I

(Acte legislative)

DIRECTIVE

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

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 Comitetului Economic și Social European ([1]),

hotărând în conformitate cu procedura legislativă ordinară ([2]),

întrucât:

(1) Rețelele împreună cu sistemele și serviciile informatice îndeplinesc un rol vital în societate. Fiabilitatea și securitatea lor sunt esențiale pentru activitățile economice și societale și, în special, pentru funcționarea pieței interne.

(2) Amploarea, frecvența și impactul incidentelor de securitate sunt în creștere și reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Sistemele respective pot să devină, de asemenea, o țintă pentru acțiunile dăunătoare deliberate menite să afecteze sau să întrerupă funcționarea sistemelor. Astfel de incidente pot să împiedice desfășurarea activităților economice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei Uniunii.

(3) Rețelele și sistemele informatice și, în principal, internetul joacă un rol esențial în facilitarea circulației transfrontaliere a produselor, serviciilor și persoanelor. Datorită naturii lor transnaționale, o perturbare majoră a acestor sisteme, intenționată sau neintenționată și indiferent de locul în care se petrece, poate afecta fiecare stat membru în parte și Uniunea în ansamblul său. Prin urmare, securitatea rețelelor și a sistemelor informatice este esențială pentru buna funcționare a pieței interne.

(4) Pe baza progreselor semnificative obținute în cadrul Forumului european al statelor membre în încurajarea dezbaterilor și a schimburilor de bune practici în materie de politici, inclusiv a elaborării principiilor de cooperare în caz de criză informatică europeană, ar trebui să se instituie un grup de cooperare, compus din reprezentanți ai statelor membre, Comisie și Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor („ENISA”)

([1]) JO C 271, 19.9.2013, p. 133.
([2]) Poziția Parlamentului European din 13 martie 2014 (nepublicată încă în Jurnalul Oficial) și Poziția în primă lectură a Consiliului din 17 mai 2016 (nepublicată încă în Jurnalul Oficial). Poziția Parlamentului European din 6 iulie 2016 (nepublicată încă în Jurnalul Oficial).

pentru a sprijini și a facilita cooperarea strategică dintre statele membre în ceea ce privește securitatea rețelelor și a sistemelor informatice. Pentru ca acest grup să fie eficace și reprezentativ, este esențial ca toate statele membre să dispună de capacitățile minime necesare și de o strategie care să asigure un nivel ridicat de securitate a rețelelor și a sistemelor informatice pe teritoriul lor. În plus, operatorilor de servicii esențiale și furnizorilor de servicii digitale ar trebui să li se aplice cerințe de securitate și de notificare pentru a se promova o cultură a gestionării riscurilor și pentru a se asigura raportarea celor mai grave incidente.

(5) Capacitățile existente nu sunt suficiente pentru asigurarea unui nivel ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Statele membre au niveluri de pregătire foarte diferite, ceea ce a condus la o abordare fragmentară în Uniune. Aceasta determină un nivel inegal de protecție a consumatorilor și a întreprinderilor și subminează nivelul general de securitate a rețelelor și a sistemelor informatice în Uniune. La rândul său, absența unor cerințe comune pentru operatorii de servicii esențiale și furnizorii de servicii digitale face imposibilă instituirea unui mecanism general și eficace de cooperare la nivelul Uniunii. Universităților și centrelor de cercetare le revine un rol decisiv în cultivarea cercetării, dezvoltării și inovării în aceste domenii.

(6) Prin urmare, pentru a răspunde eficient la provocările din domeniul securității rețelelor și a sistemelor informatice, se impune o abordare globală la nivelul Uniunii, care să includă cerințe comune privind crearea capacităților minime și planificarea, schimb de informații, cooperare și cerințe comune de securitate pentru operatorii de servicii esențiale și furnizorii de servicii digitale. Cu toate acestea, operatorii de servicii esențiale și furnizorii de servicii digitale nu sunt împiedicați să pună în aplicare măsuri de securitate care să fie mai stricte decât cele prevăzute în temeiul prezentei directive.

(7) Pentru a putea acoperi toate incidentele și riscurile relevante, prezenta directivă ar trebui să se aplice atât operatorilor de servicii esențiale, cât și furnizorilor de servicii digitale. Cu toate acestea, obligațiile care revin operatorilor de servicii esențiale și furnizorilor de servicii digitale nu ar trebui să se aplice nici întreprinderilor care pun la dispoziție rețele de comunicații publice sau servicii de comunicații electronice accesibile publicului în sensul Directivei 2002/21/CE a Parlamentului European și a Consiliului ([1]), cărora li se aplică cerințele specifice de securitate și integritate prevăzute în directiva respectivă, nici furnizorilor de servicii de încredere în sensul Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([2]), cărora li se aplică cerințele de securitate prevăzute în regulamentul respectiv.

