DIRECTIVE

DIRECTIVA (UE) 2022/2555 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

din 14 decembrie 2022

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2)

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Băncii Centrale Europene ([1]),

având în vedere avizul Comitetului Economic și Social European ([2]),

după consultarea Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară ([3]),

întrucât:

(1) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului ([4]) viza consolidarea capacităților în materie de securitate cibernetică în întreaga Uniune, atenuarea amenințărilor la adresa rețelelor și a sistemelor informatice utilizate pentru a furniza servicii esențiale în sectoare-cheie și asigurarea continuității acestor servicii atunci când se confruntă cu incidente, contribuind astfel la securitatea Uniunii și la funcționarea eficace a economiei și a societății sale.

(2) De la intrarea în vigoare a Directivei (UE) 2016/1148, s-au înregistrat progrese semnificative în ceea ce privește creșterea nivelului de reziliență cibernetică în Uniune. Reexaminarea directivei respective a arătat că aceasta a servit drept catalizator pentru abordarea instituțională și de reglementare a securității cibernetice în Uniune, deschizând calea pentru o schimbare semnificativă a mentalității. Directiva respectivă a asigurat finalizarea cadrelor naționale privind securitatea rețelelor și a sistemelor informatice prin elaborarea unor strategii naționale referitoare la securitatea rețelelor și a sistemelor informatice și prin crearea de capacități naționale, precum și prin punerea în aplicare a unor măsuri de reglementare care să vizeze infrastructurile și entitățile esențiale identificate de fiecare stat membru. De asemenea, Directiva (UE) 2016/1148 a contribuit la cooperarea la nivelul Uniunii prin instituirea Grupului de cooperare și a rețelei de echipe naționale de intervenție în caz de incidente de securitate informatică. În pofida acestor realizări, reexaminarea Directivei (UE) 2016/1148 a evidențiat deficiențe inerente care o împiedică să soluționeze în mod eficace provocările actuale și cele emergente în materie de securitate cibernetică.

(3) Rețelele și sistemele informatice au devenit o componentă centrală a vieții de zi cu zi, odată cu transformarea digitală rapidă și interconectarea societății, inclusiv în cadrul schimburilor transfrontaliere. Această transformare a condus la o extindere a peisajului amenințărilor la adresa securității cibernetice, generând noi provocări, care necesită răspunsuri adaptate, coordonate și inovatoare în toate statele membre. Incidentele sunt tot mai numeroase, mai ample, mai sofisticate, mai frecvente și cu un impact tot mai mare, acestea reprezentând o amenințare gravă la adresa funcționării rețelelor și a sistemelor informatice. Prin urmare, incidentele pot împiedica desfășurarea

([1]) JO C 233, 16.6.2022, p. 22.
([2]) JO C 286, 16.7.2021, p. 170.
([3]) Poziția Parlamentului European din 10 noiembrie 2022 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 28 noiembrie 2022.
([4]) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

activităților economice pe piața internă, pot genera pierderi financiare, pot submina încrederea utilizatorilor și pot provoca pagube majore economiei și societății Uniunii. Prin urmare, pregătirea și eficacitatea în materie de securitate cibernetică sunt acum mai importante ca niciodată pentru buna funcționare a pieței interne. În plus, securitatea cibernetică este un factor-cheie pentru ca multe sectoare critice să adopte cu succes transformarea digitală și să profite pe deplin de beneficiile economice, sociale și durabile ale digitalizării.

(4) Temeiul juridic al Directivei (UE) 2016/1148 este articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), al cărui obiectiv este instituirea și funcționarea pieței interne prin consolidarea măsurilor de apropiere a normelor naționale. Cerințele în materie de securitate cibernetică impuse entităților care furnizează servicii sau desfășoară activități care sunt semnificative din punct de vedere economic variază considerabil de la un stat membru la altul în ceea ce privește tipul de cerință, nivelul lor de detaliere și metoda de supraveghere. Disparitățile respective implică costuri suplimentare și creează dificultăți pentru entitățile care oferă bunuri sau servicii la nivel transfrontalier. Cerințele impuse de un stat membru care sunt diferite sau chiar în conflict cu cele impuse de un alt stat membru pot afecta în mod substanțial astfel de activități transfrontaliere. În plus, posibilitatea ca cerințele de securitate să fie concepute sau puse în aplicare în mod necorespunzător într-un stat membru este probabil să aibă repercusiuni asupra nivelului de securitate cibernetică din alte state membre, în special având în vedere intensitatea schimburilor transfrontaliere. Revizuirea Directivei (UE) 2016/1148 a arătat că punerea sa în aplicare diferă foarte mult de la un stat membru la altul, inclusiv în ceea ce privește domeniul său de aplicare, a cărui delimitare a fost lăsată în mare măsură la latitudinea statelor membre. Directiva (UE) 2016/1148 a acordat, de asemenea, statelor membre o marjă de apreciere foarte largă în ceea ce privește punerea în aplicare a obligațiilor de raportare privind securitatea și incidentele pe care le prevede aceasta. Prin urmare, obligațiile respective au fost puse în aplicare în moduri foarte diferite la nivel național. Există divergențe similare în ceea ce privește punerea în aplicare a dispozițiilor Directivei (UE) 2016/1148 privind supravegherea și asigurarea respectării legii.

(5) Toate aceste divergențe implică o fragmentare a pieței interne și pot avea un efect negativ asupra funcționării acesteia, afectând în special furnizarea transfrontalieră de servicii și nivelul de reziliență cibernetică din cauza aplicării unor măsuri diferite. În cele din urmă, divergențele respective ar putea duce la o vulnerabilitate mai mare a unor state membre la amenințările cibernetice, cu potențiale efecte de propagare în întreaga Uniune. Prezenta directivă urmărește să elimine astfel de divergențe marcante dintre statele membre, în special prin stabilirea unor norme minime privind funcționarea unui cadru de reglementare coordonat, prin stabilirea unor mecanisme pentru cooperarea eficace între autoritățile responsabile din fiecare stat membru, prin actualizarea listei sectoarelor și a activităților care fac obiectul obligațiilor în materie de securitate cibernetică și prin instituirea unor căi de atac și măsuri de asigurare a respectării legii eficace care sunt esențiale pentru asigurarea efectivă a respectării acestor obligații. Prin urmare, Directiva (UE) 2016/1148 ar trebui să fie abrogată și înlocuită cu prezenta directivă.

(6) Odată cu abrogarea Directivei (UE) 2016/1148, domeniul de aplicare pe sectoare ar trebui să fie extins la o parte mai mare a economiei pentru a oferi o acoperire cuprinzătoare a sectoarelor și a serviciilor de importanță vitală pentru activitățile societale și economice esențiale din cadrul pieței interne. În special, prezenta directivă vizează depășirea deficiențelor legate de diferențierea dintre operatorii de servicii esențiale și furnizorii de servicii digitale, care s-a dovedit a fi caducă, deoarece nu reflectă importanța sectoarelor sau a serviciilor pentru activitățile societale și economice din cadrul pieței interne.

(7) În temeiul Directivei (UE) 2016/1148, statele membre erau responsabile de identificarea entităților ce îndeplineau criteriile pentru a se califica ca operatori de servicii esențiale. Pentru a elimina divergențele mari dintre statele membre în această privință și pentru a asigura securitatea juridică în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare pentru toate entitățile relevante, ar trebui stabilit un criteriu uniform pentru a determina entitățile care intră în domeniul de aplicare al prezentei directive. Criteriul respectiv ar trebui să constea în aplicarea unei norme de plafonare a dimensiunii, potrivit căreia toate entitățile care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE a Comisiei ([5]), sau depășesc plafoanele aferente întreprinderilor mijlocii prevăzute la alineatul (1) din

([5]) Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

respectivul articol, și care își desfășoară activitatea în sectoarele și furnizează tipurile de servicii sau desfășoară activitățile reglementate de prezenta directivă intră în domeniul său de aplicare. Statele membre ar trebui, de asemenea, să prevadă ca anumite întreprinderi mici și microîntreprinderi, astfel cum sunt definite la articolul 2 alineatele (2) și (3) din respectiva anexă, care îndeplinesc criterii specifice ce indică un rol esențial pentru societate, pentru economie sau pentru anumite sectoare sau tipuri de servicii, să intre în domeniul de aplicare al prezentei directive.

(8) Excluderea entităților administrației publice din domeniul de aplicare al prezentei directive ar trebui să se aplice entităților ale căror activități se desfășoară predominant în domeniile securității naționale, securității publice, apărării sau aplicării legii, inclusiv în domeniul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor. Cu toate acestea, entitățile administrației publice ale căror activități au doar o legătură redusă cu aceste domenii nu ar trebui să fie excluse din domeniul de aplicare al prezentei directive. În sensul prezentei directive, entitățile cu competențe de reglementare nu sunt considerate a desfășura activități în domeniul aplicării legii și, prin urmare, nu sunt excluse din acel motiv din domeniul de aplicare al prezentei directive. Entitățile administrației publice care sunt înființate în comun cu o țară terță în conformitate cu un acord internațional sunt excluse din domeniul de aplicare al prezentei directive. Prezenta directivă nu se aplică misiunilor diplomatice și consulare ale statelor membre în țări terțe sau rețelelor și sistemelor informatice ale acestora, în măsura în care aceste sisteme se află la sediul misiunii sau sunt utilizate pentru utilizatori dintr-o țară terță.

(9) Statele membre ar trebui să fie în măsură să ia măsurile necesare pentru a asigura protecția intereselor vitale de securitate națională, a apăra ordinea publică și siguranța publică și a permite prevenirea, investigarea, detectarea și urmărirea penală a infracțiunilor. În acest scop, statele membre ar trebui să poată 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, de anumite obligații prevăzute în prezenta directivă în ceea ce privește activitățile respective. În cazul în care o entitate prestează servicii exclusiv unei entități a administrației publice care este exclusă din domeniul de aplicare al prezentei directive, statele membre ar trebui să poată exonera entitatea respectivă de anumite obligații prevăzute în prezenta directivă în ceea ce privește serviciile în cauză. De asemenea, niciun stat membru nu ar trebui să aibă obligația de a furniza informații a căror divulgare ar fi contrară intereselor esențiale ale securității naționale, siguranței publice sau apărării sale. Normele Uniunii sau cele naționale privind protecția informațiilor clasificate, acordurile de nedivulgare și acordurile de nedivulgare informale, cum ar fi protocolul de schimb de informații „*Traffic Light Protocol*”, ar trebui luate în considerare în respectivul context. Protocolul de schimb de informații „*Traffic Light Protocol*” trebuie înțeles ca un mijloc de a furniza informații cu privire la orice limitări în ce privește răspândirea ulterioară a informațiilor. Acesta este utilizat în aproape toate echipele de intervenție în caz de incidente de securitate informatică (denumite în continuare „echipe CSIRT”) și în unele centre de analiză și de schimb de informații.

(10) Deși prezenta directivă se aplică entităților care desfășoară activități de producere a energiei electrice în centrale nucleare, unele dintre respectivele activități pot fi legate de securitatea națională. Într-un astfel de caz, un stat membru ar trebui să își poată exercita responsabilitatea de protejare a securității naționale în ceea ce privește activitățile respective, inclusiv activitățile din cadrul lanțului valoric nuclear, în conformitate cu tratatele.

(11) Unele entități desfășoară activități în domeniul securității naționale, al securității publice, al apărării sau al aplicării legii, inclusiv în domeniul prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, prestând în același timp servicii de încredere. Prestatorii de servicii de încredere care intră în domeniul de aplicare al Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([6]) ar trebui să intre în domeniul de aplicare al prezentei directive pentru a asigura același nivel de cerințe de securitate și de supraveghere ca cel prevăzut anterior în regulamentul respectiv în ceea ce privește prestatorii de servicii de încredere. În concordanță cu excluderea anumitor servicii specifice din Regulamentul (UE) nr. 910/2014, prezenta directivă nu ar trebui să se aplice prestării de servicii de încredere care sunt utilizate exclusiv în cadrul unor sisteme închise care decurg din dreptul intern sau din acorduri între un grup definit de participanți.

([6]) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73).

(12) Furnizorii de servicii poștale astfel cum sunt definiți în Directiva 97/67/CE a Parlamentului European și a Consiliului ([7]), inclusiv furnizorii de servicii de curierat ar trebui să intre în domeniul de aplicare al prezentei directive în cazul în care asigură cel puțin una dintre etapele lanțului de distribuție poștală, în special colectarea, sortarea, transportul sau distribuirea trimiterilor poștale, inclusiv serviciile de preluare, ținând seama totodată de gradul lor de dependență de rețele și de sistemele informatice. Serviciile de transport care nu sunt efectuate împreună cu una dintre aceste etape ar trebui să fie excluse din domeniul de aplicare al serviciilor poștale.

(13) Având în vedere intensificarea și gradul sporit de sofisticare a amenințărilor cibernetice, statele membre ar trebui să depună eforturi pentru a se asigura că entitățile care sunt excluse din domeniul de aplicare al prezentei directive ating un nivel ridicat de securitate cibernetică și pentru a sprijini punerea în aplicare a unor măsuri echivalente de gestionare a riscurilor în materie de securitate cibernetică care să reflecte natura sensibilă a entităților respective.

(14) Dreptul Uniunii privind protecția datelor și dreptul Uniunii privind protejarea confidențialității se aplică oricărei forme de prelucrare a datelor cu caracter personal în temeiul prezentei directive. În special, prezenta directivă nu aduce atingere Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului ([8]) și Directivei 2002/58/CE a Parlamentului European și a Consiliului ([9]). Prin urmare, prezenta directivă nu ar trebui să aducă atingere, printre altele, sarcinilor și competențelor autorităților competente să monitorizeze respectarea dreptului aplicabil al Uniunii în materie de protecție a datelor și a dreptului aplicabil al Uniunii privind protejarea confidențialității.

(15) Entitățile care intră în domeniul de aplicare al prezentei directive în scopul respectării măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare ar trebui clasificate în două categorii, entități esențiale și entități importante, reflectând măsura în care acestea sunt critice în ceea ce privește sectorul lor sau tipul de serviciu pe care îl prestează, precum și dimensiunea lor. În acest sens, ar trebui să se țină seama în mod corespunzător de orice evaluări ale riscurilor sau de orice orientări specifice unui sector relevante emise de către autoritățile competente, după caz. Regimurile de supraveghere și de asigurare a respectării legii corespunzătoare acestor două categorii de entități ar trebui să fie diferențiate pentru a asigura un echilibru corect între cerințele și obligațiile bazate pe riscuri, pe de o parte, și sarcina administrativă care decurge din supravegherea conformității, pe de altă parte.

(16) Pentru a evita ca entitățile care au întreprinderi partenere sau care sunt întreprinderi afiliate să fie considerate entități esențiale sau entități importante în cazul în care acest lucru ar fi disproporționat, statele membre pot ține seama de gradul de independență de care se bucură o entitate în raport cu întreprinderile sale partenere sau afiliate atunci când aplică articolul 6 alineatul (2) din anexa la Recomandarea 2003/361/CE. În special, statele membre sunt în măsură să ia în considerare faptul că o entitate este independentă de întreprinderile sale partenere sau afiliate în ceea ce privește rețelele și sistemele informatice pe care le utilizează pentru furnizarea serviciilor sale și în ceea ce privește serviciile pe care le prestează entitatea. Pe această bază, dacă este cazul, statele membre sunt în măsură să considere că o astfel de entitate nu se califică drept o întreprindere mijlocie în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE sau nu depășește plafoanele pentru o întreprindere mijlocie prevăzute la alineatul (1) din respectivul articol dacă, după luarea în considerare a gradului de independență a entității respective, nu s-ar fi considerat că acea entitate se califică drept o întreprindere mijlocie sau că depășește plafoanele respective în cazul în care ar fi fost luate în considerare numai propriile date. Acest lucru nu aduce atingere obligațiilor prevăzute în prezenta directivă ale întreprinderilor partenere și afiliate care intră în domeniul de aplicare al prezentei directive.

(17) Statele membre ar trebui să poată decide că entitățile identificate înainte de intrarea în vigoare a prezentei directive ca operatori de servicii esențiale în conformitate cu Directiva (UE) 2016/1148 trebuie să fie considerate entități esențiale.

([7]) Directiva 97/67/CE a Parlamentului European și a Consiliului din 15 decembrie 1997 privind normele comune pentru dezvoltarea pieței interne a serviciilor poștale ale Comunității și îmbunătățirea calității serviciului (JO L 15, 21.1.1998, p. 14).

([8]) 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 (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([9]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

(18) Pentru a asigura o imagine de ansamblu clară a entităților care intră în domeniul de aplicare al prezentei directive, statele membre ar trebui să stabilească o listă a entităților esențiale și a entităților importante, precum și a entităților care furnizează servicii de înregistrare a numelor de domenii. În acest scop, statele membre ar trebui să solicite entităților să transmită autorităților competente cel puțin următoarele informații, și anume denumirea, adresa și datele de contact actualizate, inclusiv adresele de e-mail, seriile IP și numerele de telefon ale entității și, după caz, sectorul și subsectorul pertinente menționate în anexe, precum și, după caz, o listă a statelor membre în care prestează servicii care intră în domeniul de aplicare al prezentei directive. În acest scop, Comisia, cu sprijinul Agenției pentru Securitate Cibernetică a Uniunii Europene (ENISA), ar trebui să ofere, fără întârzieri nejustificate, orientări și modele privind obligația de a prezenta informații. Pentru a înlesni întocmirea și actualizarea listei entităților esențiale și a entităților importante, precum și a entităților care furnizează servicii de înregistrare a numelor de domenii, statele membre ar trebui să poată institui mecanisme naționale care să le permită entităților să se înregistreze ele însele. În cazul în care există registre la nivel național, statele membre pot decide cu privire la mecanismele adecvate care să permită identificarea entităților care intră în domeniul de aplicare al prezentei directive.

(19) Statele membre ar trebui să fie responsabile de transmiterea către Comisie cel puțin a numărului de entități esențiale și entități importante pentru fiecare sector și subsector menționat în anexe, precum și a informațiilor pertinente cu privire la numărul entităților identificate și dispoziția, dintre cele prevăzute în prezenta directivă, pe baza cărora au fost identificate, precum și tipul de serviciu pe care îl furnizează. Statele membre sunt încurajate să facă schimb de informații cu Comisia cu privire la entitățile esențiale și entitățile importante și, în cazul unui incident de securitate cibernetică de mare amploare, de informații pertinente, cum ar fi denumirea entității în cauză.

(20) Comisia, în cooperare cu Grupul de cooperare și după consultarea părților interesate pertinente, ar trebui să ofere orientări privind punerea în aplicare a criteriilor aplicabile microîntreprinderilor și întreprinderilor mici pentru a evalua dacă acestea intră în domeniul de aplicare al prezentei directive. Comisia ar trebui, de asemenea, să asigure faptul că se oferă orientări adecvate microîntreprinderilor și întreprinderilor mici care intră în domeniul de aplicare al prezentei directive. Comisia ar trebui, cu sprijinul statelor membre, să le pună la dispoziție microîntreprinderilor și întreprinderilor mici informații în acest sens.

(21) Comisia ar putea oferi orientări pentru a sprijini statele membre în punerea în aplicare a dispozițiilor prezentei directive privind domeniul de aplicare și în evaluarea proporționalității măsurilor care trebuie luate în temeiul prezentei directive, în special în ceea ce privește entitățile cu modele de afaceri sau medii de funcționare complexe, în care o entitate poate îndeplini simultan criteriile atribuite entităților esențiale și celor importante sau poate desfășura simultan activități, dintre care unele se încadrează în domeniul de aplicare al prezentei directive, iar altele nu se încadrează.

(22) Prezenta directivă stabilește nivelul de referință pentru măsurile de gestionare a riscurilor în materie de securitate cibernetică și pentru obligațiile de raportare în toate sectoarele care intră în domeniul său de aplicare. Pentru a evita fragmentarea dispozițiilor privind securitatea cibernetică din actele juridice ale Uniunii, în cazul în care se consideră a fi necesare alte acte juridice sectoriale ale Uniunii referitoare la măsurile de gestionare a riscurilor în materie de securitate cibernetică și la obligațiile de raportare pentru a asigura un nivel ridicat de securitate cibernetică în întreaga Uniune, Comisia ar trebui să evalueze dacă astfel de dispoziții suplimentare ar putea fi stipulate într-un act de punere în aplicare în temeiul prezentei directive. În cazul în care un astfel de act de punere în aplicare nu este adecvat scopului respectiv, actele juridice sectoriale ale Uniunii ar putea contribui la asigurarea unui nivel ridicat de securitate cibernetică în întreaga Uniune, ținând seama pe deplin de particularitățile și de complexitatea sectoarelor în cauză. În acest scop, prezenta directivă nu împiedică adoptarea altor acte juridice sectoriale ale Uniunii care abordează măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare care iau în considerare în mod corespunzător necesitatea unui cadru de securitate cibernetică cuprinzător și coerent. Prezenta directivă nu aduce atingere competențelor de executare existente care i-au fost conferite Comisiei într-o serie de sectoare, inclusiv în domeniul transporturilor și în cel al energiei.

(23) În cazul în care un act juridic sectorial al Uniunii cuprinde dispoziții care impun entităților esențiale sau entităților importante să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să notifice incidentele semnificative, și în cazul în care cerințele respective au un efect cel puțin echivalent cu efectul obligațiilor prevăzute

în prezenta directivă, dispozițiile respective, inclusiv cele privind supravegherea și aplicarea legii, ar trebui să se aplice acestor entități. În cazul în care un act juridic sectorial al Uniunii nu include toate entitățile dintr-un anumit sector care intră în domeniul de aplicare al prezentei directive, dispozițiile relevante ale prezentei directive ar trebui să se aplice în continuare entităților care nu fac obiectul dispozițiilor actului respectiv.

(24) În cazul în care dispozițiile unui act juridic sectorial al Uniunii impun entităților esențiale sau entităților importante să respecte obligațiile de raportare care au un efect cel puțin echivalent cu cel al obligațiilor de raportare prevăzute în prezenta directivă, ar trebui să se asigure coerența și eficacitatea gestionării notificărilor incidentelor. În acest scop, dispozițiile privind notificarea incidentelor din actul juridic sectorial al Uniunii ar trebui, în temeiul prezentei directive, să ofere echipelor CSIRT, autorităților competente sau punctelor unice de contact privind securitatea cibernetică (denumite în continuare „puncte unice de contact") un acces imediat la notificările incidentelor transmise în conformitate cu actul juridic sectorial al Uniunii. În special, un astfel de acces imediat poate fi asigurat dacă notificările incidentelor sunt înaintate fără întârzieri nejustificate către echipa CSIRT, autoritatea competentă sau punctul unic de contact în temeiul prezentei directive. După caz, statele membre ar trebui să instituie un mecanism de raportare automată și directă care să asigure schimbul sistematic și imediat de informații cu echipele CSIRT, cu autoritățile competente sau cu punctele unice de contact cu privire la gestionarea unor astfel de notificări ale incidentelor. În scopul simplificării informării și al punerii în aplicare a mecanismului de raportare automată și directă, statele membre ar putea, în concordanță cu actul juridic sectorial al Uniunii, să utilizeze un punct de intrare unic.

(25) Actele juridice sectoriale ale Uniunii care prevăd măsuri de gestionare a riscurilor în materie de securitate cibernetică sau obligații de raportare care au un efect cel puțin echivalent cu cele prevăzute în prezenta directivă ar putea prevedea ca autoritățile competente în temeiul respectivelor acte să își exercite competențele de supraveghere și de aplicare a legii în raport cu respectivele măsuri sau obligații, cu sprijinul autorităților competente desemnate în temeiul prezentei directive. Autoritățile competente în cauză ar putea încheia acorduri de cooperare în acest scop. Astfel de acorduri de cooperare ar putea specifica, printre altele, procedurile privind coordonarea activităților de supraveghere, inclusiv procedurile de investigare și de inspecție la fața locului în conformitate cu dreptul intern, precum și un mecanism pentru schimbul de informații relevante privind supravegherea și aplicarea legii între autoritățile competente, inclusiv accesul la informațiile legate de domeniul cibernetic solicitate de autoritățile competente în temeiul prezentei directive.

(26) În cazul în care actele juridice sectoriale ale Uniunii impun entităților sau oferă stimulente acestora pentru ca acestea să notifice amenințările cibernetice semnificative, statele membre ar trebui, de asemenea, să încurajeze schimbul de informații cu privire la amenințările cibernetice semnificative cu echipele CSIRT, cu autoritățile competente sau cu punctele unice de contact în temeiul prezentei directive, pentru a asigura un nivel sporit de conștientizare a organismelor respective cu privire la contextul amenințărilor cibernetice și pentru a le permite să răspundă în mod eficace și în timp util în cazul în care amenințările cibernetice semnificative se materializează.

