului, de depozitare și de transport		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 articolul 2 litera (f) din Directiva 2009/119/CE a Consiliului(4)		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	
1. Energie d) Gaze	Întreprinderile de furnizare, astfel cum sunt definite la articolul 2 punctul 8 din Directiva 2009/73/CE a Parlamentului European și a Consiliului(5)		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 articolul 2 punctul 6 din Directiva 2009/73/CE		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 articolul 2 punctul 4 din Directiva 2009/73/CE		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 articolul 2 punctul 10 din Directiva 2009/73/CE		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 la articolul 2 punctul 12 din Directiva 2009/73/CE		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 la articolul 2 punctul 1 din Directiva 2009/73/CE		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		Operatorii de instalație de rafinare și de tratare a gazelor naturale	
1. Energie e) Hidrogen	Operatorii de producție, stocare și transport de hidrogen		Operatorii de producție, stocare și transport de hidrogen	
1. Energie f) Beneficiarii proiectelor finanțate din fonduri nerambursabile, iar tipul de entitate care va avea următorul conținut	Beneficiarii prevăzuți de OUG nr. 60/2022 privind stabilirea cadrului instituțional și financiar de implementare și gestionare a fondurilor alocate României prin Fondul pentru modernizare, precum și pentru modificarea și completarea unor acte normative		Beneficiarii prevăzuți de OUG nr. 60/2022 privind stabilirea cadrului instituțional și financiar de implementare și gestionare a fondurilor alocate României prin Fondul pentru modernizare, precum și pentru modificarea și completarea unor acte normative	
2. Transport a) Transport aerian	Transportatorii aerieni, astfel cum sunt definiți la articolul 3 punctul 4 din Regulamentul (CE) nr. 300/2008, utilizați în scop comercial		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 la articolul 2 punctul 2 din Directiva 2009/12/CE a Parlamentului European și a Consiliului(6), aeroporturile, astfel cum sunt definite la articolul 2 punctul 1 din directiva respectivă, inclusiv aeroporturile principale enumerate în secțiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului(7), precum și entitățile care operează instalații auxiliare în cadrul aeroporturilor		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(8)		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)	
2. Transport b) Transport feroviar	Administratorii infrastructurii, astfel cum sunt definiți la articolul 3 punctul 2 din Directiva 2012/34/UE a Parlamentului European și a Consiliului(9)		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 la articolul 3 punctul 1 din Directiva 2012/34/UE, inclusiv operatorii unei infrastructuri de servicii, astfel cum sunt definiți la articolul 3 punctul 12 din directiva respectivă		Întreprinderile feroviare, astfel cum sunt definite ca "operatori de transport feroviar" la art. 3 pct. 18 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	
2. Transport 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(10)fără a include navele individuale operate de companiile respective		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 articolul 3 punctul 1 din Directiva 2005/65/CE a Parlamentului European şi a Consiliului(11), inclusiv instalaţiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004, şi entităţile care realizează lucrări şi operează echipamente în cadrul porturilor		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 securităţii portuare, inclusiv instalaţiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004, şi entităţile care realizează lucrări şi operează echipamente în cadrul porturilor	
	Operatorii de servicii de trafic maritim (STM), astfel cum sunt definiţi la articolul 3 litera (o) din Directiva 2002/59/CE a Parlamentului European şi a Consiliului(12)		Operatorii de servicii de trafic maritim (STM), astfel cum sunt definiţi la art. 3 lit. t) din Hotărârea Guvernului nr. 1016/2010 pentru stabilirea Sistemului de informare şi monitorizare a traficului navelor maritime care intră/ies în/din apele naţionale navigabile ale României, cu modificările şi completările ulterioare	
2. Transport d) Transport rutier	Autorităţile rutiere, astfel cum sunt definite la articolul 2 punctul 12 din Regulamentul delegat (UE) 2015/962 al Comisiei(13)responsabile cu controlul gestionării traficului, cu excepţia entităţilor publice în cazul cărora gestionarea traficului sau exploatarea sistemelor de transport inteligente reprezintă doar o parte neesenţială a activităţii lor generale		Autorităţile 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 şi a Consiliului în ceea ce priveşte prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic responsabile cu controlul gestionării traficului, cu excepţia entităţilor publice în cazul cărora gestionarea traficului sau exploatarea sistemelor de transport inteligente reprezintă doar o parte neesenţială a activităţii lor generale	
	Operatorii de sisteme de transport inteligente, astfel cum sunt definite la articolul 4 punctul 1 din Directiva 2010/40/UE a Parlamentului European şi a Consiliului(14)		Operatorii de sisteme de transport inteligente, astfel cum sunt definite la art. 4 lit. a din Ordonanţa Guvernului nr. 7 din 25 ianuarie 2012 privind implementarea sistemelor de transport inteligente în domeniul transportului	