(8) Prezenta directivă nu ar trebui să aducă atingere posibilității de care dispune fiecare stat membru de a lua măsurile necesare pentru a asigura protecția intereselor sale esențiale de securitate, a apăra ordinea și siguranța publică și a permite investigarea, detectarea și urmărirea infracțiunilor. În conformitate cu articolul 346 din Tratatul privind funcționarea Uniunii Europene (TFUE), niciun stat membru nu are obligația de a furniza informații a căror divulgare o consideră contrară intereselor esențiale ale siguranței sale. În acest context, sunt relevante Decizia 2013/488/UE a Consiliului ([3]) și acordurile de nedivulgare sau acordurile de nedivulgare informale, precum „Traffic Light Protocol".

(9) Anumite sectoare ale economiei sunt deja reglementate sau ar putea fi reglementate în viitor prin acte juridice ale Uniunii specifice fiecărui sector care includ norme legate de securitatea rețelelor și a sistemelor informatice. Atunci când aceste acte juridice ale Uniunii conțin dispoziții care impun cerințe privind securitatea rețelelor și a sistemelor informatice sau notificarea incidentelor, aceste dispoziții ar trebui să se aplice în cazul în care conțin cerințe care sunt cel puțin echivalente ca efect cu obligațiile conținute în prezenta directivă. În acest caz, statele membre ar trebui să aplice dispozițiile unor astfel de acte juridice ale Uniunii specifice fiecărui sector, inclusiv cele privind jurisdicția, și nu ar trebui să execute procesul de identificare pentru operatorii de servicii esențiale definit de prezenta directivă. În acest context, statele membre ar trebui să furnizeze Comisiei informații privind aplicarea dispoziției privind astfel de dispoziții de *lex specialis*. Atunci când se stabilește dacă cerințele privind securitatea rețelelor și a sistemelor informatice și notificarea incidentelor conținute de acte juridice ale Uniunii specifice fiecărui sector sunt echivalente cu cele prevăzute de prezenta directivă, ar trebui să se ia în considerare doar dispozițiile actelor juridice relevante ale Uniunii și aplicarea acestora în statele membre.

(10) În sectorul transportului pe apă, cerințele de securitate pentru societăți, nave, instalații portuare, porturi și servicii de trafic naval în temeiul actelor juridice ale Uniunii reglementează toate operațiunile, inclusiv sistemele de radio și telecomunicații, sistemele informatice și rețelele. Printre procedurile obligatorii care trebuie să fie urmate se numără raportarea tuturor incidentelor și ar trebui, prin urmare, să fie considerate *lex specialis*, în măsura în care cerințele respective sunt cel puțin echivalente cu dispozițiile corespunzătoare ale prezentei directive.

([1]) Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice (Directivă-cadru) (JO L 108, 24.4.2002, p. 33).

([2]) 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).

([3]) Decizia 2013/488/UE a Consiliului din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 274, 15.10.2013, p. 1).

(11) La identificarea operatorilor din sectorul transportului pe apă, statele membre ar trebui să țină cont de codurile și orientările internaționale existente și viitoare elaborate în special de Organizația Maritimă Internațională, pentru a se oferi operatorilor maritimi individuali o abordare coerentă.

(12) Reglementarea și supravegherea în sectoarele infrastructurilor bancare și ale piețelor financiare sunt armonizate în mare măsură la nivelul Uniunii prin utilizarea legislației primare și a celei secundare ale Uniunii și a standardelor elaborate împreună cu autoritățile europene de supraveghere. În cadrul uniunii bancare, aplicarea și supravegherea acestor cerințe sunt asigurate de mecanismul unic de supraveghere. Pentru statele membre care nu fac parte din uniunea bancară, acestea sunt asigurate de autoritățile de reglementare relevante din domeniul bancar ale statelor membre. În alte domenii ale reglementării sectorului financiar, Sistemul european al supraveghetorilor financiari asigură și el un grad înalt de asemănare și convergență în practicile de supraveghere. De asemenea, Autoritatea Europeană pentru Valori Mobiliare și Piețe are un rol direct de supraveghere pentru anumite entități, mai precis pentru agenții de rating de credit și registre centrale de tranzacții.