(27) Viitoarele acte juridice sectoriale ale Uniunii ar trebui să țină seama în mod corespunzător de definițiile și de cadrul de supraveghere și de asigurare a respectării legii prevăzute în prezenta directivă.

(28) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului ([10]) ar trebui considerat a fi un act juridic sectorial al Uniunii în legătură cu prezenta directivă în ce privește entitățile financiare. Dispozițiile Regulamentului (UE) 2022/2554 referitoare la gestionarea riscurilor legate de tehnologia informației și comunicațiilor (TIC), la gestionarea incidentelor legate de TIC și, în special, la raportarea incidentelor majore legate de TIC, precum și la testarea rezilienței operaționale digitale, la acordurile privind schimbul de informații și la riscurile TIC generate de părți terțe ar trebui să se aplice în locul celor prevăzute în prezenta directivă. Prin urmare, statele membre nu ar trebui să aplice dispozițiile prezentei directive privind gestionarea riscurilor în materie de securitate cibernetică și obligațiile de raportare, supraveghere și aplicarea legii, entităților financiare care fac obiectul Regulamentului (UE) 2022/2554. În același timp, este important ca, în temeiul prezentei directive, să se mențină o relație puternică cu sectorul financiar și să se facă un schimb de informații cu acesta. În acest scop, Regulamentul (UE) 2022/2554 permite autorităților europene de supraveghere (AES) și autorităților competente în temeiul respectivului regulament să participe la activitățile Grupului de cooperare și să facă schimb de informații și să coopereze cu punctele unice de contact, precum și cu echipele CSIRT și cu autoritățile competente în temeiul prezentei directive. Autoritățile competente în temeiul Regulamentului (UE) 2022/2554 ar trebui, de asemenea, să transmită detaliile

([10]) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (a se vedea pagina 1 din prezentul Jurnal Oficial).

incidentelor majore legate de TIC și, după caz, ale amenințărilor cibernetice semnificative echipelor CSIRT, autorităților competente sau punctelor unice de contact în temeiul prezentei directive. Acest lucru se poate realiza prin asigurarea accesului imediat la notificările privind incidentele și prin înaintarea acestora fie în mod direct, fie prin intermediul unui punct de intrare unic. În plus, statele membre ar trebui să includă în continuare sectorul financiar în strategiile lor de securitate cibernetică, iar echipele CSIRT pot include sectorul financiar în activitățile lor.

(29) Pentru a evita lacunele și suprapunerile obligațiilor în materie de securitate cibernetică impuse entităților din sectorul aviației, autoritățile naționale desemnate în temeiul Regulamentului (CE) nr. 300/2008 ([11]) și Regulamentului (UE) 2018/1139 ([12]) ale Parlamentului European și ale Consiliului și autoritățile competente desemnate în temeiul prezentei directive ar trebui să coopereze în ceea ce privește punerea în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și supravegherea conformării cu aceste măsuri la nivel național. Respectarea de către o entitate a cerințelor de securitate prevăzute în Regulamentul (CE) nr. 300/2008 și Regulamentul (UE) 2018/1139 și în actele delegate și de punere în aplicare relevante adoptate în temeiul regulamentelor respective ar putea fi considerată de către autoritățile competente în temeiul prezentei directive ca reprezentând conformarea cu cerințele corespunzătoare prevăzute în prezenta directivă.

(30) Având în vedere interconexiunile dintre securitatea cibernetică și securitatea fizică a entităților, ar trebui să se asigure o abordare coerentă între Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului ([13]) și prezenta directivă. Pentru a realiza acest lucru, entitățile identificate drept entități critice în temeiul Directivei (UE) 2022/2557 ar trebui să fie considerate a fi entități esențiale în temeiul prezentei directive. Mai mult, fiecare stat membru ar trebui să se asigure că strategia sa națională de securitate cibernetică oferă un cadru de politică pentru o coordonare consolidată în statul membru respectiv între autoritățile sale competente în temeiul prezentei directive și cele competente în temeiul Directivei (UE) 2022/2557 în contextul schimbului de informații privind riscurile, amenințările cibernetice și incidentele, precum și privind riscurile, amenințările și incidentele de altă natură decât cibernetică și cel al exercitării sarcinilor de supraveghere. Autoritățile competente în temeiul prezentei directive și cele competente în temeiul Directivei (UE) 2022/2557 ar trebui să coopereze și să facă schimb de informații fără întârzieri nejustificate, în special în ceea ce privește identificarea entităților critice, a riscurilor, a amenințărilor cibernetice și a incidentelor, precum și în legătură cu riscurile, amenințările și incidentele de altă natură decât cibernetică ce afectează entitățile critice, inclusiv măsurile în materie de securitate cibernetică și măsurile fizice adoptate de entitățile critice precum și rezultatele activităților de supraveghere desfășurate în legătură cu astfel de entități.

În plus, pentru a raționaliza activitățile de supraveghere între autoritățile competente în temeiul prezentei directive și al Directivei (UE) 2022/2557 și pentru a reduce la minimum sarcina administrativă pentru entitățile în cauză, autoritățile competente ar trebui să depună eforturi pentru a armoniza modelele de notificare a incidentelor și procesele de supraveghere. După caz, autoritățile competente în temeiul Directivei (UE) 2022/2557 ar trebui să poată 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 drept o entitate critică în temeiul Directivei (UE) 2022/2557. Autoritățile competente în temeiul prezentei directive și cele competente în temeiul Directivei (UE) 2022/2557 ar trebui, atunci când este posibil în timp real, să coopereze și să facă schimb de informații în acest scop.

(31) Entitățile care aparțin sectorului infrastructurii digitale se bazează, în esență, pe rețele și sisteme informatice și, prin urmare, obligațiile impuse acestor entități în temeiul prezentei directive ar trebui să abordeze în mod cuprinzător securitatea fizică a acestor sisteme, ca parte a măsurilor lor de gestionare a riscurilor și a obligațiilor de raportare în materie de securitate cibernetică. Întrucât aceste aspecte sunt reglementate de prezenta directivă, obligațiile prevăzute în capitolele III, IV și VI din Directiva (UE) 2022/2557 nu se aplică acestor entități.

([11]) Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului din 11 martie 2008 privind norme comune în domeniul securității aviației civile și de abrogare a Regulamentului (CE) nr. 2320/2002 (JO L 97, 9.4.2008, p. 72).

([12]) Regulamentul (UE) 2018/1139 al Parlamentului European și al Consiliului din 4 iulie 2018 privind normele comune în domeniul aviației civile și de înființare a Agenției Uniunii Europene pentru Siguranța Aviației, de modificare a Regulamentelor (CE) nr. 2111/2005, (CE) nr. 1008/2008, (UE) nr. 996/2010, (UE) nr. 376/2014 și a Directivelor 2014/30/UE și 2014/53/UE ale Parlamentului European și ale Consiliului, precum și de abrogare a Regulamentelor (CE) nr. 552/2004 și (CE) nr. 216/2008 ale Parlamentului European și ale Consiliului și a Regulamentului (CEE) nr. 3922/91 al Consiliului (JO L 212, 22.8.2018, p. 1).

([13]) Directiva (UE) 2022/2557 a Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (a se vedea pagina 164 din prezentul Jurnal Oficial).

(32) Sprijinirea și menținerea unui sistem fiabil, rezilient și sigur de nume de domenii (DNS) reprezintă factori-cheie pentru menținerea integrității internetului și sunt esențiali pentru funcționarea sa continuă și stabilă, de care depind economia digitală și societatea. Prin urmare, prezenta directivă ar trebui să se aplice registrelor de nume de domenii de prim nivel (TLD) și prestatorilor de servicii DNS care trebuie înțelese ca fiind entități care furnizează servicii de rezolvare recursivă a numelor de domenii accesibile publicului pentru utilizatorii finali de internet sau ca servicii de rezolvare a numelor de domenii cu autoritate pentru utilizarea de către terți. Prezenta directivă nu ar trebui să se aplice serverelor pentru numele primare.

(33) Serviciile de *cloud computing* ar trebui să cuprindă serviciile digitale care permit administrarea la cerere și accesul amplu de 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 locuri. Resursele informatice includ resurse precum rețelele, serverele sau alte infrastructuri, sistemele de operare, programele informatice (software), stocarea, aplicațiile și serviciile. Modelele de servicii de *cloud computing* includ, printre altele, infrastructura ca serviciu (IaaS), platforma ca serviciu (PaaS), software-ul ca serviciu (SaaS) și rețeaua ca serviciu (NaaS). Modelele de implementare a *cloud computingului* ar trebui să includă tehnologiile de tip *cloud* private, comunitare, publice și hibride. Modelele de servicii și de implementare de *cloud computing* au același înțeles ca și termenii modelelor de servicii și de implementare definiți în standardul ISO/IEC 17788:2014. Capacitatea utilizatorului de *cloud computing* de a furniza în mod unilateral capacități de calcul autonome, cum ar fi ora serverului sau stocarea în rețea, fără nicio interacțiune umană din partea furnizorului de servicii de *cloud computing*, ar putea fi descrisă ca administrare la cerere.

Termenul „acces amplu de la distanță” este utilizat pentru a descrie faptul că capacitățile de *cloud* sunt furnizate prin rețea și accesate prin mecanisme care promovează utilizarea unor platforme eterogene, subțiri sau groase, pentru clienți, inclusiv telefoane mobile, tablete, laptopuri și stații de lucru. Termenul „redimensionabil” se referă la resursele informatice care sunt alocate în mod flexibil de către furnizorul de servicii de *cloud*, indiferent de localizarea geografică a resurselor, pentru a face față fluctuațiilor cererii. Termenul „bazin elastic” se referă la resursele informatice care sunt furnizate și puse la dispoziție în funcție de cerere, pentru a amplifica și a reduce rapid resursele disponibile în conformitate cu volumul de lucru. Expresia „care pot fi puse în comun” este utilizată pentru a descrie acele resurse informatice care sunt furnizate mai multor utilizatori care au acces comun la serviciu, dar tratamentul se efectuează separat pentru fiecare utilizator, deși serviciul este prestat de același echipament electronic. Termenul „distribuit” se referă la resursele informatice care sunt situate pe diferite calculatoare sau dispozitive în rețea și care comunică și se coordonează între ele prin transmiterea de mesaje.

(34) Având în vedere apariția unor tehnologii inovatoare și a unor noi modele de afaceri, se preconizează că pe piața internă vor apărea noi servicii de *cloud computing* și noi modele de implementare ca răspuns la nevoile în continuă evoluție ale clienților. În acest context, serviciile de *cloud computing* pot fi prestate într-o formă foarte distribuită, chiar mai aproape de locul în care datele sunt generate sau colectate, trecând astfel de la modelul tradițional la unul foarte distribuit („tehnica de calcul la margine” – *edge computing*).

(35) Este posibil ca serviciile oferite de prestatorii de servicii de centre de date să nu fie întotdeauna prestate sub formă de servicii de *cloud computing*. În consecință, este posibil ca centrele de date să nu constituie întotdeauna o parte a infrastructurii de *cloud computing*. Pentru a gestiona toate riscurile la adresa securității rețelelor și a sistemelor informatice, prezenta directivă ar trebui să vizeze, prin urmare, furnizorii de servicii de centre de date care nu sunt servicii de *cloud computing*. În sensul prezentei directive, termenul „serviciu de centre de date” ar trebui să includă prestarea unui serviciu care cuprinde structuri sau grupuri de structuri destinate instalării centralizate, interconectării și funcționării tehnologiei informației (IT) și 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. Termenul „serviciu de centru de date” nu ar trebui să se aplice centrelor de date corporative interne, deținute și exploatate de entitatea în cauză, în scopuri proprii.

(36) Activitățile de cercetare joacă un rol esențial în dezvoltarea de noi produse și procese. Multe dintre respectivele activități sunt desfășurate de entități care partajează, diseminează sau exploatează rezultatele cercetării lor în scopuri comerciale. Prin urmare, aceste entități pot fi actori importanți în lanțurile valorice, ceea ce face ca securitatea rețelelor și a sistemelor lor informatice să fie parte integrantă din securitatea cibernetică globală a pieței interne. Organizațiile de cercetare ar trebui înțelese ca incluzând entitățile care își concentrează partea esențială a

activităților pe desfășurarea de cercetare aplicată sau dezvoltare experimentală, în sensul Manualului Frascati 2015 al Organizației pentru Cooperare și Dezvoltare Economică: *Guidelines for Collecting and Reporting Data on Research and Experimental Development* (Orientări pentru colectarea și raportarea datelor privind cercetarea și dezvoltarea experimentală), în vederea exploatării rezultatelor acestora în scopuri comerciale, cum ar fi fabricarea sau dezvoltarea unui produs sau a unui proces, furnizarea unui serviciu sau comercializarea acestora.

(37) Interdependențele din ce în ce mai mari sunt rezultatul unei rețele din ce în ce mai transfrontaliere și interdependente de prestare de servicii care utilizează infrastructuri-cheie din întreaga Uniune în sectoare precum energia, transporturile, infrastructura digitală, apa potabilă și apele uzate, sănătatea, anumite aspecte ale administrației publice, precum și spațiul, în măsura în care furnizarea anumitor servicii în funcție de infrastructurile terestre care sunt deținute, gestionate și exploatate fie de statele membre, fie de părți private, nu cuprinde, prin urmare, infrastructurile deținute, gestionate sau exploatate de Uniune sau în numele acesteia, ca parte a programului său spațial. Aceste interdependențe înseamnă că orice perturbare, chiar dacă inițial este limitată la o singură entitate sau la un singur sector, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea efecte negative de amploare și de lungă durată asupra furnizării de servicii pe piața internă. Intensificarea atacurilor cibernetice în timpul pandemiei de COVID-19 a demonstrat vulnerabilitatea societăților noastre, care sunt din ce în ce mai interdependente în fața riscurilor cu probabilitate redusă de producere.

(38) Având în vedere diferențele dintre structurile naționale de administrare și pentru a proteja acordurile specifice unui sector sau organismele de supraveghere și de reglementare ale Uniunii deja existente, statele membre ar trebui să fie în măsură să desemneze sau să instituie una sau mai multe autorități competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere în temeiul prezentei directive.

(39) Pentru a facilita cooperarea și comunicarea transfrontalieră între autorități și pentru a permite punerea în aplicare efectivă a prezentei directive, este necesar ca fiecare stat membru să desemneze un punct unic de contact responsabil cu coordonarea aspectelor legate de securitatea rețelelor și a sistemelor informatice și cu cooperarea transfrontalieră la nivelul Uniunii.

(40) Punctele unice de contact ar trebui să asigure o cooperare transfrontalieră eficace cu autoritățile competente din alte state membre și, după caz, cu Comisia și cu ENISA. Punctele unice de contact ar trebui, prin urmare, să fie însărcinate cu înaintarea notificărilor incidentelor semnificative cu impact transfrontalier către punctele unice de contact ale altor state membre afectate, la cererea echipei CSIRT sau a autorității competente. La nivel național, punctele unice de contact ar trebui să înlesnească o bună cooperare transsectorială cu alte autorități competente. Punctele unice de contact ar putea fi, de asemenea, destinatarii informațiilor relevante privind incidentele referitoare la entitățile financiare transmise de autoritățile competente în temeiul Regulamentului (UE) 2022/2554 pe care ele ar trebui să le poată înainta, după caz, echipelor CSIRT sau autorităților competente în temeiul prezentei directive.

(41) Statele membre ar trebui să fie dotate în mod adecvat, din punctul de vedere al capacității atât tehnice, cât și organizatorice, pentru a preveni, a detecta, a răspunde și a se redresa de pe urma incidentelor și a riscurilor, precum și a atenua impactul acestora. Prin urmare, statele membre ar trebui să instituie sau să desemneze una sau mai multe echipe CSIRT în temeiul prezentei directive și să se asigure că acestea dispun de resurse și capacități tehnice adecvate. Echipele CSIRT ar trebui să respecte cerințele stabilite în prezenta directivă pentru a garanta existența unor capacități efective și compatibile de gestionare a incidentelor și a riscurilor și pentru a asigura o cooperare eficientă la nivelul Uniunii. Statele membre ar trebui să poată desemna în calitate de echipe CSIRT echipe existente de intervenție în caz de urgență informatică („CERT”). În vederea consolidării relației de încredere dintre entități și echipe CSIRT, în cazurile în care o echipe CSIRT face parte din autoritatea competentă, statele membre ar trebui să poată avea în vedere separarea funcțională a sarcinilor operaționale furnizate de echipele CSIRT, în special în ceea ce privește schimbul de informații și sprijinul acordat entităților, și activitățile de supraveghere ale autorităților competente.

(42) Echipele CSIRT au sarcina de a administra incidentele. Aceasta include prelucrarea unor volume mari de date uneori sensibile. Statele membre ar trebui să se asigure că echipele CSIRT dispun de o infrastructură pentru schimbul de informații și prelucrarea acestora, precum și de personal bine echipat, care asigură confidențialitatea și credibilitatea operațiunilor lor. Echipele CSIRT ar putea adopta, de asemenea, coduri de conduită în acest sens.

(43) În ceea ce privește datele cu caracter personal, echipele CSIRT ar trebui să poată furniza, în concordanță cu Regulamentul (UE) 2016/679, la cererea unei entități esențiale sau a unei entități importante, o scanare proactivă a rețelelor și a sistemelor informatice utilizate pentru prestarea serviciilor lor. Atunci când este cazul, statele membre ar trebui să vizeze asigurarea unui nivel egal de capacități tehnice pentru toate echipele CSIRT specifice unui sector. Statele membre ar trebui să poată solicita asistența ENISA pentru instituirea echipelor lor CSIRT.

(44) Echipele CSIRT ar trebui să aibă capacitatea, la cererea unei entități esențiale sau a unei entități importante, de a monitoriza resursele conectate la internet ale entității, atât la locurile în care își desfășoară activitatea, cât și în exteriorul acestora, pentru identifica, a înțelege și a gestiona riscurile organizaționale generale ale entității cu privire la compromisurile sau vulnerabilitățile critice nou-identificate din lanțul de aprovizionare. Entitatea ar trebui să fie încurajată să comunice echipei CSIRT dacă utilizează o interfață de gestionare privilegiată, deoarece acest lucru ar putea afecta viteza de desfășurare a unor acțiuni de atenuare.

(45) Având în vedere importanța cooperării internaționale în privința securității cibernetice, echipele CSIRT ar trebui să aibă posibilitatea de a participa la rețele de cooperare internațională, în plus față de rețeaua CSIRT instituită prin prezenta directivă. Prin urmare, în scopul îndeplinirii sarcinilor care le revin, echipele CSIRT și autoritățile competente ar trebui să poată face schimb de informații, inclusiv de date cu caracter personal, cu echipele naționale de intervenție în caz de incidente de securitate informatică sau cu autoritățile competente din țări terțe, cu condiția să fie îndeplinite condițiile prevăzute de dreptul Uniunii privind protecția datelor pentru transferurile de date cu caracter personal către țări terțe, printre altele cele prevăzute la articolul 49 din Regulamentul (UE) 2016/679.

(46) Este esențial să se asigure resurse adecvate pentru îndeplinirea obiectivelor prevăzute în prezenta directivă și pentru a facilita îndeplinirea de către autoritățile competente și echipele CSIRT a sarcinilor prevăzute în prezenta directivă. Statele membre pot institui la nivel național un mecanism de finanțare care să acopere cheltuielile necesare în legătură cu îndeplinirea sarcinilor entităților publice responsabile cu securitatea cibernetică în statul membru în temeiul prezentei directive. Un astfel de mecanism ar trebui să respecte dreptul Uniunii și ar trebui să fie proporțional și nediscriminatoriu și ar trebui să țină seama de diferitele abordări în ceea ce privește prestarea de servicii sigure.

(47) Rețeaua CSIRT ar trebui să contribuie în continuare la consolidarea încrederii și la promovarea unei cooperări operaționale rapide și eficace între statele membre. Pentru a consolida cooperarea operațională la nivelul Uniunii, rețeaua CSIRT ar trebui să aibă în vedere invitarea organelor și agențiilor Uniunii implicate în politica de securitate cibernetică, cum ar fi Europol, să participe la activitatea sa.

(48) În scopul atingerii și menținerii unui nivel ridicat de securitate cibernetică, strategiile naționale de securitate cibernetică necesare în temeiul prezentei directive ar trebui să constea în cadre coerente care să ofere obiective și priorități strategice în domeniul securității cibernetice și administrarea necesară pentru realizarea acestora. Aceste strategii pot fi compuse dintr-unul sau mai multe instrumente legislative sau fără caracter legislativ.

(49) Politicile de igienă cibernetică asigură baza pentru protecția infrastructurilor de rețele și sisteme informatice, pentru securitatea hardware, software și a aplicațiilor online, precum și pentru protecția datelor întreprinderilor sau ale utilizatorilor finali pe care se bazează entitățile. Politicile de igienă cibernetică care cuprind un set de practici de referință comun, inclusiv actualizări de software și hardware, modificări ale parolelor, gestionarea noilor instalări, limitarea conturilor cu acces la nivel de administrator și copierea de rezervă a datelor, permit un cadru proactiv de pregătire și de siguranță și securitate generale în caz de incidente sau amenințări cibernetice. ENISA ar trebui să monitorizeze și să analizeze politicile de igienă cibernetică ale statelor membre.

(50) Sensibilizarea cu privire la securitatea cibernetică și igiena cibernetică sunt esențiale pentru a crește nivelul de securitate cibernetică în Uniune, în special având în vedere numărul crescând de dispozitive conectate care sunt utilizate din ce în ce mai mult în atacurile cibernetice. Ar trebui depuse eforturi pentru a crește nivelul general de conștientizare a riscurilor legate de astfel de dispozitive, în timp ce evaluările la nivelul Uniunii ar putea contribui la asigurarea unei înțelegeri comune a acestor riscuri în cadrul pieței interne.

(51) Statele membre ar trebui să încurajeze utilizarea oricărei tehnologii inovatoare, inclusiv a inteligenței artificiale, a cărei utilizare ar putea îmbunătăți detectarea și prevenirea atacurilor cibernetice, permițând deturnarea resurselor către atacuri cibernetice într-un mod mai eficace. Prin urmare, statele membre ar trebui să încurajeze, în cadrul strategiei lor naționale de securitate cibernetică, activitățile de cercetare și dezvoltare pentru a înlesni utilizarea unor astfel de tehnologii, în special a celor legate de instrumentele automatizate sau semi automatizate în materie de securitate cibernetică și, după caz, schimbul de date necesare pentru formarea utilizatorilor unei astfel de tehnologii și pentru îmbunătățirea acesteia. Utilizarea oricărei tehnologii inovatoare, inclusiv a inteligenței artificiale, ar trebui să respecte dreptul Uniunii în materie de protecție a datelor, inclusiv principiile de protecție a datelor, și anume acuratețea, reducerea la minimum a datelor, echitatea și transparența, precum și securitatea datelor, cum ar fi criptarea de ultimă generație. Cerințele privind protecția datelor începând cu momentul conceperii și protecția implicită a datelor prevăzute în Regulamentul (UE) 2016/679 ar trebui să fie exploatate pe deplin.

(52) Instrumentele și aplicațiile de securitate cibernetică cu sursă deschisă pot contribui la un grad mai ridicat de deschidere și pot avea un impact pozitiv asupra eficienței inovării industriale. Standardele deschise înlesnesc interoperabilitatea dintre instrumentele de securitate, aducând beneficii securității părților interesate din industrie. Instrumentele și aplicațiile de securitate cibernetică cu sursă deschisă pot stimula comunitatea mai largă a dezvoltatorilor, permițând diversificarea furnizorilor. Sursa deschisă poate duce la un proces mai transparent de verificare a instrumentelor legate de securitatea cibernetică și la un proces de descoperire a vulnerabilităților bazat pe comunitate. Prin urmare, statele membre ar trebui să fie în măsură să promoveze utilizarea de software cu sursă deschisă și de standarde deschise prin aplicarea de politici privind utilizarea datelor deschise și a surselor deschise ca parte a securității prin transparență. Politicile care promovează introducerea și utilizarea durabilă a instrumentelor de securitate cibernetică cu sursă deschisă sunt de o importanță deosebită pentru întreprinderile mici și mijlocii care se confruntă cu costuri semnificative pentru punerea în aplicare, care ar putea fi reduse prin reducerea nevoii de aplicații sau instrumente specifice.