			rutier şi pentru realizarea interfeţelor cu alte moduri de transport	
3. Sectorul bancar	Instituţiile de credit, astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European şi al Consiliului(15)		Instituţiile de credit, astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European şi al Consiliului din 26 iunie 2013 privind cerinţele prudenţiale pentru instituţiile de credit şi societăţile de investiţii şi de modificare a Regulamentului (UE) nr. 648/2012	
4. Infrastructuri ale pieţei financiare	Operatorii de locuri de tranzacţionare, astfel cum sunt definite la articolul 4 punctul 24 din Directiva 2014/65/UE a Parlamentului European şi a Consiliului(16)		Operatorii de locuri de tranzacţionare, astfel cum sunt definite la articolul 3 alin. 1 pct. 40 din Legea nr. 126 din 11 iunie 2018 privind pieţele de instrumente financiare	
	Contrapărţile centrale (CPC), astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European şi al Consiliului(17)		Contrapărţile centrale (CPC), astfel cum sunt definite la art. 3 alin. (1) pct. 16 din Legea nr. 126 din 11 iunie 2018 privind pieţele de instrumente financiare, cu modificările şi completările ulterioare	
5. Sectorul sănătăţii	Furnizorii de servicii medicale, astfel cum sunt definiţi la articolul 3 litera (g) din Directiva 2011/24/UE a Parlamentului European şi a Consiliului(18)		Furnizorii de servicii medicale, astfel cum sunt definiţi de art. 347 lit. c din Legea nr. 95 din 14 aprilie 2006 (republicată) privind reforma în domeniul sănătăţii, cu modificările şi completările ulterioare	
	Laboratoarele de referinţă ale UE, astfel cum sunt definite la articolul 15 din Regulamentul (UE) 2022/2371 al Parlamentului European şi al Consiliului(19)		Laboratoarele de referinţă ale UE, astfel cum sunt definite la articolul 15 din Regulamentul (UE) 2022/2371 al Parlamentului European şi al Consiliului din 23 noiembrie 2022 privind ameninţările transfrontaliere grave pentru sănătate şi de abrogare a Deciziei nr. 1082/2013/UE	
	• Entităţile care desfăşoară activităţi de cercetare şi dezvoltare a medicamentelor, astfel cum sunt definite la articolul 1 punctul 2 din Directiva 2001/83/CE a Parlamentului European şi a Consiliului(20)		• Entităţile care desfăşoară activităţi de cercetare şi dezvoltare a medicamentelor • Entităţile care fabrică produse farmaceutice de bază şi preparate	

	• 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(21)		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 destinată consumului uman, astfel cum este definită la articolul 2 punctul 1 litera (a) din Directiva (UE) 2020/2184 a Parlamentului European și a Consiliului(22)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		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 urbane reziduale, ape menajere uzate sau ape industriale uzate, astfel cum sunt definite la articolul 2 punctele 1, 2 și 3 din Directiva 91/271/CEE a Consiliului(23)cu		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	