(13) Riscul operațional reprezintă o parte esențială a reglementării și supravegherii prudențiale în sectoarele infrastructurilor bancare și ale pieței financiare. Acesta acoperă toate operațiunile, inclusiv securitatea, integritatea și reziliența rețelelor și a sistemelor informatice. Cerințele cu privire la aceste sisteme, care depășesc adesea cerințele prevăzute în temeiul prezentei directive, figurează în mai multe acte juridice ale Uniunii, inclusiv în normele privind accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a firmelor de investiții și în normele privind cerințele prudențiale pentru instituțiile de credit și firmele de investiții, care includ cerințe privind riscul operațional; norme privind piețele instrumentelor financiare, care includ cerințe privind evaluarea riscului pentru firmele de investiții și pentru piețele reglementate, dar și în normele privind instrumentele financiare derivate extrabursiere, contrapartidele centrale și registrele centrale de tranzacții, care includ cerințe privind riscul operațional pentru contrapartidele centrale și registrele centrale de tranzacții și în normele privind îmbunătățirea decontării titlurilor de valoare în Uniune și privind depozitarele centrale pentru instrumente financiare, care includ cerințe privind riscul operațional. În plus, cerințele de notificare a incidentelor fac parte din practica normală de supraveghere în sectorul financiar și sunt incluse adesea în manualele de supraveghere. Statele membre ar trebui să ia în considerare dispozițiile și cerințele respective atunci când aplică *lex specialis*.

(14) După cum a remarcat Banca Centrală Europeană în avizul său din 25 iulie 2014 ([1]), prezenta directivă nu afectează regimul de supraveghere, în temeiul dreptului Uniunii, de către Eurosistem a sistemelor de plată și de decontare. Ar fi adecvat ca autoritățile responsabile pentru această supraveghere să facă schimb de experiență în aspecte legate de securitatea rețelelor și a sistemelor informatice cu autoritățile competente în temeiul prezentei directive. Aceeași considerație se aplică și membrilor Sistemului European al Băncilor Centrale care nu fac parte din zona euro, care exercită această supraveghere a sistemelor de plată și de decontare pe baza actelor legislative și de reglementare naționale.

(15) O piață online ar trebui să permită consumatorilor și comercianților să încheie contracte de vânzări sau servicii online cu comercianții și reprezintă destinația finală pentru încheierea acestor contracte. Aceasta nu ar trebui să includă servicii online care folosesc doar ca intermediar pentru servicii prestate de o parte terță prin care în final se încheie un contract. Prin urmare, aceasta nu ar trebui să includă serviciile online care compară prețul anumitor produse sau servicii de la diferiți comercianți și reorientează apoi utilizatorul la comerciantul preferat pentru achiziționarea produsului. Serviciile de calcul oferite de piața online pot include tratarea tranzacțiilor, cumularea datelor sau profilarea utilizatorilor. Magazinele de aplicații, care funcționează ca magazine online, permițând distribuția digitală a aplicațiilor sau a programelor software de la părți terțe, urmează să fie înțelese ca un tip de piață online.

(16) Un motor de căutare online permite utilizatorului să efectueze căutări în principiu pe toate site-urile internet pe baza unei interogații pe orice subiect. Alternativ, această căutare s-ar putea concentra pe site-uri internet într-o anumită limbă. Definiția unui motor de căutare online prevăzută de prezenta directivă nu ar trebui să cuprindă funcțiile de căutare limitate la conținutul unui anumit site internet, chiar și atunci când funcția de căutare este furnizată de un motor de căutare extern. De asemenea, aceasta nu ar trebui să acopere serviciile online care compară prețul anumitor produse sau servicii de la diferiți comercianți și reorientează apoi utilizatorul la comerciantul preferat pentru achiziționarea produsului.

(17) Serviciile de cloud computing includ o gamă largă de activități care pot fi oferite în funcție de diferite modele. În sensul prezentei directive, „servicii de cloud computing” înseamnă servicii care permit accesul la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun. Noțiunea „resurse informatice” include resurse precum rețelele, serverele sau alte infrastructuri, stocarea, aplicațiile și serviciile. Noțiunea de „redimensionabil” se referă la resursele informatice care se alocă flexibil de către furnizorul de servicii cloud, indiferent de poziția geografică a resurselor, pentru a administra fluctuațiile de cerere. Noțiunea „bazin elastic” descrie acele resurse informatice care sunt atribuite și transferate în funcție de cerere, pentru a înmulți și a reduce

([1]) JO C 352, 7.10.2014, p. 4.

rapid resursele disponibile în conformitate cu necesarul de lucru. Sintagma „care pot fi puse în comun” 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 furnizat de același echipament electronic.