(53) Utilitățile sunt din ce în ce mai conectate la rețelele digitale din orașe, în scopul îmbunătățirii rețelelor de transport urban, al modernizării instalațiilor de alimentare cu apă și de eliminare a deșeurilor și al creșterii eficienței iluminatului și a încălzirii clădirilor. Respectivele utilități digitalizate sunt vulnerabile la atacurile cibernetice și riscă, în cazul unui atac cibernetic reușit, să prejudicieze cetățenii la scară largă din cauza interconectării lor. Statele membre ar trebui să elaboreze o politică care să abordeze dezvoltarea unor astfel de orașe conectate sau inteligente și efectele lor potențiale asupra societății, ca parte a strategiei lor naționale de securitate cibernetică.

(54) În ultimii ani, Uniunea s-a confruntat cu o creștere exponențială a atacurilor de tip *ransomware*, în care programele malware criptează date și sisteme și solicită o plată de răscumpărare pentru a le decripta. Frecvența și gravitatea tot mai mare a atacurilor de tip *ransomware* pot fi determinate de mai mulți factori, cum ar fi modele diferite de atac, modele de afaceri infracționale în jurul „*ransomware* ca serviciu" (*ransomware as a service*) și criptomonedele, cererile de răscumpărare și intensificarea atacurilor asupra lanțului de aprovizionare. Statele membre ar trebui să elaboreze o politică care să abordeze creșterea numărului de atacuri de tip *ransomware* ca parte a strategiei lor naționale de securitate cibernetică.

(55) Parteneriatele public-private (PPP) în domeniul securității cibernetice pot asigura un cadru adecvat pentru schimbul de cunoștințe, de bune practici și pentru stabilirea unui nivel comun de înțelegere între părțile interesate. Statele membre ar trebui să promoveze politici care stau la baza instituirii unor PPP specifice securității cibernetice. Respectivele politici ar trebui să clarifice, printre altele, domeniul de aplicare și părțile interesate implicate, modelul de administrare, opțiunile de finanțare disponibile, precum și interacțiunea dintre părțile interesate participante în ceea ce privește PPP. PPP pot valorifica cunoștințele specializate ale entităților din sectorul privat pentru a ajuta autoritățile competente în dezvoltarea unor servicii și procese de ultimă generație, inclusiv în schimbul de informații, alertele timpurii, exercițiile pentru amenințări cibernetice și incidente, gestionarea crizelor și planificarea rezilienței.

(56) În strategiile lor naționale de securitate cibernetică, statele membre ar trebui să abordeze nevoile specifice în materie de securitate cibernetică ale întreprinderilor mici și mijlocii. La nivelul Uniunii, întreprinderile mici și mijlocii reprezintă un procentaj ridicat din piața industrială și de afaceri și adesea se luptă să se adapteze la noile practici comerciale într-o lume mai conectată și la mediul digital, în care angajații lucrează de acasă, iar activitățile de afaceri se desfășoară tot mai mult online. Unele întreprinderi mici și mijlocii se confruntă cu provocări specifice în materie de securitate cibernetică, cum ar fi un nivel scăzut de sensibilizare în domeniul cibernetic, lipsa securității informatice de la distanță, costul ridicat al soluțiilor de securitate cibernetică și un nivel crescut de amenințare, cum ar fi programele de tip *ransomware*, pentru care ar trebui să primească îndrumări și ajutor. Întreprinderile mici și mijlocii devin din ce în ce mai mult ținta atacurilor asupra lanțului de aprovizionare, din cauza măsurilor lor mai puțin riguroase de gestionare a riscurilor în materie de securitate cibernetică și a gestionării atacurilor, precum și din cauza faptului că au resurse de securitate limitate. Astfel de atacuri asupra lanțului de aprovizionare nu numai că au

un impact asupra întreprinderilor mici și mijlocii și asupra operațiunilor acestora în mod izolat, ci pot avea, de asemenea, un efect în cascadă rezultând în atacuri mai ample asupra entităților pe care le-au aprovizionat. Prin intermediul strategiilor lor naționale de securitate cibernetică, statele membre ar trebui să ajute întreprinderile mici și mijlocii să abordeze provocările cu care se confruntă în lanțurile lor de aprovizionare. Statele membre ar trebui să aibă un punct de contact pentru întreprinderile mici și mijlocii la nivel național sau regional, care fie să ofere orientări și asistență întreprinderilor mici și mijlocii, fie să le direcționeze către organele corespunzătoare pentru orientare și asistență în ceea ce privește aspectele legate de securitatea cibernetică. Statele membre sunt încurajate, de asemenea, să ofere servicii precum configurarea de site-uri web și înlesnirea jurnalizării pentru microîntreprinderile și întreprinderile mici care nu dispun de aceste capacități.

(57) Ca parte a strategiilor lor naționale de securitate cibernetică, statele membre ar trebui să adopte politici privind promovarea unei protecții cibernetice active ca parte a unei strategii defensive mai ample. În loc să răspundă reactiv, protecția cibernetică activă constă în prevenirea, detectarea, monitorizarea, analizarea și atenuarea în mod activ ale încălcărilor securității rețelei, combinată cu utilizarea capacităților desfășurate în interiorul și în afara rețelei afectate. Aceasta ar putea include oferirea de către statele membre a unor servicii sau instrumente gratuite anumitor entități, inclusiv verificări în regim de autoservire, instrumente de detectare și servicii de retragere. Capacitatea de a partaja și a înțelege rapid și automat informații și analize privind amenințările, alertele privind activitățile cibernetice și acțiunile de răspuns este esențială pentru a permite unitatea eforturilor în prevenirea, detectarea, abordarea și blocarea cu succes a atacurilor împotriva rețelelor și a sistemelor informatice. Protecția cibernetică activă se bazează pe o strategie defensivă care exclude măsurile ofensive.

(58) Întrucât exploatarea vulnerabilităților din cadrul rețelelor și al sistemelor informatice poate provoca perturbări și prejudicii semnificative, identificarea și remedierea rapidă a unor astfel de vulnerabilități constituie un factor important în reducerea riscului. Entitățile care dezvoltă sau administrează rețele și sisteme informatice ar trebui, prin urmare, să stabilească proceduri adecvate de gestionare a vulnerabilităților atunci când acestea sunt descoperite. Întrucât vulnerabilitățile sunt adesea descoperite și divulgate de părți terțe, producătorul sau furnizorul de produse TIC sau servicii TIC ar trebui, de asemenea, să instituie procedurile necesare pentru a primi de la terți informații privind vulnerabilitatea. În acest sens, standardele internaționale ISO/IEC 30111 și ISO/IEC 29147 oferă orientări privind gestionarea și divulgarea vulnerabilităților. Întărirea coordonării dintre persoanele fizice și juridice raportoare și producătorii ori furnizorii de produse TIC sau servicii TIC este deosebit de importantă în scopul facilitării cadrului voluntar de divulgare a vulnerabilităților. Divulgarea coordonată a vulnerabilităților definește un proces structurat prin care informații privind vulnerabilitățile sunt transmise producătorului sau furnizorului de produse TIC sau de servicii TIC potențial vulnerabile într-o manieră care să îi permită acestuia să diagnosticheze și să remedieze vulnerabilitatea înainte ca informațiile detaliate privind vulnerabilitatea să fie dezvăluite unor terțe părți sau publicului. Divulgarea coordonată a vulnerabilităților ar trebui să includă, de asemenea, coordonarea dintre persoana fizică sau juridică raportoare și producătorul sau furnizorul de produse TIC sau de servicii TIC potențial vulnerabile în ceea ce privește calendarul de remediere și publicare a vulnerabilităților.

(59) Comisia, ENISA și statele membre ar trebui să continue să încurajeze alinierea la standardele internaționale și la bunele practici existente din sector în domeniul gestionării riscurilor în materie de securitate cibernetică, de exemplu în domeniul evaluărilor securității lanțului de aprovizionare, al schimbului de informații și al divulgării vulnerabilităților.

(60) Statele membre, în cooperare cu ENISA, ar trebui să ia măsuri pentru a înlesni divulgarea coordonată a vulnerabilităților prin stabilirea unei politici naționale relevante. Ca parte a politicii lor naționale, statele membre ar trebui să își propună să facă față, în măsura posibilului, încercărilor cu care se confruntă cercetătorii în domeniul vulnerabilității, inclusiv expunerea potențială a acestora la răspunderea penală, în conformitate cu dreptul intern. Având în vedere faptul că persoanele fizice și juridice care cercetează vulnerabilități ar putea fi expuse, în unele state membre, răspunderii penale și civile, statele membre sunt încurajate să adopte orientări în ceea ce privește neurmărirea penală a cercetătorilor în domeniul securității informațiilor și exonerarea de răspundere civilă pentru activitățile desfășurate de aceștia.

(61) Statele membre ar trebui să desemneze una din echipele sale CSIRT drept coordonator, acționând, dacă este necesar, ca intermediar de încredere între persoanele fizice sau juridice care raportează și producătorii sau furnizorii de produse TIC sau servicii TIC care ar putea fi afectați de vulnerabilitate. Sarcinile echipei CSIRT desemnate drept coordonator ar trebui să includă identificarea și contactarea entităților în cauză, asistarea persoanelor fizice sau juridice care raportează o vulnerabilitate, negocierea calendarelor de divulgare și gestionarea vulnerabilităților care

afectează mai multe entități (divulgarea coordonată a vulnerabilităților de către mai multe părți). Atunci când vulnerabilitatea raportată ar putea avea un impact semnificativ asupra entităților în mai multe state membre, echipele CSIRT desemnate drept coordonatori ar trebui să coopereze în cadrul rețelei CSIRT, dacă este cazul.

(62) Accesul la informații corecte și în timp util cu privire la vulnerabilitățile care afectează produsele TIC și serviciile TIC contribuie la o mai bună gestionare a riscurilor în materie de securitate cibernetică. Sursele de informații accesibile publicului cu privire la vulnerabilități reprezintă un instrument important pentru entități și pentru utilizatorii serviciilor acestora, dar și pentru autoritățile competente și pentru echipele CSIRT. Din acest motiv, ENISA ar trebui să creeze o bază de date europeană a vulnerabilităților în care entitățile, indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, și furnizorii lor de rețele și sisteme informatice, precum și autoritățile competente și echipele CSIRT să poată divulga și înregistra, în mod voluntar, vulnerabilități cunoscute publicului, pentru a permite utilizatorilor să ia măsuri adecvate de atenuare. Scopul acestei baze de date este de a răspunde provocărilor unice pe care le constituie riscurile pentru entitățile din Uniune. În plus, ENISA ar trebui să stabilească o procedură adecvată în ceea ce privește procesul de publicare, pentru a acorda entităților timpul necesar pentru a lua măsuri de atenuare a vulnerabilităților lor și pentru a utiliza măsuri de gestionare a riscului în materie de securitate cibernetică de ultimă generație, precum și seturi de date care pot fi citite automat și interfețele corespunzătoare. Pentru a încuraja o cultură a divulgării vulnerabilităților, divulgarea nu ar trebui să aibă efecte negative asupra persoanei fizice sau juridice raportoare.

(63) Deși există registre sau baze de date ale vulnerabilităților similare, ele sunt găzduite și întreținute de entități care nu sunt stabilite în Uniune. O bază de date europeană a vulnerabilităților întreținută de ENISA ar oferi o mai mare transparență în ceea ce privește procesul de publicare înainte de dezvăluirea oficială a vulnerabilității, precum și reziliență în cazul unei perturbări sau al unei întreruperi ale furnizării de servicii similare. Pentru a evita, în măsura posibilului, dublarea eforturilor și pentru a urmări complementaritatea, ENISA ar trebui să analizeze posibilitatea de a încheia acorduri de cooperare structurată cu registre sau baze de date similare care intră sub jurisdicția unei țări terțe. În special, ENISA ar trebui să analizeze posibilitatea unei cooperări strânse cu operatorii sistemului comun de vulnerabilități și expuneri (CVE).

(64) Grupul de cooperare ar trebui să sprijine și să înlesnească cooperarea strategică și schimbul de informații, precum și să întărească încrederea între statele membre. Grupul de cooperare ar trebui să elaboreze un program de lucru o dată la doi ani. Programul de lucru ar trebui să includă acțiunile ce urmează să fie întreprinse de Grupul de cooperare în vederea punerii în aplicare a obiectivelor și sarcinilor sale. Calendarul pentru instituirea primului program de lucru în temeiul prezentei directive ar trebui să fie aliniat la calendarul ultimului program de lucru stabilit în temeiul Directivei (UE) 2016/1148, pentru a se evita eventualele perturbări ale activității Grupului de cooperare.

(65) Atunci când elaborează documente de orientare, Grupul de cooperare ar trebui, în mod consecvent, să inventarieze soluțiile și experiențele naționale, să evalueze impactul rezultatelor Grupului de cooperare asupra abordărilor naționale, să discute provocările legate de punerea în aplicare și să formuleze recomandări specifice, în special în ceea ce privește înlesnirea alinierii în transpunerea prezentei directive în statele membre, care să fie abordată printr-o mai bună punere în aplicare a normelor existente. Grupul de cooperare ar putea, de asemenea, să inventarieze soluțiile naționale pentru a promova compatibilitatea soluțiilor de securitate cibernetică aplicate în fiecare sector specific din întreaga Uniune. Acest lucru este deosebit de relevant pentru sectoarele care au un caracter internațional sau transfrontalier.

(66) Grupul de cooperare ar trebui să rămână un forum flexibil și să poată reacționa la prioritățile și provocările noi și în schimbare în materie de politici, ținând seama, în același timp, de disponibilitatea resurselor. Acesta ar putea organiza reuniuni comune periodice cu părțile interesate relevante din sectorul privat din întreaga Uniune pentru a discuta despre activitățile pe care le desfășoară Grupul de cooperare și a colecta date și informații cu privire la provocările emergente în materie de politici. În plus, Grupul de cooperare ar trebui să efectueze o evaluare periodică a situației amenințărilor sau incidentelor cibernetice, cum ar fi cele de tip *ransomware*. Pentru a întări cooperarea la nivelul Uniunii, Grupul de cooperare ar trebui să aibă în vedere invitarea instituțiilor, organelor, oficiilor și agențiilor

relevante ale Uniunii implicate în politica de securitate cibernetică, cum ar fi Parlamentul European, Europol, Comitetul european pentru protecția datelor, Agenția Uniunii Europene pentru Siguranța Aviației, instituită prin Regulamentul (UE) 2018/1139, și Agenția Uniunii Europene pentru Programul Spațial, instituită prin Regulamentul (UE) 2021/696 al Parlamentului European și al Consiliului ([14]), să participe la lucrările sale.

(67) Autoritățile competente și echipele CSIRT ar trebui să aibă posibilitatea să participe la programe de schimb pentru funcționari din alte state membre, într-un cadru specific și, după caz, sub rezerva autorizării de securitate necesare a funcționarilor care participă la aceste programe de schimb, în vederea îmbunătățirii cooperării și a întăririi încrederii dintre statele membre. Autoritățile competente ar trebui să ia măsurile necesare ca funcționarii din alte state membre să poată juca un rol efectiv în activitățile autorității competente gazdă sau ale echipelor CSIRT gazdă.

(68) Statele membre ar trebui să contribuie la instituirea cadrului UE de răspuns la crizele de securitate cibernetică, astfel cum este prevăzut în Recomandarea (UE) 2017/1584 a Comisiei ([15]), prin intermediul rețelelor de cooperare existente, în special Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe), rețeaua CSIRT și Grupul de cooperare. EU-CyCLONe și rețeaua CSIRT ar trebui să coopereze pe baza modalităților procedurale care precizează detaliile acestei cooperări și să evite orice suprapunere a sarcinilor. Regulamentul de procedură al EU-CyCLONe ar trebui să precizeze în detaliu modalitățile prin care ar trebui să funcționeze această rețea, inclusiv rolurile, mijloacele de cooperare, interacțiunile rețelei cu alți actori relevanți și modelele pentru schimbul de informații, precum și mijloacele de comunicare. Pentru gestionarea crizelor la nivelul Uniunii, părțile relevante ar trebui să se bazeze pe mecanismul integrat al UE pentru un răspuns politic la crize în temeiul Deciziei de punere în aplicare (UE) 2018/1993 a Consiliului ([16]) (mecanismul IPCR). În acest scop, Comisia ar trebui să utilizeze procesul ARGUS de coordonare transsectorială la nivel înalt în situații de criză. În cazul în care criza presupune o importantă dimensiune externă sau de politică de securitate și apărare comună, ar trebui activat mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă.

(69) În conformitate cu anexa la Recomandarea (UE) 2017/1584, un incident de securitate cibernetică de mare amploare ar trebui să însemne un incident care provoacă un nivel de perturbare care depășește capacitatea unui stat membru de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două state membre. În funcție de cauza și de impactul lor, incidentele de securitate cibernetică de mare amploare pot escalada și se pot transforma în crize de sine stătătoare, care să împiedice buna funcționare a pieței interne sau să prezinte riscuri grave pentru securitatea și siguranța publică, pentru entități sau cetățeni, în mai multe state membre sau în Uniune în ansamblul său. Având în vedere domeniul larg de aplicare și, în cele mai multe cazuri, natura transfrontalieră a unor astfel de incidente, statele membre și instituțiile, organele, oficiile și agențiile relevante ale Uniunii ar trebui să coopereze la nivel tehnic, operațional și politic pentru a coordona în mod corespunzător răspunsul în întreaga Uniune.

(70) Incidentele de securitate cibernetică de mare amploare și crizele de la nivelul Uniunii necesită acțiuni coordonate pentru a asigura un răspuns rapid și eficace, din cauza gradului ridicat de interdependență dintre sectoare și statele membre. Disponibilitatea unor rețele și sisteme informatice reziliente din punct de vedere cibernetic, precum și disponibilitatea, confidențialitatea și integritatea datelor sunt vitale pentru securitatea Uniunii și pentru protecția cetățenilor, întreprinderilor și instituțiilor acesteia împotriva incidentelor și a amenințărilor cibernetice, precum și pentru consolidarea încrederii persoanelor și a organizațiilor în capacitatea Uniunii de a promova și de a proteja un spațiu cibernetic global, deschis, liber, stabil și sigur, bazat pe drepturile omului, libertățile fundamentale, democrație și statul de drept.

([14]) Regulamentul (UE) 2021/696 al Parlamentului European și al Consiliului din 28 aprilie 2021 de instituire a Programului spațial al Uniunii și a Agenției Uniunii Europene pentru Programul spațial și de abrogare a Regulamentelor (UE) nr. 912/2010, (UE) nr. 1285/2013 și (UE) nr. 377/2014 și a Deciziei nr. 541/2014/UE (JO L 170, 12.5.2021, p. 69).

([15]) Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).

([16]) Decizia de punere în aplicare (UE) 2018/1993 a Consiliului din 11 decembrie 2018 privind mecanismul integrat al Uniunii pentru un răspuns politic la crize (JO L 320, 17.12.2018, p. 28).

(71) EU-CyCLONe ar trebui să acționeze ca intermediar între nivelul tehnic și cel politic în timpul incidentelor de securitate cibernetică de mare amploare și al crizelor și ar trebui să consolideze cooperarea la nivel operațional și să sprijine procesul decizional la nivel politic. În cooperare cu Comisia, având în vedere competența Comisiei în domeniul gestionării crizelor, EU-CyCLONe ar trebui să se bazeze pe constatările rețelei CSIRT și să își utilizeze propriile capacități pentru a crea o analiză a impactului incidentelor de securitate cibernetică de mare amploare și al crizelor.

(72) Atacurile cibernetice au un caracter transfrontalier, iar un incident semnificativ poate perturba și afecta infrastructurile critice de informații de care depinde buna funcționare a pieței interne. Recomandarea (UE) 2017/1584 abordează rolul tuturor actorilor relevanți. În plus, Comisia este responsabilă, în cadrul mecanismului de protecție civilă al Uniunii instituit prin Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului ([17]), de acțiunile generale în materie de pregătire, inclusiv de gestionarea Centrului de coordonare a răspunsului la situații de urgență și a sistemului comun de comunicare și informare în caz de urgență, de menținerea și dezvoltarea în continuare a capacității de conștientizare a situației și de analiză, precum și de instituirea și gestionarea capacității de a mobiliza și de a trimite echipe de experți în cazul unei cereri de asistență din partea unui stat membru sau a unei țări terțe. Comisia are, de asemenea, responsabilitatea de a furniza rapoarte analitice pentru mecanismul IPCR în temeiul Deciziei de punere în aplicare (UE) 2018/1993, inclusiv în ceea ce privește conștientizarea situației și pregătirea în materie de securitate cibernetică, precum și conștientizarea situației și răspunsul la situații de criză în domeniile agriculturii, condițiilor meteorologice nefavorabile, cartografierii și prognozelor privind conflictele, sistemelor de alertă timpurie în caz de dezastre naturale, urgențelor sanitare, supravegherii bolilor infecțioase, sănătății plantelor, incidentelor chimice, siguranței alimentelor și a hranei pentru animale, sănătății animalelor, migrației, vămilor, urgențelor nucleare și radiologice și energiei.

(73) După caz, Uniunea poate să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaționale cu țări terțe sau organizații internaționale, care să permită și să organizeze participarea acestora la anumite activități ale Grupului de cooperare, ale rețelei CSIRT, precum și ale EU-CyCLONe. Astfel de acorduri ar trebui să asigure interesele Uniunii și o protecție adecvată a datelor. Acest lucru nu ar trebui să excludă dreptul statelor membre de a coopera cu țări terțe în legătură cu gestionarea vulnerabilităților și a riscurilor în materie de securitate cibernetică, înlesnind raportarea și schimbul general de informații în conformitate cu dreptul Uniunii.

(74) Pentru a facilita punerea în aplicare eficace a prezentei directive în ceea ce privește, printre altele, gestionarea vulnerabilităților, măsurile de gestionare a riscurilor în materie de securitate cibernetică, obligațiile de raportare și acordurile privind schimbul de informații în materie de securitate cibernetică, statele membre pot coopera cu țări terțe și pot desfășura activități considerate a fi adecvate acestui scop, inclusiv schimburi de informații cu privire la amenințări cibernetice, incidente, vulnerabilități, instrumente și metode, tactici, tehnici și proceduri, pregătire și exerciții pentru gestionarea crizelor în materie de securitate cibernetică, formare, consolidare a încrederii și acorduri structurate privind schimbul de informații.

(75) Ar trebui introduse evaluări *inter pares* pentru a se putea învăța din experiențe comune, a consolida încrederea reciprocă și a atinge un nivel comun ridicat de securitate cibernetică. Evaluările *inter pares* pot conduce la idei și recomandări valoroase, consolidând capacitățile generale în materie de securitate cibernetică, creând o altă cale funcțională pentru schimbul de bune practici între statele membre și contribuind la îmbunătățirea nivelurilor de maturitate ale statelor membre în materie de securitate cibernetică. În plus, evaluările *inter pares* ar trebui să țină seama de rezultatele unor mecanisme similare, cum ar fi sistemul de evaluare *inter pares* al rețelei CSIRT, să aducă valoare adăugată și să evite suprapunerile. Implementarea sistemului de evaluări *inter pares* nu ar trebui să aducă atingere dreptului Uniunii sau dreptului intern privind protecția informațiilor confidențiale sau clasificate.

(76) Grupul de cooperare ar trebui să stabilească o metodologie de autoevaluare pentru statele membre, cu scopul de a acoperi factori precum nivelul de punere în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare, nivelul capacităților și eficacitatea exercitării sarcinilor autorităților competente, capacitățile operaționale ale echipelor CSIRT, nivelul de punere în aplicare a asistenței reciproce, nivelul de punere în aplicare a acordurilor privind schimbul de informații în materie de securitate cibernetică sau aspecte specifice de natură transfrontalieră sau transsectorială. Statele membre ar trebui să fie încurajate să efectueze autoevaluări în mod regulat și să prezinte și să discute rezultatele autoevaluării lor în cadrul Grupului de cooperare.

([17]) Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului din 17 decembrie 2013 privind un mecanism de protecție civilă al Uniunii (JO L 347, 20.12.2013, p. 924).

(77) Responsabilitatea de a asigura securitatea rețelelor și a sistemelor informatice revine în mare măsură entităților esențiale și entităților importante. Ar trebui să se promoveze și să se dezvolte o cultură a gestionării riscurilor, care să implice evaluări ale riscurilor și aplicarea unor măsuri de gestionare a riscurilor în materie de securitate cibernetică adecvate riscurilor întâmpinate.