	excepția întreprinderilor pentru care colectarea, evacuarea sau tratarea apelor urbane reziduale, a apelor menajere uzate sau a apelor industriale uzate reprezintă o parte neesențială a activității lor generale		respectiv 3 din Anexa 1 - Norme Tehnice din 28 februarie 2002 privind colectarea, epurarea şi 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 IXP (internet exchange point)	
	Furnizorii de servicii DNS, cu excepția operatorilor de servere pentru nume primare		Furnizorii de servicii DNS, cu excepția operatorilor de servere pentru nume primare	
	Registrele de nume TLD		Registrele de nume TLD	
	Furnizorii de servicii de cloud computing		Furnizorii de servicii de cloud computing	
	Furnizorii de servicii de centre de date		Furnizorii de servicii de centre de date	
	Furnizorii de rețele de furnizare de conținut		Furnizorii de rețele de difuzare de conținut	
	Furnizorii de servicii de încredere		Prestatorii de servicii de încredere	
	Furnizorii de rețele publice de comunicații electronice Furnizorii de servicii de comunicații electronice accesibile publicului		Furnizorii de rețele publice de comunicații electronice	
	Furnizorii de IXP (internet exchange point)			Sunt menționați de 2 ori în Directivă.
9. Gestionarea serviciilor TIC (business-to-business)	• Furnizorii de servicii gestionate • Furnizorii de servicii de securitate gestionate		• Furnizorii de servicii gestionate • Furnizorii de servicii de securitate gestionate	
10. Administrație publică	Entitățile de administrație publică din administrația centrală, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern		Entitățile administrației publice centrale, cu excepția instituțiilor din domeniul apărării, ordinii publice şi securității naționale, Oficiului Registrului Național al Informațiilor Secrete de Stat, instituțiile de învățământ superior, domeniul juridicar, justiție, inclusiv Ministerul	

			Public, Parlamentul României, Secretariatul General al Guvernului, Cancelaria Prim-Ministrului, Administrația Prezidențială, ASF, BNR și ANCOM.	
	Entitățile de administrație publică la nivel regional, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern			!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
11. Spațiu	Operatorii de infrastructură terestră deținută, gestionată și operată de statele membre sau de părți private, care sprijină furnizarea de servicii spațiale, cu excepția furnizorilor de rețele publice de comunicații electronice		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	
ANEXA II				
1. Servicii poștale și de curierat	Furnizorii de servicii poștale, astfel cum sunt definiți la articolul 2 punctul 1a din Directiva 97/67/CE, inclusiv furnizori de servicii 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 este definită la articolul 3 punctul 9 din Directiva 2008/98/CE a Parlamentului European și a Consiliului(1), cu excepția întreprinderilor pentru care gestionarea deșeurilor nu reprezintă principala activitate economică		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(2)și întreprinderile care produc articole, astfel cum sunt definite la articolul 3 punctul 3 din		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	

	regulamentul respectiv, din substanțe sau amestecuri		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 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(3)și întreprinderile care produc articole, astfel cum sunt definite la articolul 3 punctul 3 din regulamentul respectiv, din substanțe sau amestecuri		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(4), 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(5), cu excepția entităților care fabrică dispozitive medicale menționate în anexa I punctul 5 a cincea liniuță din prezenta directivă		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 şi al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic in vitro şi de abrogare a Directivei 98/79/CE şi a Deciziei 2010/227/UE a Comisiei, cu excepţia entităţilor care fabrică dispozitive medicale menţionate în anexa I punctul 5	
5. Fabricare: (b) Fabricarea computerelor şi a produselor electronice şi optice	Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în secţiunea C diviziunea 26 din NACE Rev. 2		Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în diviziunea 26 din CAEN Rev. 2	
5. Fabricare: (c) Fabricarea echipamentelor electrice	Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în secţiunea C diviziunea 27 din NACE Rev. 2		Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în diviziunea 27 din CAEN Rev. 2	
5. Fabricare: (d) Fabricarea altor maşini şi echipamente n.c.a.	Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în secţiunea C diviziunea 28 din NACE Rev. 2		Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în diviziunea 28 din CAEN Rev. 2	
5. Fabricare: (e) Fabricarea autovehiculelor, remorcilor şi semiremorcilor	Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în secţiunea C diviziunea 29 din NACE Rev. 2		Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în diviziunea 29 din CAEN Rev. 2	
5. Fabricare: (f) Fabricarea altor echipamente de transport	Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în secţiunea C diviziunea 30 din NACE Rev. 2		Întreprinderile care desfăşoară oricare dintre activităţile economice menţionate în diviziunea 30 din CAEN Rev. 2	
6. Furnizori digitali	Furnizorii de pieţe online		Furnizorii de pieţe online	
	Furnizorii de motoare de căutare online		Furnizorii de motoare de căutare online	
	Furnizorii de platforme de servicii de socializare în reţea		Furnizorii de platforme de servicii de socializare în reţea	
7. Cercetare	Organizaţiile de cercetare		Organizaţiile de cercetare	