(18) Funcția unui *internet exchange point* (IXP) este de a interconecta rețele. Un IXP nu oferă acces la rețea și nici nu acționează ca furnizor sau transportator de tranzit. De asemenea, un IXP nu furnizează nici alte servicii care nu au legătură cu interconectarea (deși aceasta nu împiedică un operator IXP să furnizeze și astfel de servicii). Un IXP există pentru a interconecta rețele separate din punct de vedere tehnic și organizațional. Noțiunea de „sistem autonom” se utilizează pentru a descrie o rețea care se autosusține din punct de vedere tehnic.

(19) Statele membre ar trebui să fie responsabile pentru stabilirea entităților care îndeplinesc criteriile definiției operatorului de servicii esențiale. Pentru a se asigura o abordare uniformă, toate statele membre ar trebui să aplice în mod consistent definiția operatorului de servicii esențiale. În acest scop, prezenta directivă prevede evaluarea entităților active în sectoare și subsectoare specifice, instituirea unei liste de servicii esențiale, luarea în considerare a unei liste comune a factorilor transsectoriali care urmează să stabilească dacă un incident potențial ar avea un efect perturbator semnificativ, un proces de consultare care să implice statele membre relevante în cazul entităților care furnizează servicii în mai multe state membre și sprijinul grupului de cooperare în procesul de identificare. Pentru a asigura reflectarea corectă a posibilelor modificări în piață, statele membre ar trebui să revizuiască periodic lista operatorilor identificați și ar trebui să o actualizeze atunci când este necesar. În sfârșit, statele membre ar trebui să transmită Comisiei informațiile necesare pentru a evalua măsura în care această metodologie comună permite o aplicare coerentă a definiției de către statele membre.

(20) În procesul de identificare a operatorilor de servicii esențiale, statele membre ar trebui să evalueze, cel puțin pentru fiecare subsector menționat în prezenta directivă, care dintre servicii trebuie să fie considerate drept esențiale pentru susținerea activităților societale și economice de cea mai mare importanță și să evalueze dacă entitățile enumerate în sectoarele și în subsectoarele menționate în prezenta directivă care furnizează serviciile respective îndeplinesc criteriile de identificare a operatorilor. Atunci când se evaluează dacă o entitate furnizează un serviciu esențial pentru susținerea activităților societale și economice de cea mai mare importanță, este suficient să se examineze dacă o anumită entitate furnizează un serviciu inclus pe lista serviciilor esențiale. În plus, ar trebui să se demonstreze că furnizarea unui serviciu esențial depinde de rețele și de sisteme informatice. În sfârșit, atunci când evaluează dacă un incident ar avea un efect perturbator semnificativ asupra furnizării serviciului, statele membre ar trebui să țină cont de mai mulți factori transsectoriali, precum și, după caz, de factorii sectoriali specifici.

(21) Pentru identificarea operatorilor de servicii esențiale, instituirea într-un stat membru implică exercitarea efectivă și reală a activității prin acorduri stabile. Forma juridică a acestor acorduri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.

(22) Este posibil ca entitățile care operează în sectoarele și subsectoarele menționate în prezenta directivă să furnizeze atât servicii esențiale, cât și neesențiale. De exemplu, în sectorul transportului aerian, aeroporturile furnizează servicii care pot fi considerate de către un stat membru ca fiind esențiale, precum gestionarea pistelor de aterizare/decolare, dar și mai multe servicii care pot fi considerate neesențiale, precum furnizarea de spații comerciale. Operatorii de servicii esențiale ar trebui să facă obiectul unor cerințe de securitate specifice doar în legătură cu serviciile considerate esențiale. Pentru identificarea operatorilor, statele membre ar trebui, prin urmare, să stabilească o listă a serviciilor considerate drept esențiale.

(23) Lista serviciilor ar trebui să conțină toate serviciile furnizate pe teritoriul unui anumit stat membru care îndeplinesc cerințele prevăzute de prezenta directivă. Statele membre ar trebui să fie capabile să includă noi servicii pe lista existentă. Lista serviciilor ar trebui să servească drept punct de referință statelor membre, permițând identificarea operatorilor de servicii esențiale. Scopul acesteia este de a identifica tipurile de servicii esențiale în orice sector dat menționat în prezenta directivă, distingându-le, astfel, de activitățile neesențiale de care ar putea fi răspunzătoare o entitate activă în orice sector determinat. Lista serviciilor instituită de fiecare stat membru ar servi drept informație suplimentară în evaluarea practicii de reglementare a fiecărui stat membru, în vederea asigurării nivelului general de coerență între statele membre al procesului de identificare.