(78) Măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să țină seama de gradul de dependență al entității esențiale sau al entității importante de rețelele și sistemele informatice și să includă măsuri pentru identificarea oricăror riscuri de incidente, prevenirea și detectarea incidentelor, răspunsul la incidente și redresarea în urma acestora, precum și pentru atenuarea impactului lor. Securitatea rețelelor și a sistemelor informatice ar trebui să includă securitatea datelor stocate, transmise și prelucrate. Măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să asigure o analiză sistemică, ținând seama de factorul uman, cu scopul de a obține o imagine completă privind securitatea rețelelor și a sistemelor informatice.

(79) Întrucât amenințările la adresa securității rețelelor și a sistemelor informatice pot avea origini diferite, măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie bazate pe o abordare multirisc, care vizează protecția rețelelor și a sistemelor informatice și a mediului fizic al acestor sisteme împotriva unor evenimente cum ar fi furturile, incendiile, inundațiile, defecțiunile la nivelul telecomunicațiilor sau al alimentării cu energie, accesul fizic neautorizat și deteriorarea și interferența la nivelul informațiilor deținute de o entitate esențială sau de o entitate importantă sau al echipamentelor entității respective de prelucrare a informațiilor, care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate sau a serviciilor oferite de rețelele și sistemele informatice sau accesibile prin intermediul acestora. Prin urmare, măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să abordeze, de asemenea, securitatea fizică și a mediului în cazul rețelelor și al sistemelor informatice prin includerea unor măsuri pentru a le proteja împotriva defecțiunilor de sistem, a erorilor umane, a acțiunilor răuvoitoare sau a fenomenelor naturale, în conformitate cu standardele europene și internaționale, cum ar fi cele incluse în seria ISO/IEC 27000. În acest sens, entitățile esențiale și entitățile importante ar trebui, în cadrul măsurilor lor de gestionare a riscurilor în materie de securitate cibernetică, să abordeze și securitatea resurselor umane și să dispună de politici adecvate de control al accesului. Măsurile respective ar trebui să respecte Directiva (UE) 2022/2557.

(80) Pentru a dovedi respectarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică și în absența unor sisteme europene adecvate de certificare a securității cibernetice adoptate în conformitate cu Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului ([18]), statele membre ar trebui, cu consultarea Grupului de cooperare și a Grupului european pentru certificarea securității cibernetice, să promoveze utilizarea standardelor europene și internaționale relevante de către entitățile esențiale și entitățile importante sau pot solicita entităților să utilizeze produse TIC, servicii TIC și procese TIC certificate.

(81) Pentru a se evita impunerea unei sarcini financiare și administrative disproporționate asupra entităților esențiale și entităților importante, măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri și, după caz, de standardele europene și internaționale relevante, precum și de costul punerii lor în aplicare.

(82) Măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie proporționale cu gradul de expunere a entității esențiale sau a entității importante la riscuri și cu impactul societal și economic pe care un incident l-ar avea. Atunci când se stabilesc măsuri de gestionare a riscurilor în materie de securitate cibernetică adaptate entităților esențiale și entităților importante, ar trebui să se țină seama în mod corespunzător de expunerea divergentă la risc a entităților esențiale și a entităților importante, cum ar fi importanța critică a entității, riscurile, inclusiv riscurile societale, la care este expusă, dimensiunea entității și probabilitatea producerii incidentelor și gravitatea acestora, inclusiv impactul lor societal și economic.

([18]) 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) (JO L 151, 7.6.2019, p. 15).

(83) Entitățile esențiale și entitățile importante ar trebui să asigure securitatea rețelelor și a sistemelor informatice pe care le utilizează pentru a-și desfășura activitatea. Aceste sisteme sunt în principal rețele și sisteme informatice private, care sunt gestionate de către personalul IT intern al entităților esențiale și al entităților importante sau a căror securitate a fost externalizată. Măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare prevăzute în prezenta directivă ar trebui să li se aplice entităților esențiale și entităților importante relevante, indiferent dacă entitățile respective întrețin la nivel intern rețelele și sistemele lor informatice sau dacă externalizează întreținerea acestora.

(84) Având în vedere caracterul lor transfrontalier, 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 ar trebui să facă obiectul unui grad ridicat de armonizare la nivelul Uniunii. Prin urmare, implementarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică în ceea ce privește respectivele entități ar trebui facilitată printr-un act de punere în aplicare.

(85) Abordarea riscurilor care decurg din lanțul de aprovizionare al unei entități și din relația acesteia cu furnizorii săi, cum ar fi furnizorii de servicii de stocare și de prelucrare de date sau furnizorii de servicii de securitate gestionate și editorii de software, este deosebit de importantă, având în vedere prevalența incidentelor în care entitățile au fost victime ale atacurilor cibernetice și în care actori răuvoitori au fost în măsură să compromită securitatea rețelelor și a sistemelor informatice ale unei entități prin exploatarea vulnerabilităților care afectează produsele și serviciile unei părți terțe. Prin urmare, entitățile esențiale și entitățile importante ar trebui să evalueze și să țină seama de calitatea generală și de reziliența produselor și a serviciilor, de măsurile de gestionare a riscurilor în materie de securitate cibernetică integrate în acestea, precum și de practicile în materie de securitate cibernetică ale furnizorilor și ale prestatorilor lor de servicii, inclusiv de procedurile lor de dezvoltare sigure. Entitățile esențiale și entitățile importante ar trebui, în special, să fie încurajate să includă măsuri de gestionare a riscurilor în materie de securitate cibernetică în acordurile contractuale cu furnizorii lor direcți și cu prestatorii lor de servicii direcți. Entitățile respective ar putea lua în considerare riscurile generate de alte niveluri de furnizori și de prestatori de servicii.

(86) În rândul furnizorilor de servicii, furnizorii de servicii de securitate gestionate în domenii precum răspunsul în caz de incidente, testele de penetrare, auditurile de securitate și consultanța joacă un rol deosebit de important în sprijinirea entităților în eforturile lor de a preveni și de a detecta incidente, de a răspunde la acestea și de a se redresa după incidente. Totuși, și furnizorii de servicii de securitate gestionate au fost ținta atacurilor cibernetice și, din cauza integrării lor strânse în operațiunile entităților, prezintă un risc deosebit. Prin urmare, entitățile esențiale și entitățile importante ar trebui să dea dovadă de o diligență sporită în selectarea unui furnizor de servicii de securitate gestionate.

(87) Autoritățile competente, în contextul sarcinilor lor de supraveghere, pot beneficia, de asemenea, de servicii de securitate cibernetică, cum ar fi audituri de securitate, teste de penetrare sau răspunsuri la incidente.

(88) Entitățile esențiale și entitățile importante ar trebui, de asemenea, să abordeze riscurile care decurg din interacțiunile și din relațiile lor cu alte părți interesate în cadrul unui ecosistem mai larg, inclusiv în ceea ce privește combaterea spionajului industrial și protejarea secretelor comerciale. În special, entitățile respective ar trebui să ia măsurile adecvate pentru a se asigura că activitatea lor de cooperare cu instituțiile academice și de cercetare se desfășoară în conformitate cu politicile lor în materie de securitate cibernetică și respectă bunele practici în ceea ce privește accesul și diseminarea în condiții de siguranță a informațiilor, în general, și protecția proprietății intelectuale, în special. În mod similar, având în vedere importanța și valoarea datelor pentru activitățile pe care le desfășoară entitățile esențiale și entitățile importante, atunci când se bazează pe servicii de transformare și de analiză a datelor furnizate de terți, entitățile respective ar trebui să ia toate măsurile adecvate de gestionare a riscurilor în materie de securitate cibernetică.

(89) Entitățile esențiale și entitățile importante ar trebui să adopte o gamă largă de practici de bază în materie de igienă cibernetică, cum ar fi principii „încredere zero”, actualizări ale software-ului, configurarea dispozitivelor, segmentarea rețelelor, gestionarea identității și a accesului sau sensibilizarea utilizatorilor, să organizeze cursuri pentru personalul lor și să crească gradul de informare cu privire la amenințările cibernetice, *phishing* sau tehnici de inginerie socială. În plus, entitățile respective ar trebui să își evalueze propriile capacități în materie de securitate cibernetică și, atunci când este cazul, să urmărească integrarea tehnologiilor de îmbunătățire a securității cibernetice, cum ar fi sisteme de inteligență artificială sau de învățare automată pentru a consolida capacitățile proprii și securitatea rețelelor și a sistemelor informatice.

(90) Pentru a aborda în continuare principalele riscuri din cadrul lanțului de aprovizionare și pentru a oferi asistență entităților esențiale și entitățile importante care își desfășoară activitatea în sectoarele reglementate de prezenta directivă în privința gestionării adecvate a riscurilor legate de lanțul de aprovizionare și de furnizori, Grupul de cooperare ar trebui să efectueze, în cooperare cu Comisia și ENISA și, după caz, după consultarea părților interesate relevante, inclusiv din industrie, evaluări coordonate ale riscurilor de securitate la nivelul lanțurilor de aprovizionare critice, astfel cum s-a procedat deja în cazul rețelelor 5G ca urmare a Recomandării (UE) 2019/534 a Comisiei ([19]), cu scopul de a identifica, pentru fiecare sector în parte, serviciile TIC, sistemele TIC sau produsele TIC critice, amenințările și vulnerabilitățile relevante. Astfel de evaluări coordonate ale riscurilor de securitate ar trebui să identifice măsurile, planurile de atenuare și cele mai bune practici împotriva dependențelor critice, a potențialelor puncte unice de defecțiune, a amenințărilor, a vulnerabilităților și a altor riscuri asociate lanțului de aprovizionare și ar trebui să exploreze modalități de a încuraja adoptarea lor pe scară mai largă de către entități esențiale și entități importante. Printre factorii de risc potențiali fără caracter tehnic, cum ar fi influența nejustificată a unei țări terțe asupra furnizorilor și a prestatorilor de servicii, în special în cazul modelelor alternative de guvernanță, se numără vulnerabilitățile ascunse sau „ușile secrete” și eventualele întreruperi sistemice ale aprovizionării, în special în cazul blocajelor tehnologice sau al dependenței de furnizori.

(91) Evaluările coordonate ale riscurilor de securitate din cadrul lanțurilor de aprovizionare critice, având în vedere caracteristicile sectorului în cauză, ar trebui să țină seama atât de factori tehnici, cât și, după caz, de factori fără caracter tehnic, inclusiv de cei definiți în Recomandarea (UE) 2019/534, în evaluarea coordonată de UE a riscurilor legate de securitatea cibernetică a rețelelor 5G și în setul de instrumente al UE privind securitatea cibernetică 5G convenit de Grupul de cooperare. Pentru a identifica lanțurile de aprovizionare care ar trebui să facă obiectul unei evaluări coordonate a riscurilor de securitate, ar trebui să se țină seama de următoarele criterii: (i) în ce măsură entitățile esențiale și entitățile importante utilizează și se bazează pe servicii TIC, sisteme TIC sau produse TIC critice specifice; (ii) relevanța serviciilor TIC, a sistemelor TIC sau a produselor TIC critice specifice pentru îndeplinirea funcțiilor critice sau sensibile, printre care se numără și prelucrarea datelor cu caracter personal; (iii) disponibilitatea unor servicii TIC, sisteme TIC sau produse TIC alternative; (iv) reziliența întregului lanț de aprovizionare cu servicii TIC, sisteme TIC sau produse TIC pe parcursul întregului lor ciclu de viață împotriva evenimentelor perturbatoare și (v) pentru serviciile TIC, sistemele TIC sau produsele TIC emergente, potențiala lor importanță viitoare pentru activitățile entităților. În plus, ar trebui să se pună un accent deosebit pe serviciile TIC, sistemele TIC sau produsele TIC care fac obiectul unor cerințe specifice impuse de țări terțe.

(92) Pentru a raționaliza obligațiile impuse furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului și prestatorilor de servicii de încredere în ceea ce privește securitatea rețelelor și a sistemelor lor informatice, precum și pentru a permite acestor entități și autorităților competente în temeiul Directivei (UE) 2018/1972 a Parlamentului European și a Consiliului ([20]) și, respectiv, al Regulamentului (UE) nr. 910/2014 să beneficieze de cadrul juridic instituit prin prezenta directivă, inclusiv desemnarea unei echipe CSIRT responsabile de gestionarea incidentelor, participarea autorităților competente în cauză la activitățile Grupului de cooperare și ale rețelei CSIRT, entitățile respective ar trebui să intre în domeniul de aplicare al prezentei directive. Prin urmare, dispozițiile corespunzătoare prevăzute în Regulamentul (UE) nr. 910/2014 și în Directiva (UE) 2018/1972 referitoare la impunerea de cerințe de securitate și de notificare pentru aceste tipuri de entități ar trebui eliminate. Normele privind obligațiile de raportare prevăzute în prezenta directivă nu ar trebui să aducă atingere nici Regulamentului (UE) 2016/679, nici Directivei 2002/58/CE.

(93) Obligațiile în materie de securitate cibernetică prevăzute în prezenta directivă ar trebui considerate a fi complementare cerințelor impuse prestatorilor de servicii de încredere în temeiul Regulamentului (UE) nr. 910/2014. Prestatorilor de servicii de încredere ar trebui să li se impună să ia toate măsurile adecvate și proporționale pentru a gestiona riscurile la care sunt expuse serviciile lor, inclusiv în ceea ce privește clienții și beneficiarii terți, și să raporteze incidentele în temeiul prezentei directive. Astfel de obligații în materie de securitate cibernetică și de raportare ar trebui să vizeze, de asemenea, protecția fizică a serviciilor prestate. Cerințele pentru prestatorii de servicii de încredere calificați prevăzute la articolul 24 din Regulamentul (UE) nr. 910/2014 continuă să se aplice.

([19]) Recomandarea (UE) 2019/534 a Comisiei din 26 martie 2019 intitulată „Securitatea cibernetică a rețelelor 5G” (JO L 88, 29.3.2019, p. 42).

([20]) Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (JO L 321, 17.12.2018, p. 36).

(94) Statele membre pot atribui rolul autorităților competente pentru serviciile de încredere organismelor de supraveghere în temeiul Regulamentului (UE) nr. 910/2014, pentru a asigura continuarea practicilor curente și pentru a valorifica cunoștințele și experiența dobândite odată cu aplicarea regulamentului respectiv. Într-un astfel de caz, autoritățile competente în temeiul prezentei directive ar trebui să coopereze îndeaproape și în timp util cu respectivele organisme de supraveghere prin schimburi de informații relevante, pentru a asigura supravegherea eficace și conformarea prestatorilor de servicii de încredere cu cerințele prevăzute în prezenta directivă și în Regulamentul (UE) nr. 910/2014. Dacă este cazul, echipa CSIRT sau autoritatea competentă în temeiul prezentei directive ar trebui să informeze imediat organismul de supraveghere în temeiul Regulamentului (UE) nr. 910/2014 cu privire la orice amenințare cibernetică semnificativă sau incident notificat care afectează serviciile de încredere, precum și cu privire la orice încălcare de către un prestator de servicii de încredere a prezentei directive. În scopul raportării, statele membre pot utiliza, după caz, punctul de intrare unic instituit pentru a realiza o raportare automată și comună a incidentelor atât către organismul de supraveghere în temeiul Regulamentului (UE) nr. 910/2014, cât și către echipa CSIRT sau autoritatea competentă în temeiul prezentei directive.

(95) După caz și pentru a evita perturbările inutile, orientările naționale existente adoptate pentru transpunerea normelor referitoare la măsurile de securitate prevăzute la articolele 40 și 41 din Directiva (UE) 2018/1972 ar trebui să fie luate în considerare la transpunerea prezentei directive, valorificând astfel cunoștințele și competențele deja dobândite în temeiul Directivei (UE) 2018/1972 privind măsurile de securitate și notificarea incidentelor. ENISA poate, de asemenea, să elaboreze orientări privind cerințele în materie de securitate și obligațiile de raportare pentru furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, pentru a facilita armonizarea și tranziția și pentru a reduce la minimum perturbările. Statele membre pot atribui rolul de autorități competente pentru comunicațiile electronice autorităților de reglementare naționale în temeiul Directivei (UE) 2018/1972, pentru a asigura continuarea practicilor curente și pentru a valorifica cunoștințele și experiența dobândite ca rezultat al punerii în aplicare a respectivei directive.

(96) Având în vedere importanța crescândă a serviciilor de comunicații interpersonale care nu se bazează pe numere, astfel cum sunt definite în Directiva (UE) 2018/1972, este necesar să se asigure că astfel de servicii fac, de asemenea, obiectul unor cerințe corespunzătoare în materie de securitate, în conformitate cu natura lor specifică și cu importanța lor economică. Pe măsură ce suprafața de atac continuă să se extindă, serviciile de comunicații interpersonale care nu se bazează pe numere, cum ar fi serviciile de mesagerie, devin vectori de atac larg răspândiți. Actorii răuvoitori utilizează platformele pentru a comunica și a atrage victimele să deschidă pagini web compromise, crescând așadar probabilitatea unor incidente care implică exploatarea datelor cu caracter personal și, prin extensie, securitatea rețelelor și a sistemelor informatice. Furnizorii serviciilor de comunicații interpersonale care nu se bazează pe numere ar trebui să asigure un nivel de securitate a rețelelor și a sistemelor informatice adecvat riscurilor prezentate. Având în vedere faptul că furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere nu exercită în mod normal un control efectiv asupra transmiterii semnalelor în rețea, gradul de risc aferent unor astfel de servicii poate fi considerat, în unele privințe, mai redus decât în cazul serviciilor tradiționale de comunicații electronice. Același lucru este valabil și pentru serviciile de comunicații interpersonale, astfel cum sunt definite în Directiva (UE) 2018/1972, care utilizează numere și care nu exercită un control efectiv asupra transmiterii semnalului.

(97) Piața internă depinde mai mult decât oricând de funcționarea internetului. Serviciile ale aproape tuturor entităților esențiale și entităților importante depind de serviciile furnizate pe internet. Pentru a asigura furnizarea fără probleme a serviciilor asigurate de entități esențiale și entități importante, este important ca toți furnizorii de rețele publice de comunicații electronice să dispună de măsuri adecvate în materie de securitate cibernetică și să raporteze incidentele semnificative legate de aceasta. Statele membre ar trebui să se asigure că securitatea rețelelor publice de comunicații electronice este menținută și că interesele lor vitale de securitate sunt protejate împotriva sabotajului și a spionajului. Întrucât conectivitatea internațională consolidează și accelerează digitalizarea competitivă a Uniunii și a economiei sale, incidentele care afectează cablurile de comunicații submarine ar trebui raportate echipei CSIRT sau, după caz, autorității competente. Strategia națională de securitate cibernetică ar trebui, după caz, să țină seama de securitatea cibernetică a cablurilor de comunicații submarine și să includă o inventariere a riscurilor potențiale în materie de securitate cibernetică și măsuri de atenuare pentru a asigura cel mai înalt nivel de protecție a acestora.

(98) Pentru a se garanta securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice accesibile publicului, ar trebui promovată utilizarea tehnologiilor de criptare, în special a criptării de la un capăt la altul, și a conceptelor de securitate centrate pe date, cum ar fi cartografierea, segmentarea, etichetarea, politica de acces și gestionarea accesului, precum și deciziile privind accesul automat. Atunci când este necesar, utilizarea criptării, în special a criptării de la un capăt la altul, ar trebui să fie obligatorie pentru furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, în conformitate cu principiile securității și confidențialității implicite și din momentul conceperii, în sensul prezentei directive. Utilizarea criptării de la un capăt la altul ar trebui să fie reconciliată cu competențele statelor membre de a asigura protecția intereselor lor esențiale în materie de securitate și de siguranță publică și de a permite prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor în conformitate cu dreptul Uniunii. Acest lucru nu ar trebui însă să slăbească criptarea de la un capăt la altul, care este o tehnologie esențială pentru protecția eficace a datelor și a confidențialității și pentru securitatea comunicațiilor.

(99) Pentru a proteja securitatea și a preveni abuzul și manipularea rețelelor publice de comunicații electronice și ale serviciilor de comunicații electronice accesibile publicului, ar trebui promovată utilizarea unor standarde de rutare sigure pentru a asigura integritatea și robustețea funcțiilor de rutare în întregul ecosistem al furnizorilor de servicii de acces la internet.

(100) Pentru a proteja funcționalitatea și integritatea internetului și pentru a promova securitatea și reziliența DNS, părțile interesate relevante, inclusiv entitățile din sectorul privat din Uniune, furnizorii de servicii de comunicații electronice accesibile publicului, în special furnizorii de servicii de acces la internet, și furnizorii de motoare de căutare online, ar trebui încurajate să adopte o strategie de diversificare a rezoluției DNS. În plus, statele membre ar trebui să încurajeze dezvoltarea și utilizarea unui serviciu european public și sigur de rezoluție a DNS.

(101) Prezenta directivă stabilește o abordare în mai multe etape a raportării incidentelor semnificative pentru a se ajunge la un echilibru adecvat între, pe de o parte, raportarea rapidă care contribuie la atenuarea unei eventuale răspândiri a incidentelor semnificative și le permite entităților esențiale și entităților importante să solicite asistență și, pe de altă parte, raportarea aprofundată, care permite extragerea unor învățăminte valoroase din incidentele individuale și îmbunătățește în timp reziliența cibernetică a entităților individuale și a unor sectoare întregi. În acest sens, prezenta directivă ar trebui să includă raportarea incidentelor care, pe baza unei evaluări inițiale efectuate de entitatea în cauză, ar putea cauza entității respective perturbări operaționale ale serviciilor sau pierderi financiare substanțiale sau ar putea afecta alte persoane fizice sau juridice, provocând prejudicii materiale sau morale considerabile. O astfel de evaluare inițială ar trebui să ia în considerare, printre altele, rețeaua și sistemele informatice afectate, în special importanța acestora în furnizarea serviciilor entității, gravitatea și caracteristicile tehnice ale unei amenințări cibernetice și orice vulnerabilitate subiacentă care este exploatată, precum și experiența entității în ceea ce privește incidente similare. Indicatori precum măsura în care funcționarea serviciului este afectată, durata unui incident sau numărul de destinatari afectați ai serviciilor ar putea juca un rol important în identificarea gravității perturbării operaționale a serviciului.

(102) Dacă entitățile esențiale sau entitățile importante iau cunoștință de un incident semnificativ, acestea ar trebui să aibă obligația de a transmite o alertă timpurie fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore. Această alertă timpurie ar trebui să fie urmată de o notificare a incidentului. Entitățile în cauză ar trebui să transmită o notificare a incidentului fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore din momentul în care au luat cunoștință de incidentul semnificativ, cu scopul, în special, de a actualiza informațiile transmise prin alerta timpurie și de a prezenta o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili. Un raport final ar trebui prezentat în termen de cel mult o lună de la notificarea incidentului. Alerta timpurie ar trebui să includă numai informațiile necesare pentru a aduce la cunoștința echipei CSIRT sau, după caz, a autorității competente incidentul semnificativ și pentru a permite entității în cauză să solicite asistență, dacă este necesar. O astfel de alertă timpurie, după caz, ar trebui să indice dacă se suspectează că incidentul semnificativ a fost cauzat de acte ilegale sau răuvoitoare și dacă este probabil să aibă un impact transfrontalier. Statele membre ar trebui să se asigure că obligația de a transmite respectiva alertă timpurie sau notificarea ulterioară a incidentului nu deviază resursele entității notificatoare de la activitățile legate de gestionarea incidentelor cărora ar trebui să li se acorde prioritate, pentru a preîntâmpina ca

obligațiile de raportare a incidentului fie să devieze resurse de la gestionarea răspunsului la incidente semnificative, fie să compromită în alt mod eforturile entității în acest sens. În cazul unui incident în desfășurare la momentul prezentării raportului final, statele membre ar trebui să se asigure că entitățile în cauză prezintă la momentul respectiv un raport privind progresele înregistrate și un raport final în termen de o lună de la gestionarea incidentului semnificativ.

(103) După caz, entitățile esențiale și entitățile importante ar trebui să comunice fără întârziere destinatarilor serviciilor lor orice măsură sau măsură corectivă pe care o pot lua pentru a atenua riscurile generate de o amenințare cibernetică semnificativă. Entitățile respective ar trebui, după caz și în special dacă este probabil ca amenințarea cibernetică semnificativă să se materializeze, să își informeze, de asemenea, destinatarii serviciilor cu privire la amenințarea în sine. Cerința de a informa destinatarii cu privire la amenințările cibernetice semnificative ar trebui îndeplinită cu maxima diligență posibilă, dar nu ar trebui să scutească entitățile respective de obligația de a lua, pe cheltuiala proprie, măsuri adecvate și imediate pentru a preveni sau remedia orice astfel de amenințare și pentru a restabili nivelul normal de securitate al serviciului. Furnizarea unor astfel de informații privind amenințările cibernetice semnificative la adresa securității destinatarilor serviciilor ar trebui să fie gratuită și informațiile ar trebui să fie redactate într-un limbaj ușor de înțeles.