(24) În sensul procesului de identificare, atunci când o entitate furnizează un serviciu esențial în două sau mai multe state membre, statele membre respective ar trebui să intre în discuții bilaterale sau multilaterale unele cu altele. Acest proces de consultare este destinat să le ajute să evalueze importanța operatorului din punct de vedere al impactului transfrontalier și să permită fiecărui stat membru implicat să își exprime opiniile în privința riscurilor asociate serviciilor furnizate. Statele membre implicate ar trebui să țină cont de opiniile exprimate de fiecare dintre ele în cadrul acestui proces și ar trebui să poată solicita în această privință asistența grupului de cooperare.

(25) Ca rezultat al procesului de identificare, statele membre ar trebui să adopte la nivel național măsuri prin care se stabilesc entitățile cărora le revin obligații referitoare la securitatea rețelelor și a sistemelor informatice. Acest rezultat ar putea fi obținut prin adoptarea unei liste care include toți operatorii de servicii esențiale sau prin adoptarea la nivel național a unor măsuri care includ criterii obiective cuantificabile (de exemplu, rezultatele operatorului sau numărul de utilizatori), care permit să se determine căror entități le revin obligații referitoare la securitatea rețelelor și a sistemelor informatice. Măsurile la nivel național deja existente sau cele adoptate în cadrul prezentei directive ar trebui să includă toate măsurile legislative, administrative și de politică permițând identificarea operatorilor de servicii esențiale în temeiul prezentei directive.

(26) Pentru a indica importanța operatorilor de servicii esențiale identificați în raport cu sectorul în cauză, statele membre ar trebui să țină cont de numărul și de dimensiunea operatorilor respectivi, de exemplu în ceea ce privește cota de piață sau cantitatea produsă sau transportată, fără a fi obligate să divulge informații care ar dezvălui care operatori au fost identificați.

(27) Pentru a stabili importanța efectului perturbator al unui incident asupra unui serviciu esențial, statele membre ar trebui să țină cont de o serie de diverși factori, ca de exemplu numărul utilizatorilor serviciului respectiv în scop privat sau profesional. Utilizarea serviciului respectiv poate fi directă, indirectă sau prin intermediere. La evaluarea impactului pe care l-ar putea avea respectivul incident, din punct de vedere al gradului și duratei acestuia, asupra activităților economice și societale sau a siguranței publice, statele membre ar trebui să evalueze și intervalul de timp probabil până când discontinuitatea ar începe să aibă un impact negativ.

(28) Pentru a stabili dacă un incident ar putea avea un efect perturbator asupra furnizării unui serviciu, în afara factorilor transsectoriali, ar trebui să se ia în considerare și factori specifici fiecărui sector. În ceea ce privește furnizorii de energie, printre acești factori s-ar putea număra volumul sau proporția de energie generată la nivel național; pentru furnizorii de petrol, volumul zilnic; pentru transportul aerian, inclusiv aeroporturile și transportatorii aerieni, transportul feroviar și porturile maritime, volumul de trafic național și numărul de pasageri sau de operațiuni de transport de mărfuri pe an; pentru infrastructurile piețelor bancare sau financiare, importanța lor sistemică, pe baza activelor totale sau a raportului dintre activele totale respective și PIB; pentru sectorul sănătății, numărul anual de pacienți aflați în grija furnizorului; pentru producția, tratarea și furnizarea de apă, volumul și numărul și tipul de utilizatori incluzând, de exemplu, spitale, organizații de serviciu public sau persoane fizice, precum și existența surselor de apă alternative care să acopere aceeași zonă geografică.

(29) Pentru a atinge și menține un nivel ridicat de securitate a rețelelor și a sistemelor informatice, fiecare stat membru ar trebui să aibă o strategie națională privind securitatea rețelelor și a sistemelor informatice, care să definească obiectivele strategice și acțiunile concrete de politică ce trebuie puse în aplicare.

(30) Având în vedere diferențele dintre structurile naționale de guvernanță și pentru a salvgarda acordurile sectoriale sau organismele de supraveghere și de reglementare ale Uniunii deja existente și a evita suprapunerile, statele membre ar trebui să fie capabile să desemneze mai multe autorități naționale competente responsabile cu îndeplinirea atribuțiilor legate de securitatea rețelelor și a sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale în temeiul prezentei directive.

(31) Pentru a facilita cooperarea și comunicarea transfrontalieră și pentru a permite aplicarea efectivă a prezentei directive, este necesar ca fiecare stat membru, fără a aduce atingere acordurilor de reglementare sectoriale, să desemneze un punct unic de contact la nivel național responsabil pentru coordonarea aspectelor legate de securitatea rețelelor și a sistemelor informatice și pentru cooperarea transfrontalieră la nivelul Uniunii. Ar trebui să se acorde autorităților competente și punctelor unice de contact resurse tehnice, financiare și umane adecvate pentru a se asigura posibilitatea acestora de a-și îndeplini efectiv și eficient atribuțiile și a realiza astfel obiectivele prezentei directive. Având în vedere că prezenta directivă vizează îmbunătățirea funcționării pieței interne prin consolidarea încrederii reciproce, este necesar ca organismele statelor membre să aibă posibilitatea de a coopera efectiv cu actorii economici și să fie structurate în consecință.

(32) Autoritățile competente sau echipele de intervenție în caz de incidente de securitate informatică („CSIRT") ar trebui să primească notificările incidentelor. Punctele unice de contact nu ar trebui să primească direct nicio notificare de incident, cu excepția cazului în care acționează și în calitate de autoritate competentă sau de CSIRT. Totuși, o autoritate competentă sau o CSIRT ar trebui să poată atribui punctului unic de contract responsabilitatea de a transmite notificările de incidente punctelor unice de contact ale altor state membre afectate.

(33) Pentru a furniza efectiv informații statelor membre și Comisiei, punctul unic de contact ar trebui să transmită grupului de cooperare un raport de sinteză care ar trebui să fie anonimizat pentru a se păstra confidențialitatea notificărilor și identitatea operatorilor de servicii esențiale și a furnizorilor de servicii digitale, deoarece informațiile privind identitatea entităților care notifică nu sunt necesare pentru schimbul de bune practici în grupul de cooperare. Raportul de sinteză ar trebui să includă informații privind numărul de notificări primite, dar și să indice natura incidentelor notificate, precum tipurile de încălcări ale securității, gravitatea sau durata acestora.

(34) Statele membre ar trebui să fie echipate în mod adecvat, din punct de vedere al capacității atât tehnice, cât și organizatorice, pentru a preveni, a detecta, a combate și a atenua incidentele și riscurile la care sunt supuse rețelele și sistemele informatice. Prin urmare, statele membre ar trebui să se asigure că dețin CSIRT care funcționează corespunzător, cunoscute și drept echipe de intervenție în caz de urgență informatică („CERT"), care respectă cerințele esențiale pentru a garanta existența capacităților eficace și compatibile care să administreze incidentele și riscurile și să asigure o cooperare eficientă la nivelul Uniunii. Pentru ca toate tipurile de operatori de servicii esențiale și furnizori de servicii digitale să beneficieze de pe urma acestor capacități și a acestei cooperări, statele membre ar trebui să se asigure că toate tipurile sunt acoperite de o CSIRT desemnată. Având în vedere importanța cooperării internaționale în privința securității cibernetice, CSIRT ar trebui să aibă posibilitatea să participe la rețele de cooperare internațională, în plus față de rețeaua CSIRT instituită prin prezenta directivă.

(35) Deoarece majoritatea rețelelor și a sistemelor informatice au operatori privați, cooperarea dintre sectorul public și cel privat este esențială. Operatorii de servicii esențiale și furnizorii de servicii digitale ar trebui să fie încurajați să-și creeze propriile mecanisme de cooperare informală pentru asigurarea securității rețelelor și a sistemelor informatice. Grupul de cooperare ar trebui să aibă posibilitatea de a invita părți interesate relevante la discuții, după caz. Pentru a încuraja efectiv schimbul de informații și de bune practici, este esențial să se asigure că operatorii de servicii esențiale și furnizorii de servicii digitale care participă la aceste schimburi nu sunt dezavantajați ca urmare a cooperării lor.