(104) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului ar trebui să pună în aplicare securitatea din momentul conceperii și securitatea implicită și să își informeze destinatarii serviciilor cu privire la amenințările cibernetice semnificative și cu privire la măsurile pe care le pot lua pentru a-și proteja securitatea dispozitivelor și a comunicațiilor, de exemplu prin folosirea unor anumite tipuri de software sau de tehnologii de criptare.

(105) O abordare proactivă a amenințărilor cibernetice este o componentă vitală a măsurilor de gestionare a riscurilor în materie de securitate cibernetică, care ar trebui să permită autorităților competente să prevină în mod eficace materializarea amenințărilor cibernetice în incidente care pot cauza prejudicii materiale sau morale considerabile. În acest scop, notificarea amenințărilor cibernetice prezintă o importanță majoră. În acest sens, entitățile sunt încurajate să raporteze în mod voluntar amenințările cibernetice.

(106) Pentru a simplifica raportarea informațiilor solicitate în temeiul prezentei directive, precum și pentru a reduce sarcina administrativă pentru entități, statele membre ar trebui să pună la dispoziție mijloace tehnice, cum ar fi un punct de intrare unic, sisteme automatizate, formulare online, interfețe ușor de utilizat, modele, platforme specifice pentru utilizarea de către entități, indiferent dacă intră în domeniul de aplicare al prezentei directive sau nu, pentru transmiterea informațiilor relevante care trebuie raportate. Finanțarea din partea Uniunii în sprijinul punerii în aplicare a prezentei directive, în special în cadrul programului Europa digitală instituit prin Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului ([21]), ar putea include sprijin pentru punctele de intrare unice. În plus, entitățile se află adesea într-o situație în care, din cauza caracteristicilor sale, un anumit incident trebuie raportat mai multor autorități ca urmare a obligațiilor de notificare incluse în diferite instrumente juridice. Astfel de cazuri creează o sarcină administrativă suplimentară și ar putea conduce, de asemenea, la incertitudini în ceea ce privește formatul unor asemenea notificări și procedurile aferente acestora. În cazul în care se instituie un punct de intrare unic, statele membre sunt încurajate, de asemenea, să utilizeze respectivul punct de intrare unic pentru notificarea incidentelor de securitate solicitată în temeiul altor acte legislative ale Uniunii, cum ar fi Regulamentul (UE) 2016/679 și Directiva 2002/58/CE. Utilizarea unui astfel de punct de intrare unic pentru raportarea incidentelor de securitate în temeiul Regulamentului (UE) 2016/679 și al Directivei 2002/58/CE nu ar trebui să afecteze aplicarea dispozițiilor Regulamentului (UE) 2016/679 și ale Directivei 2002/58/CE, în special a celor referitoare la independența autorităților menționate în acestea. ENISA, în cooperare cu Grupul de cooperare, ar trebui să elaboreze modele comune de notificare prin intermediul unor orientări pentru a simplifica și a raționaliza informațiile care trebuie raportate în temeiul dreptului Uniunii și a reduce sarcina administrativă impusă entităților notificatoare.

(107) Atunci când există suspiciuni că un incident ar fi legat de activități infracționale grave în temeiul dreptului Uniunii sau al dreptului intern, statele membre ar trebui să încurajeze entitățile esențiale și entitățile importante, pe baza normelor aplicabile în materie de proceduri penale în conformitate cu dreptul Uniunii, să raporteze autorităților de aplicare a legii incidentele despre care există suspiciuni că ar avea un caracter infracțional grav. După caz și fără a aduce atingere normelor de protecție a datelor cu caracter personal aplicabile Europol, este de dorit ca procesul de coordonare dintre autoritățile competente și autoritățile de aplicare a legii din diferite state membre să fie facilitat de Centrul european de combatere a criminalității informatice (EC3) și de ENISA.

([21]) Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului din 29 aprilie 2021 de instituire a programului „Europa digitală” și de abrogare a Deciziei (UE) 2015/2240 (JO L 166, 11.5.2021, p. 1).

(108) În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente. În acest context, autoritățile competente ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante cu autoritățile menționate în Regulamentul (UE) 2016/679 și Directiva 2002/58/CE.

(109) Menținerea unor baze de date exacte și complete conținând datele de înregistrare a numelor de domenii (date WHOIS) și furnizarea unui acces legal la astfel de date sunt aspecte esențiale pentru a asigura securitatea, stabilitatea și reziliența DNS, sistem care, la rândul său, contribuie la un nivel comun ridicat de securitate cibernetică în întreaga Uniune. În acest scop specific, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să aibă obligația de a prelucra anumite date necesare pentru atingerea acestui scop. O astfel de prelucrare ar trebui să constituie o obligație legală în sensul articolului 6 alineatul (1) litera (c) din Regulamentul (UE) 2016/679. Respectiva obligație nu aduce atingere posibilității de a colecta date privind înregistrarea numelor de domenii în alte scopuri, de exemplu pe baza unor dispoziții contractuale sau a unor cerințe juridice stabilite în alte acte legislative ale Uniunii sau naționale. Obligația respectivă vizează realizarea unui set complet și exact de date de înregistrare și nu ar trebui să conducă la colectarea acelorași date de mai multe ori. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să coopereze pentru a evita duplicarea acestei sarcini.

(110) Disponibilitatea și accesibilitatea în timp util a datelor de înregistrare a numelor de domenii pentru solicitanții legitimi de acces sunt esențiale pentru prevenirea și combaterea utilizării abuzive a DNS, precum și pentru prevenirea și detectarea incidentelor și răspunsul la acestea. Prin solicitanți legitimi de acces se înțelege orice persoană fizică sau juridică care formulează o cerere în temeiul dreptului Uniunii sau al dreptului intern. Printre acestea se pot număra autoritățile competente în temeiul prezentei directive și cele care sunt competente în temeiul dreptului Uniunii sau al dreptului intern pentru prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor, precum și CERT sau echipele CSIRT. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să aibă obligația de a permite accesul legal al solicitanților legitimi de acces la date specifice de înregistrare a numelor de domenii, care sunt necesare în scopul cererii de acces, în conformitate cu dreptul Uniunii și cu dreptul intern. Cererea solicitanților legitimi de acces ar trebui să fie însoțită de o expunere de motive care să permită evaluarea necesității accesului la date.

(111) Pentru a asigura disponibilitatea unor date exacte și complete de înregistrare a numelor de domeniu, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să colecteze și să garanteze integritatea și disponibilitatea datelor de înregistrare a numelor de domenii. În special, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să stabilească politici și proceduri pentru colectarea și păstrarea unor date de înregistrare a numelor de domenii exacte și complete, precum și pentru prevenirea și corectarea datelor de înregistrare inexacte, în conformitate cu dreptul Uniunii privind protecția datelor. Respectivele politici și proceduri ar trebui să țină seama, în măsura posibilului, de standardele elaborate de structurile de guvernanță multipartite la nivel internațional. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să adopte și să pună în aplicare proceduri proporționale pentru a verifica datele de înregistrare a numelor de domenii. Aceste proceduri ar trebui să reflecte cele mai bune practici utilizate în domeniu și, în măsura posibilului, progresele înregistrate în domeniul identificării electronice. Printre exemplele de proceduri de verificare se pot număra controalele *ex ante* efectuate în momentul înregistrării și controalele *ex post* efectuate după înregistrare. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui, în special, să verifice cel puțin un mijloc de contact al solicitantului înregistrării.

(112) Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să aibă obligația de a pune la dispoziția publicului datele de înregistrare a numelor de domenii care nu intră în domeniul de aplicare al dreptului Uniunii privind protecția datelor, cum ar fi datele care se referă la persoanele juridice, în conformitate cu preambulul Regulamentului (UE) 2016/679. Pentru persoanele juridice, registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să pună la dispoziția publicului cel puțin numele solicitantului înregistrării și numărul de telefon de contact. Adresa de e-mail de contact ar trebui, de asemenea, publicată, cu condiția să nu conțină date cu caracter personal cum ar fi în cazul pseudonimelor de e-mail sau al conturilor funcționale. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui, de asemenea, să le permită solicitanților legitimi de acces, în conformitate cu legislația Uniunii privind protecția datelor, accesul legal la date specifice de înregistrare a numelor de domenii privind persoanele fizice. Statele membre ar trebui să solicite registrelor de nume TLD și entităților care furnizează servicii de înregistrare a numelor de domenii să răspundă fără întârzieri nejustificate solicitărilor de divulgare a datelor de înregistrare a numelor de domenii formulate de solicitanții legitimi de acces. Registrele de nume TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii ar trebui să stabilească politici și proceduri pentru

publicarea și divulgarea datelor de înregistrare, inclusiv acorduri privind nivelul serviciilor pentru a trata cererile de acces din partea solicitanților legitimi de acces. Respectivele politici și proceduri ar trebui să țină seama, în măsura posibilului, de orice orientări și standarde elaborate de structurile de guvernanță multipartite la nivel internațional. Procedura de acces ar putea include, de asemenea, utilizarea unei interfețe, a unui portal sau a unui alt instrument tehnic, scopul fiind furnizarea unui sistem eficient de solicitare și accesare a datelor de înregistrare. În vederea promovării unor practici armonizate pe piața internă, Comisia poate, fără a aduce atingere competențelor Comitetului european pentru protecția datelor, să ofere orientări cu privire la astfel de proceduri, care să țină seama, în măsura posibilului, de standardele elaborate de structurile de guvernanță multipartite la nivel internațional. Statele membre ar trebui să se asigure că toate tipurile de acces la datele de înregistrare a numelor de domenii cu caracter personal și fără caracter personal sunt gratuite.

(113) Entitățile care intră în domeniul de aplicare al prezentei directive ar trebui considerate ca fiind sub jurisdicția statului membru în care sunt stabilite. Totuși, ar trebui să se considere că furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice accesibile publicului intră sub jurisdicția statului membru în care își prestează serviciile. Ar trebui să se considere că 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 se află sub jurisdicția statului membru în care își au sediul principal în Uniune. Entitățile administrației publice ar trebui să intre sub jurisdicția statului membru care le-a instituit. În cazul în care entitatea furnizează servicii sau își are sediul în mai multe state membre, aceasta ar trebui să intre sub jurisdicția separată și concurentă a fiecăruia dintre respectivele state membre. Autoritățile competente din respectivele state membre ar trebui să coopereze, să își ofere asistență reciprocă și, după caz, să întreprindă acțiuni comune de supraveghere. În cazul în care statele membre își exercită jurisdicția, acestea nu ar trebui să aplice măsuri de asigurare a respectării legii sau sancțiuni de mai multe ori pentru același comportament, în conformitate cu principiul ne bis in idem.

(114) Pentru a ține seama de caracterul transfrontalier al serviciilor și operațiunilor furnizorilor de servicii DNS, ale registrelor de nume TLD, ale entităților care furnizează servicii de înregistrare a numelor de domenii, ale furnizorilor de servicii de *cloud computing*, ale furnizorilor de servicii de centre de date, ale furnizorilor de rețele de furnizare de conținut, ale furnizorilor de servicii gestionate, ale furnizorilor de servicii de securitate gestionate, precum și ale furnizorilor de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, doar un stat membru ar trebui să aibă jurisdicție asupra entităților respective. Jurisdicția ar trebui să fie atribuită statului membru în care entitatea respectivă își are sediul principal în Uniune. Criteriul stabilirii în sensul prezentei directive implică exercitarea efectivă a activității prin intermediul unor forme de instalare stabilă. Forma juridică a unor astfel de instalări stabile, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință. Respectarea acestui criteriu nu ar trebui să depindă de localizarea fizică a rețelei și a sistemelor informatice într-un anumit loc; prezența și utilizarea unor astfel de sisteme nu constituie, în sine, un astfel de sediu principal și, prin urmare, acestea nu sunt criterii decisive pentru stabilirea sediului principal. Sediul principal ar trebui considerat a fi în statul membru în care sunt luate în mod predominant deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică în Uniune. Acesta va corespunde, de regulă, locului în care se află administrația centrală a entităților din Uniune. Dacă un astfel de stat membru nu poate fi stabilit sau dacă astfel de decizii nu sunt luate în Uniune, sediul principal ar trebui considerat a fi în statul membru în care se desfășoară operațiunile de securitate cibernetică. Dacă un astfel de stat membru nu poate fi determinat, ar trebui să se considere că sediul principal se află în statul membru în care entitatea are sediul cu cel mai mare număr de angajați din Uniune. Dacă serviciile sunt prestate de un grup de întreprinderi, sediul principal al întreprinderii care exercită controlul ar trebui considerat drept sediul principal al grupului de întreprinderi.

(115) Dacă un serviciu DNS recurent accesibil publicului este furnizat de un furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului numai ca parte a serviciului de acces la internet, entitatea ar trebui să fie considerată a se afla sub jurisdicția tuturor statelor membre în care sunt furnizate serviciile sale.

(116) În cazul în care un furnizor de servicii DNS, un registru de nume TLD, o entitate care furnizează servicii de înregistrare a numelor de domenii, un furnizor de servicii de *cloud computing*, un furnizor de servicii de centru de date, un furnizor de rețele de furnizare de conținut, un furnizor de servicii gestionate, un furnizor de servicii de securitate gestionate sau un 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, oferă servicii în Uniune, acesta ar trebui să desemneze un reprezentant în Uniune. Pentru a determina dacă o astfel de entitate oferă servicii în cadrul Uniunii, ar trebui să se determine dacă entitatea intenționează să ofere servicii persoanelor din unul sau mai multe state membre. Simpla accesibilitate în Uniune a unui site al entității sau al unui intermediar ori disponibilitatea unei adrese de e-mail sau a altor date de contact sau utilizarea unei limbi folosite în general în țara terță în care este stabilită entitatea ar trebui să fie considerate insuficiente pentru a se confirma o astfel de intenție. Cu toate acestea, factori precum utilizarea unei limbi sau a unei monede utilizate în general în unul sau mai multe state membre cu posibilitatea de a comanda servicii în respectiva limbă ori menționarea unor clienți sau utilizatori din Uniune ar putea conduce la concluzia că entitatea intenționează să ofere servicii în Uniune. Reprezentantul ar trebui să acționeze în numele entității, iar autoritățile competente sau echipele CSIRT ar trebui să se poată adresa reprezentantului. Reprezentantul ar trebui să fie desemnat explicit printr-un mandat scris al entității pentru a acționa în numele acesteia în privința obligațiilor acesteia prevăzute în prezenta directivă, inclusiv în privința raportării incidentelor.

(117) Pentru a asigura o imagine de ansamblu clară asupra furnizorilor de servicii DNS, a registrelor de nume TLD, a entităților care furnizează servicii de înregistrare a numelor de domenii, a furnizorilor de servicii de *cloud computing*, a furnizorilor de servicii de centre de date, a furnizorilor de rețele de furnizare de conținut, a furnizorilor de servicii gestionate, a furnizorilor de servicii de securitate gestionate, precum și a furnizorilor de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, care furnizează servicii care intră în domeniul de aplicare al prezentei directive în întreaga Uniune, ENISA ar trebui să creeze și să mențină un registru al acestor entități, pe baza informațiilor primite de statele membre, dacă este cazul prin intermediul mecanismelor naționale instituite pentru ca entitățile să se poată înregistra. Punctele unice de contact ar trebui să înainteze către ENISA informațiile și orice modificare a acestora. Pentru a asigura acuratețea și exhaustivitatea informațiilor care urmează să fie incluse în acest registru, statele membre pot să transmită către ENISA informațiile disponibile în orice registru național cu privire la aceste entități. ENISA și statele membre ar trebui să ia măsuri pentru a facilita interoperabilitatea acestor registre, asigurând, în același timp, protecția informațiilor confidențiale sau clasificate. ENISA ar trebui să instituie protocoale adecvate de clasificare și gestionare a informațiilor pentru a asigura securitatea și confidențialitatea informațiilor divulgate și ar trebui să restricționeze accesul la informațiile respective, stocarea și transmiterea acestora către utilizatorii vizați.

(118) În cazul în care se face schimb de informații care sunt clasificate în conformitate cu dreptul Uniunii sau cu dreptul național ori astfel de informații sunt raportate sau partajate în alt mod în temeiul prezentei directive, ar trebui să se aplice normele corespunzătoare privind tratarea informațiilor clasificate. În plus, ENISA ar trebui să dispună de infrastructura, procedurile și normele în vigoare pentru a trata informațiile sensibile și clasificate în conformitate cu normele de securitate aplicabile pentru protecția informațiilor clasificate ale UE.

(119) Amenințările cibernetice devenind tot mai complexe și mai sofisticate, eficacitatea măsurilor de detectare a unor astfel de amenințări și prevenirea lor depinde în mare măsură de schimbul regulat de informații privind amenințările și vulnerabilitățile care are loc între entități. Schimbul de informații contribuie la creșterea gradului de sensibilizare cu privire la amenințările cibernetice, ceea ce, la rândul său, consolidează capacitatea entităților de a preveni materializarea unor astfel de amenințări în incidente și le permite entităților să controleze mai bine efectele incidentelor și să se redreseze mai eficient. În absența unor orientări la nivelul Uniunii, diverși factori par să fi împiedicat un astfel de schimb de informații, în special incertitudinea cu privire la compatibilitatea cu normele în materie de concurență și răspundere.

(120) Entitățile ar trebui încurajate și asistate de statele membre să își valorifice în mod colectiv cunoștințele individuale și experiența practică la nivel strategic, tactic și operațional, pentru a-și consolida capacitățile de a preveni, a detecta, a furniza un răspuns în mod adecvat la incidente și de a se redresa în urma acestora sau de a diminua impactul lor. Prin urmare, este necesar să se permită apariția, la nivelul Uniunii, a unor acorduri privind schimbul voluntar de informații în materie de securitate cibernetică. În acest scop, statele membre ar trebui să sprijine și să încurajeze în mod activ entitățile, precum cele care furnizează servicii de securitate cibernetică și de cercetare, precum și cele relevante care nu intră în domeniul de aplicare al prezentei directive, să participe la astfel de acorduri privind schimbul de informații în materie de securitate cibernetică. Aceste mecanisme ar trebui să fie stabilite în conformitate cu normele Uniunii în materie de concurență și cu dreptul Uniunii în materie de protecție a datelor.

(121) Prelucrarea datelor cu caracter personal, în măsura necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor de către entități esențiale și entitățile importante, ar putea fi considerată legală pe baza faptului că o astfel de prelucrare respectă o obligație legală care îi revine operatorului, în conformitate cu cerințele de la articolul 6 alineatul (1) litera (c) și de la articolul 6 alineatul (3) din Regulamentul (UE) 2016/679. Prelucrarea datelor cu caracter personal ar putea fi, de asemenea, necesară pentru interesele legitime urmărite de entitățile esențiale și entitățile importante, precum și de furnizorii de tehnologii și servicii de securitate care acționează în numele acestor entități, în temeiul articolului 6 alineatul (1) litera (f) din Regulamentul (UE) 2016/679, inclusiv în cazul în care o astfel de prelucrare este necesară pentru acordurile privind schimbul de informații în materie de securitate cibernetică sau pentru notificarea voluntară a informațiilor relevante în conformitate cu prezenta directivă. Măsuri legate de prevenirea, detectarea, identificarea, limitarea, analizarea și combaterea incidentelor, măsuri de sensibilizare cu privire la amenințările cibernetice specifice, schimbul de informații în contextul remedierii vulnerabilității și al divulgării coordonate a vulnerabilității, schimbul voluntar de informații cu privire la incidentele respective, precum și la amenințările și vulnerabilitățile cibernetice, indicatori de compromitere, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare ar putea necesita prelucrarea anumitor categorii de date cu caracter personal, cum ar fi adrese IP, localizatoare uniforme de resurse (URL), nume de domenii, adrese de e-mail și, în cazul în care acestea dezvăluie date cu caracter personal, marcaje temporale. Prelucrarea datelor cu caracter personal de către autoritățile competente, punctele unice de contact și echipele CSIRT ar putea constitui o obligație legală sau ar putea fi considerată necesară pentru îndeplinirea unei sarcini de interes public sau în exercitarea autorității publice cu care este învestit operatorul de date în temeiul articolului 6 alineatul (1) litera (c) sau (e) și al articolului 6 alineatul (3) din Regulamentul (UE) 2016/679 sau pentru urmărirea unui interes legitim al entităților esențiale și al entităților importante, astfel cum se menționează la articolul 6 alineatul (1) litera (f) din respectivul regulament. În plus, dreptul național ar putea stabili norme care să permită autorităților competente, punctelor unice de contact și echipelor CSIRT, în măsura în care acest lucru este necesar și proporțional pentru a asigura securitatea rețelelor și a sistemelor informatice ale entităților esențiale și ale entităților importante, să prelucreze categorii speciale de date cu caracter personal în conformitate cu articolul 9 din Regulamentul (UE) 2016/679, în special prin prevederea unor măsuri adecvate și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanelor fizice, inclusiv limitări tehnice privind reutilizarea acestor date și utilizarea unor măsuri de ultimă generație de securitate și de protejare a confidențialității, cum ar fi pseudonimizarea sau criptarea, în cazul în care anonimizarea poate afecta în mod semnificativ scopul urmărit.

(122) Pentru a consolida competențele și măsurile de supraveghere care contribuie la asigurarea respectării efective, prezenta directivă ar trebui să prevadă o listă minimă de acțiuni și măsuri de supraveghere prin care autoritățile competente pot supraveghea entitățile esențiale și entitățile importante. În plus, prezenta directivă ar trebui să stabilească o diferențiere între regimul de supraveghere al entităților esențiale și cel al entităților importante, în vederea asigurării unui echilibru echitabil al obligațiilor pentru entitățile respective și pentru autoritățile competente. Prin urmare, entitățile esențiale ar trebui să fie supuse unui regim de supraveghere ex ante și ex post cuprinzător, în timp ce entitățile importante ar trebui să fie supuse unui regim de supraveghere simplificat, doar ex post. Entitățile importante nu ar trebui, așadar, să aibă obligația să documenteze în mod sistematic respectarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică, în timp ce autoritățile competente ar trebui să pună în aplicare o abordare reactivă ex post a supravegherii și, prin urmare, să nu aibă o obligație generală de a supraveghea entitățile respective. Supravegherea *ex post* a entităților importante poate fi declanșată de dovezi, indicii sau informații aduse la cunoștința autorităților competente, cu privire la care aceste autorități consideră că sugerează potențiale încălcări ale prezentei directive. De exemplu, astfel de dovezi, indicii sau informații ar putea fi de tipul celor furnizate autorităților competente de către alte autorități, de entități, cetățeni, mass-media sau alte surse, sau informații aflate la dispoziția publicului, sau ar putea rezulta din alte activități desfășurate de autoritățile competente în îndeplinirea sarcinilor lor.

(123) Executarea sarcinilor de supraveghere de către autoritățile competente nu ar trebui să împiedice în mod inutil activitățile comerciale ale entității în cauză. În cazul în care autoritățile competente își îndeplinesc sarcinile de supraveghere în legătură cu entitățile esențiale, inclusiv efectuarea de inspecții la fața locului și supravegherea *ex situ*, investigarea încălcărilor prezentei directive și efectuarea de audituri de securitate sau scanări de securitate, ar trebui să reducă la minimum impactul asupra activităților economice ale entității în cauză.

(124) În exercitarea supravegherii *ex ante*, autoritățile competente ar trebui să fie în măsură să decidă cu privire la ierarhizarea utilizării măsurilor și mijloacelor de supraveghere de care dispun, în mod proporțional. Acest lucru implică faptul că autoritățile competente pot decide cu privire la o astfel de ierarhizare a priorităților pe baza metodologiilor de supraveghere care ar trebui să urmeze o abordare bazată pe riscuri. Mai precis, astfel de metodologii ar putea include criterii sau valori de referință pentru clasificarea entităților esențiale în categorii de risc, alături de măsuri de supraveghere corespunzătoare și mijloace recomandate pentru fiecare categorie de risc, cum ar fi utilizarea, frecvența sau tipul inspecțiilor la fața locului, al auditurilor de securitate specifice sau al

scanărilor de securitate, tipul de informații care trebuie solicitate și nivelul de detaliere al informațiilor respective. Astfel de metodologii de supraveghere ar putea fi, de asemenea, însoțite de programe de lucru și pot fi evaluate și revizuite periodic, inclusiv cu privire la aspecte precum alocarea resurselor și nevoile. În ceea ce privește entitățile administrației publice, competențele de supraveghere ar trebui exercitate în conformitate cu cadrele legislative și instituționale naționale.

(125) Autoritățile competente ar trebui să se asigure că sarcinile lor de supraveghere în legătură cu entitățile esențiale și entitățile importante sunt îndeplinite de profesioniști cu formare în domeniu, care să dețină competențele necesare pentru a îndeplini sarcinile respective, în special în ceea ce privește efectuarea de inspecții la fața locului și supravegherea *ex situ*, inclusiv identificarea deficiențelor din bazele de date, de hardware, firewall-uri, de criptare și de rețele. Inspecțiile respective și supravegherea respectivă ar trebui să se desfășoare într-un mod obiectiv.

(126) În cazuri justificate în mod corespunzător în care are cunoștință de o amenințare cibernetică semnificativă sau de un risc iminent, autoritatea competentă ar trebui să fie în măsură să ia decizii imediate de executare cu scopul de a preveni un incident sau de a răspunde la acesta.

(127) Pentru ca asigurarea respectării legii să fie eficace, ar trebui stabilită o listă minimă de competențe de asigurare a respectării legii care pot fi exercitate pentru încălcarea măsurilor de gestionare a riscurilor de securitate cibernetică și a obligațiilor de raportare prevăzute în prezenta directivă, stabilind un cadru clar și coerent pentru asigurarea respectării legii în întreaga Uniune. Ar trebui să se țină seama în mod corespunzător de natura, gravitatea și durata încălcării prezentei directive, de prejudiciile materiale sau morale cauzate, de caracterul intenționat al încălcării sau de comiterea din neglijență a încălcării, de acțiunile întreprinse pentru a preveni sau a atenua prejudiciul material sau moral, de gradul de responsabilitate sau de orice încălcare anterioară relevantă, de gradul de cooperare cu autoritatea competentă și de orice alt factor agravant sau atenuant. Măsurile de asigurare a respectării legii, inclusiv amenzile administrative, ar trebui să fie proporționale, iar aplicarea lor ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „carta”), inclusiv dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare.

(128) Prezenta directivă nu impune statelor membre să prevadă răspunderea penală sau civilă a persoanelor fizice care au responsabilitatea de a se asigura că o entitate respectă prezenta directivă pentru prejudiciile suferite de terți ca urmare a încălcării prezentei directive.

(129) Pentru a asigura respectarea efectivă a obligațiilor prevăzute în prezenta directivă, fiecare autoritate competentă ar trebui să aibă competența de a aplica sau de a solicita aplicarea de amenzi administrative.

(130) În cazul în care o amendă administrativă este aplicată unei entități esențiale sau unei entități importante care este o întreprindere, întreprinderea ar trebui înțeleasă ca fiind o întreprindere în conformitate cu articolele 101 și 102 din TFUE în aceste scopuri. În cazul în care o amendă administrativă se aplică unei persoane care nu este o întreprindere, autoritatea competentă ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al amenzii. Competența de a stabili dacă și în ce măsură autorităților publice ar trebui să li se poată aplica amenzi administrative ar trebui să revină statelor membre. Aplicarea unei amenzi administrative nu aduce atingere exercitării altor competențe de către autoritățile competente sau aplicarea altor sancțiuni prevăzute în normele naționale de transpunere a prezentei directive.

(131) Statele membre ar trebui să poată stabili norme privind sancțiunile penale pentru încălcarea normelor naționale de transpunere a prezentei directive. Cu toate acestea, aplicarea de sancțiuni penale pentru încălcări ale unor asemenea norme de drept intern și de sancțiuni administrative conexe nu ar trebui să ducă la încălcarea principiului *ne bis in idem*, astfel cum a fost interpretat de Curtea de Justiție a Uniunii Europene.

(132) În cazul în care prezenta directivă nu armonizează sancțiunile administrative sau în alte cazuri, acolo unde este necesar, de exemplu în cazul unei încălcări grave a prezentei directive, statele membre ar trebui să pună în aplicare un sistem care să prevadă sancțiuni efective, proporționale și cu efect de descurajare. Natura unor astfel de sancțiuni și caracterul lor penal sau administrativ ar trebui stabilite de dreptul intern.

(133) Pentru a consolida și mai mult eficacitatea și efectul de descurajare al măsurilor de asigurare a respectării legii aplicabile în cazul încălcării prezentei directive, autoritățile competente ar trebui să fie împuternicite să suspende temporar sau să solicite suspendarea temporară a unei certificări sau a unei autorizații privind o parte din serviciile relevante furnizate de o entitate esențială sau privind ansamblul acestor servicii și să ceară impunerea unei interdicții temporare de a exercita funcții de conducere de către orice persoană fizică la nivel de director executiv sau de reprezentant legal. Având în vedere gravitatea și impactul lor asupra activităților entităților și, în cele din urmă, asupra utilizatorilor, aceste suspendări sau interdicții temporare ar trebui aplicate numai proporțional cu gravitatea încălcării și ținând seama de circumstanțele fiecărui caz individual, inclusiv de caracterul intenționat al încălcării sau de comiterea din neglijență a încălcării și de orice măsuri luate pentru a preveni sau a atenua prejudiciul material sau moral. Astfel de suspendări sau interdicții temporare ar trebui aplicate doar în ultimă instanță, adică numai după ce celelalte măsuri relevante de asigurare a respectării legii prevăzute de prezenta directivă au fost epuizate și numai până în momentul în care entitățile cărora li se aplică iau măsurile necesare pentru a remedia deficiențele sau pentru a se conforma cerințelor autorității competente pentru care au fost aplicate aceste suspendări sau interdicții temporare. Impunerea unor astfel de suspendări sau interdicții temporare ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu carta, inclusiv dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare.

(134) Pentru a asigura respectarea de către entități a obligațiilor lor prevăzute în prezenta directivă, statele membre ar trebui să coopereze și să își acorde asistență reciprocă în ceea ce privește măsurile de supraveghere și de asigurare a respectării legii, în special dacă o entitate furnizează servicii în mai multe state membre sau dacă rețelele și sistemele sale informatice sunt situate într-un alt stat membru decât cel în care furnizează servicii. Atunci când acordă asistență, autoritatea competentă căreia i se adresează solicitarea ar trebui să ia măsuri de supraveghere sau de asigurare a respectării legii în conformitate cu dreptul intern. Pentru a asigura buna funcționare a asistenței reciproce în temeiul prezentei directive, autoritățile competente ar trebui să utilizeze Grupul de cooperare ca forum pentru discutarea cazurilor și a cererilor specifice de asistență.

(135) Pentru a asigura eficacitatea supravegherii și a asigurării respectării legii, îndeosebi într-o situație cu o dimensiune transfrontalieră, un stat membru care a primit o cerere de asistență reciprocă ar trebui ca, în limitele cererii respective, să ia măsuri adecvate de supraveghere și de asigurare a respectării legii în legătură cu entitatea care face obiectul cererii respective și care furnizează servicii sau deține o rețea și un sistem informatic pe teritoriul statului membru respectiv.

(136) Prezenta directivă ar trebui să stabilească norme de cooperare între autoritățile competente și autoritățile de supraveghere în conformitate cu Regulamentul (UE) 2016/679 pentru tratarea cazurilor de încălcare a prezentei directive în materie de date cu caracter personal.

(137) Prezenta directivă ar trebui să vizeze asigurarea unui nivel ridicat de responsabilitate pentru măsurile de gestionare a riscurilor în materie de securitate cibernetică și pentru obligațiile de raportare la nivelul entităților esențiale și al entităților importante. Din aceste motive, organele de conducere ale entităților esențiale și ale entităților importante ar trebui să aprobe măsurile privind riscurile în materie de securitate cibernetică și să supravegheze punerea lor în aplicare.

(138) Pentru a asigura un nivel comun ridicat de securitate cibernetică în întreaga Uniune pe baza prezentei directive, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei în ceea ce privește completarea prezentei directive prin specificarea categoriilor de entități esențiale și 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. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare ([22]). În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

([22]) JO L 123, 12.5.2016, p. 1.

(139) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentei directive, Comisiei ar trebui să i se confere competențe de executare pentru a stabili dispozițiile procedurale necesare pentru funcționarea Grupului de cooperare și cerințele tehnice și metodologice, precum și cerințele sectoriale referitoare la măsurile de gestionare a riscurilor în materie de securitate cibernetică, precum și pentru a specifica mai în detaliu tipul de informații, formatul și procedura de notificare a incidentelor, a amenințărilor cibernetice și a incidentelor evitate la limită și a comunicărilor de amenințări cibernetice semnificative, precum și cazurile în care un incident trebuie considerat semnificativ. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([23]).

(140) Comisia ar trebui să revizuiască periodic prezenta directivă, consultându-se cu părțile interesate, în special pentru a stabili dacă este adecvat să propună modificări ca urmare a evoluției condițiilor societale, politice, tehnologice sau de piață. În cadrul acestor revizuiri, Comisia ar trebui să evalueze relevanța dimensiunii entităților vizate și a sectoarelor, a subsectoarelor și a tipurilor de entități menționate în anexele la prezenta directivă pentru funcționarea economiei și a societății în ceea ce privește securitatea cibernetică. Comisia ar trebui să evalueze, printre altele, dacă furnizorii care intră în domeniul de aplicare al prezentei directive și care sunt desemnați drept platforme online foarte mari în sensul articolului 33 din Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului ([24]) ar putea fi identificați ca entități esențiale în temeiul prezentei directive.

(141) Prezenta directivă creează noi sarcini pentru ENISA, consolidând astfel rolul acesteia, și ar putea avea totodată drept rezultat o obligație a ENISA de a-și îndeplini sarcinile existente în temeiul Regulamentului (UE) 2019/881 la un nivel mai ridicat decât înainte. Pentru a se asigura că ENISA dispune de resursele financiare și umane necesare pentru a îndeplini sarcinile existente și cele noi, precum și pentru a îndeplini orice nivel mai ridicat de execuție a sarcinilor care rezultă din rolul său consolidat, bugetul său ar trebui majorat în consecință. În plus, pentru a asigura utilizarea eficientă a resurselor, ENISA ar trebui să beneficieze de o mai mare flexibilitate în ceea ce privește modul în care poate să aloce resurse la nivel intern pentru a-și îndeplini în mod eficace sarcinile și pentru a răspunde așteptărilor.

(142) Întrucât obiectivul prezentei directive, și anume obținerea unui nivel comun ridicat de securitate cibernetică în Uniune, nu poate fi realizat în mod satisfăcător de către statele membre, dar, având în vedere efectele acțiunii, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru realizarea obiectivului respectiv.

(143) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de cartă, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare. Dreptul la o cale de atac eficientă se extinde la beneficiarii serviciilor furnizate de entități esențiale și de entități importante. Prezenta directivă ar trebui să fie pusă în aplicare în conformitate cu drepturile și principiile menționate.

(144) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([25]) și a emis un aviz la 11 martie 2021 ([26]),

---

([23]) Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

([24]) Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale) (JO L 277, 27.10.2022 , p. 1).

([25]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

([26]) JO C 183, 11.5.2021, p. 3.

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiectul

(1) Prezenta directivă stabilește măsuri care vizează obținerea unui nivel comun ridicat de securitate cibernetică în Uniune, cu scopul de a îmbunătăți funcționarea pieței interne.

(2) În acest scop, prezenta directivă stabilește:

(a) obligațiile statelor membre de a adopta strategii naționale de securitate cibernetică și 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") și echipe de intervenție în caz de incidente de securitate informatică (denumite în continuare „echipe CSIRT");

(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 pentru entitățile identificate drept entități critice în temeiul Directivei (UE) 2022/2557;

(c) normele și obligațiile privind schimbul de informații în materie de securitate cibernetică;

(d) obligațiile în materie de supraveghere și de asigurare a respectării legii pentru statele membre.

Articolul 2

Domeniul de aplicare

(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.

(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;

(b) entitatea este singurul furnizor dintr-un stat membru al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice;

(c) perturbarea serviciului furnizat de entitate ar putea avea un impact semnificativ asupra siguranței publice, a securității publice sau a sănătății 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;

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

(f) entitatea este o entitate a administrației publice:

(i) la nivel central, astfel cum este definită de un stat membru în conformitate cu dreptul intern;

(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.

(3) Prezenta directivă se aplică entităților identificate ca fiind entități critice în temeiul Directivei (UE) 2022/2557, indiferent de dimensiunea lor.

(4) Prezenta directivă se aplică entităților care furnizează servicii de înregistrare a numelor de domenii, indiferent de dimensiunea lor.

(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.

(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.

(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.

(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.

(9) Alineatele (7) și (8) nu se aplică în cazul în care o entitate acționează ca prestator de servicii de încredere.

(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.

(11) Obligațiile prevăzute în prezenta directivă nu implică furnizarea de informații a căror divulgare ar contraveni intereselor esențiale ale statelor membre în materie de securitate națională, siguranță publică sau apărare.

(12) Prezenta directivă se aplică fără a aduce atingere Regulamentului (UE) 2016/679, Directivei 2002/58/CE, Directivelor 2011/93/UE ([27]) și 2013/40/UE ([28]) ale Parlamentului European și ale Consiliului și Directivei (UE) 2022/2557.

(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.

([27]) Directiva 2011/93/UE a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO L 335, 17.12.2011, p. 1).

([28]) Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8).

(14) Entitățile, autoritățile competente, punctele unice de contact și echipele CSIRT prelucrează datele cu caracter personal în măsura necesară pentru scopurile prezentei directive și 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 rețele publice de comunicații electronice sau de către furnizorii de servicii de comunicații electronice accesibile publicului se efectuează în conformitate cu dreptul Uniunii privind protecția datelor și cu dreptul Uniunii privind protejarea confidențialității, în special cu Directiva 2002/58/CE.

Articolul 3

Entități esențiale și entități importante

(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.

(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).

(3) Până la 17 aprilie 2025, statele membre întocmesc o listă a entităților esențiale și a entităților importante, precum și a entităților care furnizează servicii de înregistrare a numelor de domenii. Statele membre revizuiesc lista în mod regulat, cel puțin o dată la doi ani, și o actualizează atunci când este cazul.

(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:

(a) denumirea entității;

(b) adresa și datele de contact actualizate, inclusiv adresele de e-mail, gama de IP-uri și numerele de telefon;

(c) dacă este cazul, sectorul și subsectorul relevante menționate în anexa I sau II; precum și

(d) după caz, o listă a statelor membre în care furnizează servicii care intră în domeniul de aplicare al prezentei directive.

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.

Comisia, cu sprijinul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), oferă, fără întârzieri nejustificate, orientări și modele privind obligațiile prevăzute în prezentul alineat.

Statele membre pot institui mecanisme naționale prin care entitățile să se înregistreze.

(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

(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).

Articolul 4

Acte juridice sectoriale ale Uniunii

(1) În cazul în care actele juridice sectoriale ale Uniunii impun entităților esențiale sau entităților importante să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să notifice incidentele semnificative, iar cerințele respective au un efect cel puțin echivalent cu efectul obligațiilor prevăzute în prezenta directivă, dispozițiile relevante ale prezentei directive, inclusiv dispozițiile privind supravegherea și asigurarea respectării legii prevăzute în capitolul VII, nu se aplică acestor entități. În cazul în care actele juridice sectoriale ale Uniunii nu acoperă toate entitățile dintr-un anumit sector care intră în domeniul de aplicare al prezentei directive, dispozițiile relevante ale prezentei directive se aplică în continuare entităților care nu fac obiectul respectivelor acte juridice sectoriale ale Uniunii.

(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.

(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.

Articolul 5

Armonizarea minimă

Prezenta directivă nu împiedică statele membre să adopte sau să mențină dispoziții care asigură un nivel mai ridicat de securitate cibernetică, cu condiția ca aceste dispoziții să fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii.

Articolul 6

Definiții

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;

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;

3. „securitate cibernetică" înseamnă securitate cibernetică astfel cum este definită la articolul 2 alineatul (1) din Regulamentul (UE) 2019/881;

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;

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

6. „incident" înseamnă un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora;

7. „incident de securitate cibernetică de mare amploare" înseamnă un incident care provoacă un nivel de perturbare care depășește capacitatea unui stat membru de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două state membre;

8. „gestionarea incidentului" înseamnă toate acțiunile și procedurile care vizează prevenirea, detectarea, analizarea și limitarea unui incident, sau vizează răspunsul la acesta și redresarea în urma incidentului;

9. „risc" înseamnă potențialul de pierderi sau de perturbări cauzate de un incident și trebuie exprimat ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului;

10. „amenințare cibernetică" înseamnă o amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;

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;

12. „produs TIC" înseamnă un produs astfel cum este definit la articolul 2 punctul 12 din Regulamentul (UE) 2019/881;

13. „serviciu TIC" înseamnă un serviciu TIC astfel cum este definit la articolul 2 punctul 13 din Regulamentul (UE) 2019/881;

14. „proces TIC" înseamnă un proces TIC astfel cum este definit la articolul 2 punctul 14 din Regulamentul (UE) 2019/881;

15. „vulnerabilitate" înseamnă un punct slab, o susceptibilitate sau o deficiență a unor produse TIC sau a unor servicii TIC care poate fi exploatată de o amenințare cibernetică;

16. „standard" înseamnă un standard astfel cum este definit la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului ([29]);

17. „specificație tehnică" înseamnă o specificație tehnică astfel cum este definită la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012;

([29]) Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

18. „internet *exchange point*" înseamnă o facilitate a rețelei care permite interconectarea a mai mult de două rețele autonome independente (sisteme autonome), în special în scopul facilitării schimbului de trafic de internet, care furnizează interconectare doar pentru sisteme autonome și care nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre orice pereche de sisteme autonome participante și nici nu modifică sau interacționează într-un alt mod cu acest trafic;

19. „sistem de nume de domenii DNS" sau „DNS" înseamnă un sistem ierarhic și distribuit de atribuire de nume care face posibilă identificarea serviciilor și a resurselor de pe internet, permițând dispozitivelor utilizatorilor finali să utilizeze serviciile de rutare și conectivitate pe internet pentru a accesa serviciile și resursele respective;

20. „furnizor de servicii DNS" înseamnă o entitate care furnizează:

    (a) servicii de rezoluție a numelor de domenii recursive accesibile publicului pentru utilizatorii finali de internet; sau

    (b) servicii de rezoluție a numelor de domenii cu autoritate pentru utilizarea de către terți, cu excepția serverelor pentru nume primare;

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 și care este responsabilă cu administrarea TLD-ului, inclusiv cu înregistrarea numelor de domenii în cadrul TLD-ului și cu exploatarea tehnică a TLD-ului, inclusiv exploatarea serverelor sale de nume, întreținerea bazelor sale de date și distribuirea 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;

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;

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 ([30]);

24. „serviciu de încredere" înseamnă un serviciu de încredere astfel cum este definit la articolul 3 punctul 16 din Regulamentul (UE) nr. 910/2014;

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;

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;

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;

28. „piață online" înseamnă o piață online astfel cum este definită la articolul 2 litera (n) din Directiva 2005/29/CE a Parlamentului European și a Consiliului ([31]);

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 și al Consiliului ([32]);

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;

([30]) Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale (JO L 241, 17.9.2015, p. 1).

([31]) Directiva 2005/29/CE a Parlamentului European și a Consiliului din 11 mai 2005 privind practicile comerciale neloiale ale întreprinderilor de pe piața internă față de consumatori și de modificare a Directivei 84/450/CEE a Consiliului, a Directivelor 97/7/CE, 98/27/CE și 2002/65/CE ale Parlamentului European și ale Consiliului și a Regulamentului (CE) nr. 2006/2004 al Parlamentului European și al Consiliului („Directiva privind practicile comerciale neloiale") (JO L 149, 11.6.2005, p. 22).

([32]) Regulamentul (UE) 2019/1150 al Parlamentului European și al Consiliului din 20 iunie 2019 privind promovarea echității și a transparenței pentru întreprinderile utilizatoare de servicii de intermediere online (JO L 186, 11.7.2019, p. 57).

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;

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;

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;

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;

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;

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;

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;

38. „entitate” înseamnă o persoană fizică sau juridică constituită și recunoscută ca atare în temeiul dreptului intern al locului său de stabilire care poate, acționând în nume propriu, să exercite drepturi și să fie supusă unor obligații;

39. „furnizor de servicii gestionate” înseamnă o entitate care furnizează servicii legate de instalarea, gestionarea, funcționarea sau întreținerea produselor, rețelelor, infrastructurii, aplicațiilor TIC sau a oricăror alte rețele și sisteme informatice, prin intermediul asistenței sau al administrării active efectuate fie la sediul clienților, fie la distanță;

40. „furnizor de servicii de securitate gestionate” înseamnă un furnizor de servicii gestionate care efectuează sau furnizează asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică;

41. „organizație de cercetare” înseamnă o entitate care are ca obiectiv principal să desfășoare activități de cercetare aplicată sau de dezvoltare experimentală în vederea exploatării rezultatelor cercetării respective în scopuri comerciale, dar care nu include instituțiile de învățământ.

CAPITOLUL II

CADRE COORDONATE ÎN MATERIE DE SECURITATE CIBERNETICĂ

Articolul 7

Strategia națională de securitate cibernetică

(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:

(a) obiectivele și prioritățile strategiei de securitate cibernetică a statului membru, care acoperă în special sectoarele menționate în anexele I și II;

(b) un cadru de guvernanță pentru realizarea obiectivelor și priorităților menționate la litera (a) de la prezentul alineat, inclusiv politicile menționate la alineatul (2);

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

(d) un mecanism care să identifice activele și o evaluare a riscurilor din statul membru respectiv;

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

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

(g) un cadru de politică menit să asigure o mai bună coordonare între autoritățile competente în temeiul prezentei directive și al Directivei (UE) 2022/2557 în scopul schimbului de informații privind riscurile, amenințările cibernetice și incidentele, precum și privind riscurile, amenințările și incidentele fără caracter cibernetic și al exercitării sarcinilor de supraveghere, după caz;

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

(2) În cadrul strategiei naționale de securitate cibernetică, statele membre adoptă politici:

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

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

(c) de gestionare a vulnerabilităților, inclusiv promovarea și facilitarea divulgării coordonate a vulnerabilităților în temeiul articolului 12 alineatul (1);

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

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

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

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

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

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

(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.

(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.

Articolul 8

Autoritățile naționale competente și punctele unice de contact

(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).

(2) Autoritățile competente menționate la alineatul (1) monitorizează punerea în aplicare a prezentei directive la nivel național.

(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.

(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.

(5) Statele membre se asigură că autoritățile lor competente și punctele unice de contact dispun de resurse adecvate pentru a-și îndeplini în mod eficace și eficient atribuțiile și a realiza astfel obiectivele prezentei directive.

(6) Fiecare stat membru notifică fără întârzieri nejustificate Comisiei identitatea autorității competente menționate la alineatul (1) și a punctului unic de contact menționat la alineatul (3), sarcinile respectivelor autorități și orice modificare ulterioară a acestora. Fiecare stat membru face publică identitatea autorității sale competente. Comisia face publică lista punctelor unice de contact.

Articolul 9

Cadrele naționale de gestionare a crizelor cibernetice

(1) Fiecare stat membru desemnează sau instituie una sau mai multe autorități competente responsabile cu gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor (denumite în continuare „autorități de gestionare a crizelor cibernetice”). Statele membre se asigură că respectivele autorități dispun de resurse adecvate pentru a îndeplini, în mod eficace și eficient, sarcinile care le-au fost încredințate. Statele membre asigură corelarea cu cadrele existente pentru gestionarea națională generală a crizelor.

(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.

(3) Fiecare stat membru identifică capacitățile, mijloacele și procedurile care pot fi utilizate în caz de criză în sensul prezentei directive.

(4) Fiecare stat membru adoptă un plan național de răspuns la incidente de securitate cibernetică de mare amploare și crize, în care sunt stabilite obiectivele și modalitățile de gestionare a incidentelor de securitate cibernetică de mare amploare și a crizelor. Planul respectiv stabilește, în special:

(a) obiectivele măsurilor și ale activităților naționale 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 naționale 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 statului membru la gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare și a crizelor la nivelul Uniunii și sprijinul acordat de acesta.

(5) În termen de trei luni de la desemnarea sau instituirea autorității de gestionare a crizelor cibernetice menționate la alineatul (1), fiecare stat membru notifică Comisiei identitatea autorității sale și orice modificări ulterioare ale acesteia. Statele membre prezintă Comisiei și Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) informații relevante referitoare la cerințele de la alineatul (4) cu privire la planurile lor naționale de răspuns la incidente de securitate cibernetică de mare amploare și crize, în termen de trei luni de la adoptarea planurilor respective. Statele membre pot exclude informații în cazul și în măsura în care o asemenea excludere este necesară pentru securitatea lor națională.