(36) ENISA ar trebui să asiste statele membre și Comisia, oferind experiență, asigurând consiliere și facilitând schimbul de bune practici. În special la aplicarea prezentei directive, Comisia ar trebui să consulte ENISA, iar statele membre ar trebui să poate să consulte ENISA, de asemenea. În vederea dezvoltării capacităților și a cunoștințelor statelor membre, grupul de cooperare ar trebui să slujească și drept instrument de schimb de bune practici, de discuție privind capacitățile și pregătirea statelor membre și, voluntar, să-i asiste pe membrii săi la evaluarea strategiilor naționale privind securitatea rețelelor și a sistemelor informatice, la consolidarea capacității și la exerciții de evaluare privind securitatea rețelelor și a sistemelor informatice.

(37) După caz, statele membre ar trebui să poată utiliza sau adapta structurile organizatorice sau strategiile existente atunci când aplică prezenta directivă.

(38) Atribuțiile grupului de cooperare, respectiv ale ENISA sunt interdependente și complementare. În general, ENISA ar trebui să ajute grupul de cooperare la îndeplinirea atribuțiilor sale, în conformitate cu obiectivul ENISA stabilit în Regulamentul (UE) nr. 526/2013 al Parlamentului European și al Consiliului ([1]), în special pentru a oferi asistență instituțiilor, organelor, oficiilor și agențiilor Uniunii și statelor membre la punerea în aplicare a politicilor necesare pentru îndeplinirea cerințelor legale și de reglementare referitoare la securitatea rețelelor și a sistemelor informatice în temeiul actelor juridice existente și viitoare ale Uniunii. În mod deosebit, ENISA ar trebui să ofere asistență în domeniile care corespund propriilor atribuții, astfel cum sunt stabilite în Regulamentul (UE) nr. 526/2013, mai precis analizarea strategiilor privind securitatea rețelelor și a sistemelor informatice, sprijinirea organizării și executării exercițiilor la nivelul Uniunii privind securitatea rețelelor și a sistemelor informatice și schimbul de informații și bune practici privind sensibilizarea și formarea. ENISA ar trebui să se implice, de asemenea, în dezvoltarea de orientări pentru criterii specifice fiecărui sector pentru stabilirea importanței impactului unui incident.

([1]) Regulamentul (UE) nr. 526/2013 al Parlamentului European și al Consiliului din 21 mai 2013 privind Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și de abrogare a Regulamentului (CE) nr. 460/2004 (JO L 165, 18.6.2013, p. 41).

(39) Pentru a promova un nivel avansat de securitate a rețelelor și a sistemelor informatice, grupul de cooperare ar trebui, după caz, să coopereze cu instituțiile, organele, oficiile și agențiile relevante ale Uniunii pentru a face schimb de cunoștințe de specialitate și de bune practici și pentru a oferi consiliere privind aspectele legate de securitatea rețelelor și a sistemelor informatice care ar putea avea un impact asupra activității acestora, respectând, în același timp, acordurile existente privind schimbul de informații cu circulație restrânsă. În cooperarea sa cu autoritățile de aplicare a legii, cu privire la aspectele de securitate a rețelelor și a sistemelor informatice care ar putea avea un impact asupra activității acestora, grupul de cooperare ar trebui să respecte canalele de informații și rețelele existente.

(40) Informațiile privind incidentele sunt tot mai valoroase pentru publicul larg și pentru întreprinderi, în special pentru întreprinderile mici și mijlocii. În unele cazuri, aceste informații se furnizează deja prin site-uri internet la nivel național, în limba unei anumite țări și sunt orientate în special asupra incidentelor și evenimentelor cu dimensiune națională. Având în vedere că întreprinderile operează din ce în ce mai mult transfrontalier și că cetățenii utilizează servicii online, informațiile privind incidentele ar trebui să fie furnizate într-o formă agregată la nivelul Uniunii. Secretariatul rețelei CSIRT este încurajat să întrețină un site internet sau să găzduiască o pagină dedicată pe un site internet existent, în care să pună la dispoziția publicului larg informații generale privind incidente de securitate grave care afectează rețelele și sistemele informatice care se petrec în întreaga Uniune, cu accent specific pe interesele și necesitățile întreprinderilor. CSIRT participante la rețeaua CSIRT sunt încurajate să furnizeze voluntar informațiile care urmează să fie publicate pe site-ul internet respectiv, fără a se include informații confidențiale sau sensibile.

(41) Dacă informațiile sunt considerate a fi confidențiale în conformitate cu normele Uniunii și cele naționale privind secretul comercial, această confidențialitate ar trebui să fie asigurată atunci când se efectuează activitățile și se îndeplinesc obiectivele stabilite de prezenta directivă.