Articolul 10

Echipele de intervenție în caz de incidente de securitate informatică (echipe CSIRT)

(1) Fiecare stat membru desemnează sau instituie una sau mai multe echipe CSIRT. Echipele CSIRT pot fi desemnate sau instituite din cadrul unei autorități competente. Echipele CSIRT respectă cerințele prevăzute la articolul 11 alineatul (1), acoperă cel puțin sectoarele, subsectoarele și tipurile de entități menționate în anexele I și II și sunt responsabile de gestionarea incidentelor în conformitate cu o procedură bine definită.

(2) Statele membre se asigură că fiecare echipă CSIRT dispune de resurse adecvate pentru a-și îndeplini efectiv sarcinile stabilite la articolul 11 alineatul (3).

(3) Statele membre se asigură că fiecare echipă CSIRT dispune de o infrastructură de comunicare și de informații adecvată, sigură și reziliență 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.

(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.

(5) Echipele CSIRT participă la evaluările *inter pares* organizate în conformitate cu articolul 19.

(6) Statele membre asigură cooperarea efectivă, eficientă și sigură a propriilor echipe CSIRT 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.

(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.

(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.

(10) Statele membre pot solicita asistența ENISA pentru instituirea echipelor lor CSIRT.

Articolul 11

Cerințele pe care trebuie să le respecte, capacitățile tehnice și sarcinile care le revin echipelor CSIRT

(1) Echipele CSIRT trebuie să respecte 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;

(b) localurile echipelor CSIRT și sistemele informatice de suport sunt situate 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;

(d) echipele CSIRT asigură 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;

(f) echipele CSIRT sunt echipate cu sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor lor.

Echipele CSIRT pot participa la rețele internaționale de cooperare.

(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.

(3) Echipelor CSIRT le revin următoarele sarcini:

(a) monitorizarea și analizarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor la nivel național și, la cerere, acordarea de asistență entităților esențiale și entităților importante implicate cu privire la monitorizarea în timp real sau în timp aproape real a rețelei lor și a sistemelor lor informatice;

(b) asigurarea unor mecanisme de avertizare timpurii, alerte, anunțuri și diseminare de informații către entitățile esențiale și entitățile importante, precum și către autoritățile competente și alte părți interesate relevante cu privire la amenințările cibernetice, vulnerabilități și incidente, în timp aproape real, dacă este posibil;

(c) răspunsul la incidente și acordarea de asistență entităților esențiale și entitățile importante implicate, atunci când este cazul;

(d) colectarea și analizarea datelor criminalistice și furnizarea de analize dinamice de risc și de incident și conștientizarea situației în materie de securitate cibernetică;

(e) furnizarea, la cererea unei entități esențiale sau a unei entități importante, a unei scanări proactive a rețelelor și a sistemelor informatice ale entității implicate pentru a detecta vulnerabilitățile cu un impact potențial semnificativ;

(f) participarea la rețeaua CSIRT și furnizarea de asistență reciprocă în funcție de capacitățile și competențele lor altor membri ai rețelei, la cererea acestora;

(g) după caz, acționarea în calitate de coordonator în scopul procesului de divulgare coordonată a vulnerabilităților menționat la articolul 12 alineatul (1);

(h) contribuirea la implementarea unor instrumente securizate de schimb de informații, în temeiul articolului 10 alineatul (3).

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.

Atunci când îndeplinesc sarcinile menționate la primul paragraf, echipele CSIRT pot acorda prioritate anumitor sarcini pe baza unei abordări bazate pe riscuri.

(4) Echipele CSIRT stabilesc relații de cooperare cu părțile interesate relevante din sectorul privat, în vederea îndeplinirii obiectivelor prezentei directive.

(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:

(a) procedurile de gestionare a incidentelor;

(b) gestionarea crizelor; și

(c) divulgarea coordonată a vulnerabilităților în temeiul articolului 12 alineatul (1).

Articolul 12

Divulgarea coordonată a vulnerabilităților și baza de date europeană a vulnerabilităților

(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:

(a) identificarea și contactarea entităților implicate;

(b) asistarea persoanelor fizice sau juridice care raportează o vulnerabilitate;

(c) negocierea calendarelor de divulgare și gestionarea 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 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.

(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 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.

Articolul 13

Cooperarea la nivel național

(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.

(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.

(3) Statele membre se asigură că echipele sale CSIRT sau, atunci când este cazul, autoritățile sale competente informează punctele lor unice de contact cu privire la notificările privind incidentele, amenințările cibernetice și incidentele evitate la limită comunicate în temeiul prezentei directive.

(4) Pentru a garanta că sarcinile și obligațiile autorităților competente, ale punctelor unice de contact și ale echipelor CSIRT sunt îndeplinite în mod eficient, statele membre asigură, în măsura posibilului, o cooperare adecvată între aceste organisme și autoritățile de aplicare a legii, autoritățile pentru protecția datelor, autoritățile naționale în temeiul Regulamentelor (CE) nr. 300/2008 și (UE) 2018/1139, organismele de supraveghere în temeiul Regulamentului (UE) nr. 910/2014, autoritățile competente în temeiul Regulamentului (UE) 2022/2554, autoritățile naționale de reglementare în temeiul Directivei (UE) 2018/1972, autoritățile competente în temeiul Directivei (UE) 2022/2557, precum și autoritățile competente în temeiul altor acte juridice sectoriale ale Uniunii, din statul membru respectiv.

(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.

(6) Statele membre simplifică raportarea prin mijloace tehnice pentru notificările menționate la articolele 23 și 30.

CAPITOLUL III

COOPERARE LA NIVELUL UNIUNII ȘI LA NIVEL INTERNAȚIONAL

Articolul 14

Grupul de cooperare

(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.

(2) Grupul de cooperare își îndeplinește sarcinile pe baza programelor bienale de lucru menționate la alineatul (7).

(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.

După caz, Grupul de cooperare poate invita să participe la lucrările sale Parlamentul European și reprezentanți ai părților interesate relevante.

Comisia asigură secretariatul.

(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;

(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 și cooperarea cu Comisia cu privire la inițiativele emergente de politică în materie de securitate cibernetică, precum și coerența generală a cerințelor de securitate cibernetică specifice fiecărui sector;

(e) schimbul de opinii și 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 și de informații cu instituțiile, organele, oficiile și agențiile relevante ale Uniunii;

(g) schimbul de opinii cu privire la punerea în aplicare a actelor juridice sectoriale ale Uniunii care conțin dispoziții privind securitatea cibernetică;

(h) atunci când este cazul, discutarea rapoartelor privind evaluarea *inter pares* menționate la articolul 19 alineatul (9) și stabilirea de concluzii și recomandări;

(i) efectuarea unor evaluări coordonate ale riscurilor de securitate la nivelul lanțurilor de aprovizionare critice, în conformitate cu articolul 22 alineatul (1);

(j) discutarea cazurilor de asistență reciprocă, inclusiv a experiențelor și rezultatelor acțiunilor comune de supraveghere transfrontaliere, astfel cum se menționează la articolul 37;

(k) la cererea unuia sau a mai multor state membre în cauză, discutarea cererilor specifice de asistență reciprocă astfel cum se menționează la articolul 37;

(l) furnizarea de orientări strategice rețelei CSIRT și EU-CyCLONe cu privire la aspecte emergente specifice;

(m) schimbul de opinii cu privire la politica privind acțiunile ulterioare incidentelor de securitate cibernetică de mare amploare și 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.

(5) Statele membre asigură cooperarea eficace, eficientă și sigură a reprezentanților lor în Grupul de cooperare.

(6) Grupul de cooperare poate solicita rețelei CSIRT un raport tehnic pe anumite teme.

(7) Până la 1 februarie 2024 și, ulterior, o dată la doi ani, Grupul de cooperare stabilește un program de lucru cu privire la acțiunile care urmează să fie întreprinse pentru punerea în aplicare a obiectivelor și a sarcinilor sale.

(8) Comisia poate adopta acte de punere în aplicare prin care se stabilesc acordurile procedurale necesare pentru funcționarea Grupului de cooperare.

Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 39 alineatul (2).

Comisia face schimb de opinii și cooperează cu Grupul de cooperare în ceea ce privește proiectele de acte de punere în aplicare menționate la primul paragraf de la prezentul alineat, în conformitate cu alineatul (4) litera (e).

(9) Grupul de cooperare se reunește periodic, și în toate cazurile cel puțin o dată pe an, cu Grupul privind reziliența entităților critice instituit în temeiul Directivei (UE) 2022/2557 pentru a promova și facilita cooperarea strategică și schimbul de informații.

Articolul 15

Rețeaua CSIRT

(1) Pentru a contribui la dezvoltarea încrederii și pentru a promova cooperarea operațională rapidă și eficace între statele membre, se stabilește o rețea a echipelor naționale CSIRT.

(2) Rețeaua echipelor CSIRT este formată din reprezentanți ai echipelor CSIRT desemnate sau instituite în temeiul articolului 10 și din Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE). Comisia participă la rețeaua CSIRT în calitate de observator. ENISA asigură secretariatul și acordă asistență în mod activ pentru cooperarea între echipele CSIRT.

(3) Rețelei CSIRT îi revin următoarele sarcini:

(a) schimbul de informații privind capacitățile echipelor CSIRT;

(b) facilitarea partajării, transferului și schimbului de tehnologie și măsuri, politici, instrumente, procese, bune practici și cadre relevante între echipele CSIRT;

(c) schimbul de informații relevante privind incidentele, incidentele evitate la limită, amenințările cibernetice, riscurile și vulnerabilitățile;

(d) schimbul de informații în ceea ce privește publicațiile și 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) și, după caz, solicitarea de orientări în acest sens;

(l) bilanțul exercițiilor de securitate cibernetică, inclusiv al celor organizate de ENISA;

(m) la cererea unei anumite echipe CSIRT, discutarea capacităților și a nivelului de pregătire al echipei CSIRT respective;

(n) cooperarea și schimbul de informații cu centrele de operațiuni de securitate la nivel regional și la nivelul Uniunii pentru a îmbunătăți conștientizarea comună a situației cu privire la incidentele și amenințările cibernetice din întreaga Uniune;

(o) atunci când este cazul, discutarea rapoartelor privind evaluarea *inter pares* menționate la articolul 19 alineatul (9);

(p) oferirea de orientări pentru a facilita convergența practicilor operaționale în ceea ce privește aplicarea dispozițiilor prezentului articol referitoare la cooperarea operațională.

(4) Până la 17 ianuarie 2025 și, ulterior, o dată la doi ani, rețeaua CSIRT evaluează, în scopul revizuirii menționate la articolul 40, progresele înregistrate în ceea ce privește cooperarea operațională și adoptă un raport. Raportul formulează, în special, concluzii și recomandări pe baza rezultatelor evaluărilor *inter pares* menționate la articolul 19, care sunt efectuate în legătură cu echipele naționale CSIRT. Raportul respectiv se transmite Grupului de cooperare.

(5) Rețeaua CSIRT își adoptă regulamentul de procedură.

(6) Rețeaua CSIRT și EU-CyCLONe convin asupra modalităților procedurale și cooperează pe baza acestora.

Articolul 16

Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU - CyCLONe)

(1) EU-CyCLONe este instituită 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, organele, oficiile și agențiile Uniunii.

(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.

ENISA asigură secretariatul EU-CyCLONe și sprijină schimbul securizat de informații și, de asemenea, furnizează instrumentele necesare pentru sprijinirea cooperării dintre statele 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.

(3) EU-CyCLONe are următoarele sarcini:

(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.

(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.

(6) EU-CyCLONe cooperează cu rețeaua CSIRT pe baza modalităților procedurale convenite prevăzute la articolul 15 alineatul (6).

(7) Până la 17 iulie 2024 și, ulterior, la fiecare 18 luni, EU-CyCLONe prezintă un raport Parlamentului European și Consiliului în care își evaluează activitatea.

Articolul 17

Cooperarea internațională

După caz, Uniunea poate să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaționale cu țări terțe sau organizații internaționale, care să permită și să organizeze participarea acestora la anumite activități ale Grupului de cooperare, ale rețelei CSIRT, precum și ale EU-CyCLONe. Aceste acorduri respectă dreptul Uniunii în materie de protecție a datelor.

Articolul 18

Raportul privind situația în materie de securitate cibernetică în Uniune

(1) ENISA adoptă, în cooperare cu Comisia și Grupul de cooperare, un raport bienal privind situația în materie de securitate cibernetică în Uniune și înaintează și prezintă respectivul raport Parlamentului European. Raportul este, printre altele, pus la dispoziție într-un format citibil automat și include următoarele:

(a) o evaluare a riscurilor în materie de securitate cibernetică la nivelul Uniunii, ținând seama de situația amenințărilor cibernetice;

(b) o evaluare a dezvoltării capacităților în materie de securitate cibernetică în sectorul public și cel privat în întreaga Uniune;

(c) o evaluare a nivelului general de sensibilizare cu privire la securitatea cibernetică și igiena cibernetică în rândul cetățenilor și entităților, inclusiv al întreprinderilor mici și mijlocii;

(d) o evaluare globală a rezultatelor evaluărilor *inter pares* menționate la articolul 19;

(e) o evaluare globală a nivelului de maturitate a capacităților și a resurselor în materie de securitate cibernetică în întreaga Uniune, inclusiv a celor de la nivel sectorial, precum și a gradului de aliniere a strategiilor naționale de securitate cibernetică ale statelor membre.

(2) Raportul include recomandări de politică specifice pentru a aborda deficiențele și a îmbunătăți nivelul de securitate cibernetică în întreaga Uniune și un rezumat al constatărilor pentru perioada respectivă incluse în rapoartele UE privind situația tehnică în materie de securitate cibernetică cu privire la incidente și amenințări 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 și rețeaua CSIRT, elaborează metodologia, inclusiv variabilele relevante, cum ar fi indicatori cantitativi și calitativi, pentru evaluarea globală menționată la alineatul (1) litera (e).

Articolul 19

Evaluări inter pares

(1) Grupul de cooperare stabilește, până la 17 ianuarie 2025, cu sprijinul Comisiei și al ENISA și, după caz, al rețelei CSIRT, metodologia și aspectele organizatorice ale evaluărilor *inter pares* pentru a învăța din experiențele comune, a consolida încrederea reciprocă, a atinge un nivel comun ridicat de securitate cibernetică, precum și a consolida capacitățile și 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 experți în materie de securitate cibernetică. Experții în materie de securitate cibernetică sunt desemnați de cel puțin două state membre, diferite de statul membru care face obiectul evaluării.

Evaluările *inter pares* acoperă cel puțin unul din următoarele elemente:

(a) nivelul punerii în aplicare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare menționate la articolele 21 și 23;

(b) nivelul capacităților, inclusiv resursele financiare, tehnice și umane disponibile, precum și eficacitatea exercitării sarcinilor autorităților competente;

(c) capacitățile operaționale ale echipelor 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.

CAPITOLUL IV

MĂSURI DE GESTIONARE A RISCURILOR ÎN MATERIE DE SECURITATE CIBERNETICĂ ȘI OBLIGAȚII DE RAPORTARE

Articolul 20

Guvernanța

(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.

(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.

Articolul 21

Măsuri de gestionare a riscurilor în materie de securitate cibernetică

(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 beneficiarilor serviciilor lor și asupra altor servicii.

Ținând seama de cele mai avansate standarde în domeniu și, atunci când este cazul, de standardele europene și internaționale relevante, precum și de costul punerii în aplicare, măsurile menționate la primul paragraf asigură un nivel de securitate a rețelelor și a sistemelor informatice corespunzător riscurilor prezentate. Atunci când se evaluează proporționalitatea acestor măsuri, se ține seama în mod corespunzător de gradul de expunere a entității la riscuri, de dimensiunea entității și de probabilitatea producerii incidentelor, precum și de gravitatea acestora, inclusiv de impactul lor societal 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:

(a) politici referitoare la analiza riscurilor și securitatea sistemelor informatice;

(b) gestionarea incidentelor;

(c) continuitatea activității, de exemplu gestionarea copiilor de rezervă și recuperarea în caz de dezastru, precum și gestionarea 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;

(e) securitatea în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice, inclusiv gestionarea vulnerabilităților și divulgarea acestora;

(f) politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor în materie de securitate cibernetică;

(g) practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice;

(h) politici și proceduri privind utilizarea criptografiei și, după caz, a criptării;

(i) 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.

(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 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).

(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.

(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 schimb de opinii și cooperează cu Grupul de cooperare și 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 menționată la articolul 39 alineatul (2).

Articolul 22

Evaluări coordonate la nivelul Uniunii ale riscurilor de securitate legate de lanțurile de aprovizionare critice

(1) Grupul de cooperare, în cooperare cu Comisia și ENISA, poate efectua evaluări coordonate ale riscurilor în materie de securitate ale anumitor servicii TIC, sisteme TIC sau lanțuri de aprovizionare cu produse TIC critice, ținând seama de factorii de risc de natură tehnică și, după caz, care nu sunt de natură tehnică.

(2) Comisia, după consultarea Grupului de cooperare și a ENISA și, atunci când este necesar, a părților interesate relevante, identifică serviciile TIC, sistemele TIC sau produsele TIC critice specifice care pot face obiectul evaluării coordonate a riscurilor de securitate menționate la alineatul (1).

Articolul 23

Obligații de raportare

(1) Fiecare stat membru se asigură că entitățile esențiale și entitățile importante notifică, fără întârzieri nejustificate, echipei CSIRT sau, după caz, autorității sale competente, în conformitate cu alineatul (4), orice incident care are un impact semnificativ asupra prestării serviciilor lor, astfel cum se menționează la alineatul (3) (incident semnificativ). Dacă este cazul, entitățile 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 entitățile respective raportează, inter alia, orice informație care îi permite echipei CSIRT sau, după caz, autorității competente să constate orice impact transfrontalier al incidentului. Simpla notificare nu expune entitatea notificatoare 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.

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).

(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.

(3) Un incident este considerat semnificativ dacă:

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

(b) a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau morale 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:

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

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

(c) la cererea unei echipe CSIRT sau, după caz, a autorității competente, un raport intermediar privind actualizarea relevantă a situației;

(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 gravității și a impactului acestuia;

(ii) tipul de amenințare sau de cauză principală care probabil că a declanșat incidentul;

(iii) măsurile de atenuare aplicate și în curs;

(iv) dacă este cazul, impactul transfrontalier al incidentului;

(e) în cazul unui incident în desfășurare la momentul prezentării raportului final menționat la litera (d), statele membre se asigură că entitățile în cauză prezintă la momentul respectiv un raport privind progresele înregistrate și 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 privește incidentele semnificative care afectează prestarea serviciilor sale de încredere, echipa CSIRT sau, după caz, autoritatea competentă, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care a luat cunoștință de incidentul semnificativ.

(5) Echipa CSIRT sau autoritatea competentă furnizează, fără întârzieri nejustificate și, 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 și, 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.

(6) După caz, și în special dacă incidentul semnificativ implică două sau mai multe state membre, echipa CSIRT, autoritatea competentă sau punctul unic de contact informează, fără întârzieri nejustificate, celelalte state membre afectate și ENISA cu privire la incidentul semnificativ. Aceste informații includ tipul de informații 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 și comerciale ale entității, precum și confidențialitatea informațiilor 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, și, după caz, echipele CSIRT sau autoritățile competente din alte state membre în cauză pot, după consultarea entității în cauză, să informeze publicul cu privire la incidentul semnificativ sau să solicite entității să facă acest lucru.

(8) La cererea echipei CSIRT sau a autorității competente, punctul unic de contact înaintează notificările primite în temeiul alineatului (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 și agregate privind incidentele semnificative, incidentele, amenințările cibernetice semnificative și incidentele evitate la limită notificate în conformitate cu alineatul (1) de la prezentul articol și cu articolul 30. Pentru a contribui la furnizarea de informații comparabile, ENISA poate adopta orientări 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.

(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.

Comisia face schimb de opinii și cooperează cu Grupul de cooperare privind proiectele de acte de punere în aplicare menționate la primul și 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 menționată la articolul 39 alineatul (2).

Articolul 24

Utilizarea sistemelor europene de certificare a securității cibernetice

(1) Pentru a demonstra conformitatea cu anumite cerințe de la articolul 21, statele membre le pot solicita entităților esențiale și entităților importante să utilizeze anumite produse TIC, servicii TIC și procese TIC, dezvoltate de entități esențiale sau de entități importante ori achiziționate de la părți terțe, care sunt certificate în cadrul sistemelor europene de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881. De asemenea, statele membre încurajează entitățile esențiale și entitățile importante să utilizeze servicii de încredere calificate.

(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.

Articolul 25

Standardizarea

(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.

(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.

CAPITOLUL V

JURISDICȚIE ȘI ÎNREGISTRARE

Articolul 26

Jurisdicție și teritorialitate

(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:

(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;

(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);

(c) entitățile administrației publice, care se consideră că intră sub jurisdicția statului membru 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.

(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.

(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.

(5) Statele membre care au primit o cerere de asistență reciprocă în legătură cu o entitate, astfel cum este menționată la alineatul (1) litera (b), pot, în limitele cererii respective, să ia măsuri adecvate de supraveghere și de asigurare a respectării legii în ceea ce privește entitatea în cauză care furnizează servicii sau care are o rețea și un sistem informatic pe teritoriul lor.

Articolul 27

Registrul entităților

(1) ENISA creează și păstrează un registru al furnizorilor de servicii DNS, registrelor de nume TLD, al entităților 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 rețele de furnizare de conținut, al furnizorilor de servicii gestionate, al furnizorilor de servicii de securitate gestionate, precum și al furnizorilor de 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:

(a) denumirea entității;

(b) sectorul, subsectorul relevant și tipul de entitate menționate în anexa I sau II, după caz;

(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);

(d) datele de contact actualizate, inclusiv adresele de e-mail și numerele de telefon ale entității și, după caz, ale reprezentantului său desemnat în temeiul articolului 26 alineatul (3);

(e) statele membre în care entitatea furnizează servicii; și

(f) gamele de adrese IP ale entității.

(3) Statele membre se asigură că entitățile menționate la alineatul (1) notifică autorității competente fără întârziere și, în orice caz, în termen de trei luni de la data modificării, orice modificare a informațiilor pe care le-au transmis în temeiul alineatului (2).

(4) După ce primește informațiile menționate la alineatele (2) și (3), cu excepția celor menționate la alineatul (2) litera (f), punctul unic de contact al statului membru în cauză le înaintează către ENISA, fără întârzieri nejustificate.

(5) După caz, informațiile menționate la alineatele (2) și (3) de la prezentul articol se transmit prin mecanismul național menționat la articolul 3 alineatul (4) al patrulea paragraf.

Articolul 28

Baza de date pentru datele de înregistrare a numelor de domenii

(1) Pentru a contribui la securitatea, stabilitatea și reziliența DNS, statele membre solicită ca registrele de nume TLD și entitățile care prestează servicii de înregistrare a numelor de domenii să colecteze și să mențină date exacte și complete privind înregistrarea numelor de domenii într-o bază de date dedicată, cu diligența necesară, în conformitate cu dreptul Uniunii în materie de protecție a datelor cu caracter personal.

(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:

(a) numele de domeniu;

(b) data înregistrării;

(c) numele, adresa de e-mail și numărul de telefon de contact 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.

(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.

(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.

(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 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.

(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.

CAPITOLUL VI

SCHIMBUL DE INFORMAȚII

Articolul 29

Acorduri privind schimbul de informații în materie de securitate cibernetică

(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:

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

(b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de limitare și prevenire a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare sau promovarea colaborării dintre entitățile publice și private în domeniul cercetării amenințărilor cibernetice.

(2) Statele membre se asigură că schimbul de informații are loc în cadrul unor comunități ale entităților esențiale și ale entităților importante și, după caz, ale prestatorilor sau furnizorilor lor de servicii. Un astfel de schimb este pus în aplicare prin acorduri privind schimbul de informații în materie de securitate cibernetică, în considerarea caracterului potențial sensibil al informațiilor partajate.

(3) Statele membre facilitează instituirea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) de la prezentul articol. Astfel de acorduri pot specifica elemente operaționale, inclusiv utilizarea platformelor TIC dedicate și a instrumentelor de automatizare, conținutul și condițiile acordurilor privind schimbul de informații. Atunci când stabilesc detaliile implicării autorităților publice în astfel de acorduri, statele membre pot impune condiții cu privire la informațiile puse la dispoziție de autoritățile competente sau de echipele CSIRT. Statele membre oferă asistență pentru aplicarea unor astfel de acorduri în conformitate cu politicile lor menționate la articolul 7 alineatul (2) litera (h).

(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.

(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.

Articolul 30

Notificarea voluntară a informațiilor relevante

(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:

(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.

(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.

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.

CAPITOLUL VII

SUPRAVEGHEREA ȘI ASIGURAREA RESPECTĂRII LEGII

Articolul 31

Aspecte generale privind supravegherea și asigurarea respectării legii

(1) Statele membre se asigură că autoritățile lor competente supraveghează în mod eficace și iau măsurile necesare pentru a asigura respectarea prezentei directive.

(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.

(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.

(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.

Articolul 32

Măsurile de supraveghere și de asigurare a respectării legii în ceea ce privește entitățile esențiale

(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.

(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;

(b) unor audituri de securitate periodice și specifice efectuate de un organism independent sau de o autoritate competentă;

(c) unor audituri ad-hoc, inclusiv în cazurile justificate de un incident semnificativ sau de o încălcare a prezentei directive de către entitatea esențială;

(d) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor, după caz cu cooperarea entității în cauză;

(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;

(f) unor cereri de acces la date, la documente și la orice informații necesare pentru îndeplinirea sarcinilor lor 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.

Auditurile de securitate specifice, menționate la primul paragraf litera (b), se bazează pe evaluări ale riscurilor efectuate de autoritatea competentă sau de entitatea auditată sau pe alte informații disponibile legate de riscuri.

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.

(3) Atunci când își exercită competențele în temeiul alineatului (2) literele (e), (f) sau (g), autoritățile competente precizează scopul solicitării și informațiile solicitate.

(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;

(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 care le solicită entităților în cauză să remedieze deficiențele identificate sau încălcările prezentei directive;

(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;

(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;

(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;

(f) de a dispune ca entitățile în cauză să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil;

(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;

(h) de a dispune ca entitățile în cauză să facă publice într-un mod specific aspectele legate de încălcări ale prezentei directive;

(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.

(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:

(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 parte sau toate serviciile relevante furnizate sau activitățile relevante desfășurate de entitatea esențială;

(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.

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.

Măsurile de asigurare a respectării legii prevăzute la prezentul alineat nu se aplică entităților administrației publice care intră în domeniul de aplicare al prezentei directive.

(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.

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.

(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:

(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 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;

(b) durata încălcării;

(c) orice încălcare anterioară relevantă comisă de entitatea în cauză;

(d) orice prejudicii materiale sau morale cauzate, inclusiv pierderile financiare sau economice, efectele asupra altor servicii și numărul de utilizatori afectați;

(e) orice intenție sau neglijență din partea autorului încălcării;

(f) orice măsuri luate de entitate pentru a preveni sau a atenua prejudiciile materiale sau morale;

(g) orice aderare la coduri de conduită aprobate sau la mecanisme de certificare aprobate;

(h) măsura în care persoanele fizice sau juridice declarate responsabile cooperează 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.

(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 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.

(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.

Articolul 33

Măsuri de supraveghere și de asigurare a respectării legii în ceea ce privește entitățile importante

(1) Atunci când li se furnizează dovezi, indicii sau informații că o entitate importantă nu ar respecta prezenta directivă, în special articolele 21 și 23, statele membre se asigură că autoritățile competente iau măsuri, dacă este necesar, prin intermediul unor măsuri de supraveghere ex post. Statele membre se asigură că aceste măsuri sunt efective, proporționale și cu efect de descurajare, ținând seama de circumstanțele fiecărui caz în parte.

(2) Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile importante, au competența de a supune entitățile respective cel puțin:

(a) unor inspecții la fața locului și unei supravegheri *ex situ ex post* realizate de profesioniști cu formare corespunzătoare;

(b) unor audituri de securitate specifice efectuate de un organism independent sau de o autoritate competentă;

(c) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor, după caz cu cooperarea entității în cauză;

(d) unor cereri de informații 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 și respectarea obligației de a transmite informații autorităților competente în temeiul articolului 27;

(e) unor cereri de acces la date, la documente și la informații 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 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 sau de entitatea auditată sau pe alte informații disponibile legate de riscuri.

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.

(3) Atunci când își exercită competențele în temeiul alineatului (2) literele (d), (e) sau (f), autoritățile competente precizează scopul solicitării și informațiile solicitate.

(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;

(b) de a adopta instrucțiuni obligatorii sau un ordin prin care le solicită entităților în cauză să remedieze deficiențele identificate sau încălcarea prezentei directive;

(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;

(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;

(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;

(f) de a dispune ca entitățile în cauză să pună în aplicare recomandările formulate în urma unui audit de securitate într-un termen rezonabil;

(g) de a dispune ca entitățile în cauză să facă publice într-un mod specific aspectele legate de încălcările prezentei directive;

(h) 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)-(g) de la prezentul alineat.

(5) Articolul 32 alineatele (6), (7) și (8) se aplică, mutatis mutandis, măsurilor de supraveghere și de asigurare a respectării legii prevăzute în prezentul articol pentru entitățile importante.

(6) 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 importantă, care este desemnată ca fiind un furnizor terț de servicii TIC critice în temeiul articolului 31 din Regulamentul (UE) 2022/2554.

Articolul 34

Condiții generale pentru aplicarea de amenzi administrative entităților esențiale și entităților importante

(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.

(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).

(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).

(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.

(5) Statele membre se asigură că, atunci când încalcă articolul 21 sau articolul 23, entitățile importante sunt supuse, în conformitate cu alineatele (2) și (3) din prezentul articol, unor amenzi administrative având o limită superioară de cel puțin 7 000 000 EUR sau având o limită superioară de cel puțin 1,4 % din cifra de afaceri mondială totală anuală, înregistrată în exercițiul financiar precedent, a întreprinderii căreia îi aparține entitatea importantă, luându-se în considerare valoarea cea mai mare dintre acestea.

(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.

(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.

Articolul 35

Încălcări care implică o încălcare a securității datelor cu caracter personal

(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).

Articolul 36

Sancțiuni

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.

Articolul 37

Asistență reciprocă

(1) Dacă o entitate furnizează servicii în mai multe state membre sau furnizează servicii în unul sau mai multe state membre iar rețeaua și sistemele sale informatice sunt situate în unul sau mai multe alte state membre, autoritățile competente ale statelor membre în cauză cooperează și își oferă asistență reciprocă, după caz. Această cooperare implică cel puțin următoarele:

(a) autoritățile competente care aplică măsuri de supraveghere sau de asigurare a respectării legii într-un stat membru informează și consultă, prin intermediul punctului unic de contact, autoritățile competente din celelalte state membre în cauză cu privire la măsurile de supraveghere și de asigurare a respectării legii luate;

(b) o autoritate competentă poate solicita unei alte autorități competente să ia măsuri de supraveghere sau de asigurare a respectării legii;

(c) la primirea unei cereri motivate din partea altei autorități competente, o autoritate competentă acordă asistență reciprocă celeilalte autorități competente proporțional 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 și consecvent.

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.

CAPITOLUL VIII

ACTE DELEGATE ȘI ACTE DE PUNERE ÎN APLICARE

Articolul 38

Exercitarea delegării de competențe

(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.

Articolul 39

Procedura comitetului

(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.

CAPITOLUL IX

DISPOZIȚII FINALE

Articolul 40

Revizuirea

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.

Articolul 41

Transpunerea

(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 directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a unei astfel de trimiteri.

Articolul 42

Modificarea Regulamentului (UE) nr. 910/2014

În Regulamentul (UE) nr. 910/2014, articolul 19 se elimină de la 18 octombrie 2024.

Articolul 43

Modificarea Directivei (UE) 2018/1972

În Directiva (UE) 2018/1972, articolele 40 și 41 se elimină de la 18 octombrie 2024.

Articolul 44

Abrogarea

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.

Articolul 45

Intrarea în vigoare

Prezenta directivă intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Articolul 46

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Strasbourg, 14 decembrie 2022.

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*
R. METSOLA	M. BEK

ANEXA I

SECTOARE CU O IMPORTANȚĂ CRITICĂ RIDICATĂ

Sectorul	Subsectorul	Tipul de entitate
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 și a Consiliului ([1]), care îndeplinesc funcția de „furnizare", astfel cum este definită la articolul 2 punctul 12 din directiva respectivă
		— Operatorii de distribuție, astfel cum sunt definiți la articolul 2 punctul 29 din Directiva (UE) 2019/944
		— Operatorii de transport și de sistem, astfel cum sunt definiți la articolul 2 punctul 35 din Directiva (UE) 2019/944
		— Producătorii, astfel cum sunt definiți la articolul 2 punctul 38 din Directiva (UE) 2019/944
		— Operatorii pieței de energie electrică desemnați, astfel cum sunt definiți la articolul 2 punctul 8 din Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului ([2]) — Participanții la piață, astfel cum sunt definiți 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 și 59 din Directiva (UE) 2019/944 — Operatorii unui punct de reîncărcare care sunt responsabili cu gestionarea și exploatarea unui punct de reîncărcare care furnizează un serviciu de reîncărcare utilizatorilor finali, inclusiv în numele și în contul unui furnizor de servicii de mobilitate
	(b) Încălzire centralizată și 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 și a Consiliului ([3])
	(c) Petrol	— Operatorii de conducte de transport al petrolului
		— 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])
	(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])
		— Operatorii de distribuție, astfel cum sunt definiți la articolul 2 punctul 6 din Directiva 2009/73/CE
		— Operatorii de transport și de sistem, astfel cum sunt definiți la articolul 2 punctul 4 din Directiva 2009/73/CE
		— Operatorii de înmagazinare, astfel cum sunt definiți la articolul 2 punctul 10 din Directiva 2009/73/CE
		— Operatorii de sistem GNL, astfel cum sunt definiți la articolul 2 punctul 12 din Directiva 2009/73/CE
		— Întreprinderile din sectorul gazelor naturale, astfel cum sunt definite la articolul 2 punctul 1 din Directiva 2009/73/CE
		— Operatorii de instalație de rafinare și de tratare a gazelor naturale
	(e) Hidrogen	— Operatorii de producție, stocare și transport de hidrogen

Sectorul	Subsectorul	Tipul de entitate
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
		— 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
		— 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])
	(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])
		— 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
	(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
		— Organele de gestionare a porturilor, astfel cum sunt definite la articolul 3 punctul 1 din Directiva 2005/65/CE a Parlamentului European și a Consiliului ([11]), inclusiv instalațiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004, și entitățile care realizează lucrări și operează echipamente în cadrul porturilor
		— Operatorii de servicii de trafic maritim (STM), astfel cum sunt definiți la articolul 3 litera (o) din Directiva 2002/59/CE a Parlamentului European și a Consiliului ([12])
	(d) Transport rutier	— Autoritățile 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 excepția entităților publice în cazul cărora gestionarea traficului sau exploatarea sistemelor de transport inteligente reprezintă doar o parte neesențială a activității lor generale
		— Operatorii de sisteme de transport inteligente, astfel cum sunt definite la articolul 4 punctul 1 din Directiva 2010/40/UE a Parlamentului European și a Consiliului ([14])
3. Sectorul bancar		Instituțiile de credit, astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului ([15])
4. Infrastructuri ale pieței financiare		— Operatorii de locuri de tranzacționare, astfel cum sunt definite la articolul 4 punctul 24 din Directiva 2014/65/UE a Parlamentului European și a Consiliului ([16])
		— Contrapărțile centrale (CPC), astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului ([17])

Sectorul	Subsectorul	Tipul de entitate
5. Sectorul sănătății		— Furnizorii de servicii medicale, astfel cum sunt definiți la articolul 3 litera (g) din Directiva 2011/24/UE a Parlamentului European și a Consiliului ([18])
		— Laboratoarele de referință ale UE, astfel cum sunt definite la articolul 15 din Regulamentul (UE) 2022/2371 al Parlamentului European și al Consiliului ([19])
		— Entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor, astfel cum sunt definite la articolul 1 punctul 2 din Directiva 2001/83/CE a Parlamentului European și a Consiliului ([20]) — 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])
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
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 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
8. Infrastructură digitală		— Furnizorii de IXP (internet *exchange point*)
		— Furnizorii de servicii DNS, cu excepția operatorilor de servere pentru nume primare
		— Registrele de nume TLD
		— Furnizorii de servicii de *cloud computing*
		— Furnizorii de servicii de centre de date
		— Furnizorii de rețele de furnizare de conținut
		— Furnizorii de servicii de încredere
		— Furnizorii de rețele publice de comunicații electronice –Furnizorii de servicii de comunicații electronice accesibile publicului
		— Furnizorii de IXP (internet *exchange point*)
9. Gestionarea serviciilor TIC (*business-to-business*)		— Furnizorii de servicii gestionate — Furnizorii de servicii de securitate gestionate

Sectorul	Subsectorul	Tipul de entitate
10. Administrație publică		— Entitățile de administrație publică din administrația centrală, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern
		— 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

([1]) Directiva (UE) 2019/944 a Parlamentului European și a Consiliului din 5 iunie 2019 privind normele comune pentru piața internă de energie electrică și de modificare a Directivei 2012/27/UE (JO L 158, 14.6.2019, p. 125).
([2]) Regulamentul (UE) 2019/943 al Parlamentului European și al Consiliului din 5 iunie 2019 privind piața internă de energie electrică (JO L 158, 14.6.2019, p. 54).
([3]) Directiva (UE) 2018/2001 a Parlamentului European și a Consiliului din 11 decembrie 2018 privind promovarea utilizării energiei din surse regenerabile (JO L 328, 21.12.2018, p. 82).
([4]) Directiva 2009/119/CE a Consiliului din 14 septembrie 2009 privind obligația statelor membre de a menține un nivel minim de rezerve de țiței și/sau de produse petroliere (JO L 265, 9.10.2009, p. 9).
([5]) Directiva 2009/73/CE a Parlamentului European și a Consiliului din 13 iulie 2009 privind normele comune pentru piața internă în sectorul gazelor naturale și de abrogare a Directivei 2003/55/CE (JO L 211, 14.8.2009, p. 94).
([6]) Directiva 2009/12/CE a Parlamentului European și a Consiliului din 11 martie 2009 privind tarifele de aeroport (JO L 70, 14.3.2009, p. 11).
([7]) 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 (JO L 348, 20.12.2013, p. 1).
([8]) 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) (JO L 96, 31.3.2004, p. 1).
([9]) Directiva 2012/34/UE a Parlamentului European și a Consiliului din 21 noiembrie 2012 privind instituirea spațiului feroviar unic european (JO L 343, 14.12.2012, p. 32).
([10]) Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului din 31 martie 2004 privind consolidarea securității navelor și a instalațiilor portuare (JO L 129, 29.4.2004, p. 6).
([11]) Directiva 2005/65/CE a Parlamentului European și a Consiliului din 26 octombrie 2005 privind consolidarea securității portuare (JO L 310, 25.11.2005, p. 28).
([12]) Directiva 2002/59/CE a Parlamentului European și a Consiliului din 27 iunie 2002 de instituire a unui sistem comunitar de monitorizare și informare privind traficul navelor maritime și de abrogare a Directivei 93/75/CEE a Consiliului (JO L 208, 5.8.2002, p. 10).
([13]) Regulamentul delegat (UE) 2015/962 al Comisiei din 18 decembrie 2014 de completare a Directivei 2010/40/UE a Parlamentului European și a Consiliului în ceea ce privește prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic (JO L 157, 23.6.2015, p. 21).
([14]) Directiva 2010/40/UE a Parlamentului European și a Consiliului din 7 iulie 2010 privind cadrul pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier și pentru interfețele cu alte moduri de transport (JO L 207, 6.8.2010, p. 1).
([15]) Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).
([16]) Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (JO L 173, 12.6.2014, p. 349).
([17]) Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții (JO L 201, 27.7.2012, p. 1).
([18]) Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).

([19]) Regulamentul (UE) 2022/2371 al Parlamentului European și al Consiliului din 23 noiembrie 2022 privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 1082/2013/UE (JO L 314, 6.12.2022, p. 26).

([20]) Directiva 2001/83/CE a Parlamentului European și a Consiliului din 6 noiembrie 2001 de instituire a unui cod comunitar cu privire la medicamentele de uz uman (JO L 311, 28.11.2001, p. 67).

([21]) 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 (JO L 20, 31.1.2022, p. 1).

([22]) Directiva (UE) 2020/2184 a Parlamentului European și a Consiliului din 16 decembrie 2020 privind calitatea apei destinate consumului uman (JO L 435, 23.12.2020, p. 1).

([23]) Directiva 91/271/CEE a Consiliului din 21 mai 1991 privind tratarea apelor urbane reziduale (JO L 135, 30.5.1991, p. 40).

ANEXA II

ALTE SECTOARE DE IMPORTANȚĂ CRITICĂ

Sectorul	Subsectorul	Tipul de entitate
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
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
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 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
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
	(b) (b) Fabricarea computerelor și a produselor electronice și optice	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 26 din NACE Rev. 2
	(c) Fabricarea echipamentelor electrice	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 27 din NACE Rev. 2
	(d) Fabricarea altor mașini și echipamente n.c.a.	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 28 din NACE Rev. 2
	(e) Fabricarea autovehiculelor, remorcilor și semiremorcilor	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 29 din NACE Rev. 2
	(f) Fabricarea altor echipamente de transport	Întreprinderile care desfășoară oricare dintre activitățile economice menționate în secțiunea C diviziunea 30 din NACE Rev. 2

Sectorul	Subsectorul	Tipul de entitate
6. Furnizori digitali		— Furnizorii de piețe online
		— Furnizorii de motoare de căutare online
		— Furnizorii de platforme de servicii de socializare în rețea
7. Cercetare		Organizațiile de cercetare

([1]) Directiva 2008/98/CE a Parlamentului European și a Consiliului din 19 noiembrie 2008 privind deșeurile și de abrogare a anumitor directive (JO L 312, 22.11.2008, p. 3).

([2]) Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului din 18 decembrie 2006 privind înregistrarea, evaluarea, autorizarea și restricționarea substanțelor chimice (REACH), de înființare a Agenției Europene pentru Produse Chimice, de modificare a Directivei 1999/45/CE și de abrogare a Regulamentului (CEE) nr. 793/93 al Consiliului și a Regulamentului (CE) nr. 1488/94 al Comisiei, precum și a Directivei 76/769/CEE a Consiliului și a Directivelor 91/155/CEE, 93/67/CEE, 93/105/CE și 2000/21/CE ale Comisiei (JO L 396, 30.12.2006, p. 1).

([3]) Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului din 18 decembrie 2006 privind înregistrarea, evaluarea, autorizarea și restricționarea substanțelor chimice (REACH), de înființare a Agenției Europene pentru Produse Chimice, de modificare a Directivei 1999/45/CE și de abrogare a Regulamentului (CEE) nr. 793/93 al Consiliului și a Regulamentului (CE) nr. 1488/94 al Comisiei, precum și a Directivei 76/769/CEE a Consiliului și a Directivelor 91/155/CEE, 93/67/CEE, 93/105/CE și 2000/21/CE ale Comisiei (JO L 396, 30.12.2006, p. 1).

([4]) 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 (JO L 117, 5.5.2017, p. 1).

([5]) Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic in vitro și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5.5.2017, p. 176).

ANEXA III

TABEL DE CORESPONDENȚĂ

Directiva (UE) 2016/1148	Prezenta directivă
Articolul 1 alineatul (1)	Articolul 1 alineatul (1)
Articolul 1 alineatul (2)	Articolul 1 alineatul (2)
Articolul 1 alineatul (3)	-
Articolul 1 alineatul (4)	Articolul 2 alineatul (12)
Articolul 1 alineatul (5)	Articolul 2 alineatul (13)
Articolul 1 alineatul (6)	Articolul 2 alineatele (6) și (11)
Articolul 1 alineatul (7)	Articolul 4
Articolul 2	Articolul 2 alineatul (14)
Articolul 3	Articolul 5
Articolul 4	Articolul 6
Articolul 5	–
Articolul 6	–
Articolul 7 alineatul (1)	Articolul 7 alineatele (1) și (2)
Articolul 7 alineatul (2)	Articolul 7 alineatul (4)
Articolul 7 alineatul (3)	Articolul 7 alineatul (3)
Articolul 8 alineatele (1)-(5)	Articolul 8 alineatele (1)-(5)
Articolul 8 alineatul (6)	Articolul 13 alineatul (4)
Articolul 8 alineatul (7)	Articolul 8 alineatul (6)
Articolul 9 alineatele (1), (2) și (3)	Articolul 10 alineatele (1), (2) și (3)
Articolul 9 alineatul (4)	Articolul 10 alineatul (9)
Articolul 9 alineatul (5)	Articolul 10 alineatul (10)
Articolul 10 alineatele (1), (2) și (3) primul paragraf	Articolul 13 alineatele (1), (2) și (3)
Articolul 10 alineatul (3) al doilea paragraf	Articolul 23 alineatul (9)
Articolul 11 alineatul (1)	Articolul 14 alineatele (1) și (2)
Articolul 11 alineatul (2)	Articolul 14 alineatul (3)
Articolul 11 alineatul (3)	Articolul 14 alineatul (4) primul paragraf literele (a)-(q) și (s), și alineatul (7)
Articolul 11 alineatul (4)	Articolul 14 alineatul (4) primul paragraf litera (r) și al doilea paragraf
Articolul 11 alineatul (5)	Articolul 14 alineatul (8)
Articolul 12 alineatele (1)-(5)	Articolul 15 alineatele (1)-(5)
Articolul 13	Articolul 17
Articolul 14 alineatele (1) și (2)	Articolul 21 alineatele (1)-(4)
Articolul 14 alineatul (3)	Articolul 23 alineatul (1)
Articolul 14 alineatul (4)	Articolul 23 alineatul (3)
Articolul 14 alineatul (5)	Articolul 23 alineatele (5), (6) și (8)

Directiva (UE) 2016/1148	Prezenta directivă
Articolul 14 alineatul (6)	Articolul 23 alineatul (7)
Articolul 14 alineatul (7)	Articolul 23 alineatul (11)
Articolul 15 alineatul (1)	Articolul 31 alineatul (1)
Articolul 15 alineatul (2) primul paragraf litera (a)	Articolul 32 alineatul (2) litera (e)
Articolul 15 alineatul (2) primul paragraf litera (b)	Articolul 32 alineatul (2) litera (g)
Articolul 15 alineatul (2) al doilea paragraf	Articolul 32 alineatul (3)
Articolul 15 alineatul (3)	Articolul 32 alineatul (4) litera (b)
Articolul 15 alineatul (4)	Articolul 31 alineatul (3)
Articolul 16 alineatele (1) și (2)	Articolul 21 alineatele (1)-(4)
Articolul 16 alineatul (3)	Articolul 23 alineatul (1)
Articolul 16 alineatul (4)	Articolul 23 alineatul (3)
Articolul 16 alineatul (5)	–
Articolul 16 alineatul (6)	Articolul 23 alineatul (6)
Articolul 16 alineatul (7)	Articolul 23 alineatul (7)
Articolul 16 alineatele (8) și (9)	Articolul 21 alineatul (5) și articolul 23 alineatul (11)
Articolul 16 alineatul (10)	–
Articolul 16 alineatul (11)	Articolul 2 alineatele (1), (2) și (3)
Articolul 17 alineatul (1)	Articolul 33 alineatul (1)
Articolul 17 alineatul (2) litera (a)	Articolul 32 alineatul (2) litera (e)
Articolul 17 alineatul (2) litera (b)	Articolul 32 alineatul (4) litera (b)
Articolul 17 alineatul (3)	Articolul 37 alineatul (1) literele (a) și (b)
Articolul 18 alineatul (1)	Articolul 26 alineatul (1) litera (b) și alineatul (2)
Articolul 18 alineatul (2)	Articolul 26 alineatul (3)
Articolul 18 alineatul (3)	Articolul 26 alineatul (4)
Articolul 19	Articolul 25
Articolul 20	Articolul 30
Articolul 21	Articolul 36
Articolul 22	Articolul 39
Articolul 23	Articolul 40
Articolul 24	–
Articolul 25	Articolul 41
Articolul 26	Articolul 45
Articolul 27	Articolul 46
Anexa I, punctul 1	Articolul 11 alineatul (1)
Anexa I, punctul 2 litera (a) punctele (i)-(iv)	Articolul 11 alineatul (2) literele (a)-(d)

Directiva (UE) 2016/1148	Prezenta directivă
Anexa I, punctul 2 litera (a) punctul (v)	Articolul 11 alineatul (2) litera (f)
Anexa I, punctul 2 litera (b)	Articolul 11 alineatul (4)
Anexa I, punctul 2 litera (c) punctele (i) și (ii)	Articolul 11 alineatul (5) litera (a)
Anexa II	Anexa I
Anexa III, punctele 1 și 2	Anexa II, punctul 6
Anexa III, punctul 3	Anexa I, punctul 8