(42) Exercițiile prin care se simulează scenarii de incidente în timp real sunt esențiale pentru testarea pregătirii statelor membre și a cooperării dintre acestea în ceea ce privește securitatea rețelelor și a sistemelor informatice. Ciclul de exerciții CyberEurope, coordonat de ENISA cu participarea statelor membre, este un instrument util pentru testarea și elaborarea recomandărilor cu privire la modul în care ar trebui să se îmbunătățească în timp administrarea incidentelor la nivelul Uniunii. Ținând cont că în prezent statelor membre nu le revine nicio obligație de a planifica exerciții sau de a participa la acestea, crearea rețelei CSIRT în temeiul prezentei directive ar trebui să permită statelor membre să participe la exerciții pe baza unei planificări precise și a unor opțiuni strategice. Grupul de cooperare instituit în temeiul prezentei directive ar trebui să abordeze deciziile strategice privind exercițiile, în special, dar nu exclusiv, în ceea ce privește regularitatea exercițiilor și concepția scenariilor. În conformitate cu mandatul său, ENISA ar trebui să sprijine organizarea și executarea exercițiilor la nivelul UE, oferindu-și expertiza și consultanța grupului de cooperare și rețelei CSIRT.

(43) Având în vedere dimensiunea mondială a problemelor de securitate care afectează rețelele și sistemele informatice, este nevoie de o cooperare internațională mai strânsă pentru a îmbunătăți standardele de securitate și schimbul de informații și pentru a promova o abordare internațională comună a aspectelor de securitate.

(44) Responsabilitatea asigurării securității rețelelor și a sistemelor informatice revine în mare măsură operatorilor de servicii esențiale și furnizorilor de servicii digitale. Ar trebui să se promoveze și să se dezvolte prin cerințe adecvate de reglementare și practici voluntare sectoriale o cultură a gestionării riscurilor, care să implice evaluarea riscurilor și aplicarea unor măsuri de securitate adecvate riscurilor întâmpinate. Stabilirea unor condiții de concurență al căror caracter echitabil să prezinte încredere este și ea esențială pentru funcționarea eficace a grupului de cooperare și a rețelei CSIRT în scopul asigurării unei cooperări efective din partea tuturor statelor membre.

(45) Prezenta directivă se aplică numai administrațiilor publice identificate drept operatori de servicii esențiale. Prin urmare, revine statelor membre responsabilitatea de a asigura securitatea rețelelor și a sistemelor informatice ale administrațiilor publice care nu intră în domeniul de aplicare al prezentei directive.

(46) Măsurile de gestionare a riscurilor includ măsurile de identificare a oricăror riscuri de incidente, de prevenire, detectare și administrare a incidentelor și de diminuare a impactului acestora. Securitatea rețelelor și a sistemelor informatice include securitatea datelor stocate, transmise și prelucrate.

(47) Autoritățile competente ar trebui să își păstreze capacitatea de a adopta orientări la nivel național privind circumstanțiale în care operatorii de servicii esențiale sunt obligați să notifice incidente.

(48) Numeroase întreprinderi din Uniune se bazează, pentru furnizarea propriilor servicii, pe furnizori de servicii digitale. Ținând cont că unele servicii digitale ar putea reprezenta o resursă importantă pentru utilizatorii lor, inclusiv operatorii de servicii esențiale, și ținând cont că acești utilizatori s-ar putea să nu aibă întotdeauna la dispoziție alternative, prezenta directivă ar trebui să se aplice și furnizorilor de astfel de servicii. Securitatea, continuitatea și fiabilitatea tipului de servicii digitale menționat în prezenta directivă sunt esențiale pentru buna funcționare a multor întreprinderi. O perturbare a unui astfel de serviciu digital ar putea împiedica furnizarea altor servicii care se bazează pe acesta și ar putea, astfel, să aibă impact asupra unor activități economice și societale esențiale în Uniune. Aceste servicii digitale ar putea fi, prin urmare, de importanță esențială pentru buna funcționare a întreprinderilor care depind de ele și, mai mult, pentru participarea acestor întreprinderi la piața internă și la comerțul transfrontalier în întreaga Uniune. Furnizorii de servicii digitale care intră sub incidența prezentei directive sunt cei considerați că oferă servicii digitale pe care se bazează din ce în ce mai mult numeroase întreprinderi din Uniune.

(49) Furnizorii de servicii digitale ar trebui să asigure un nivel de securitate proporțional cu gradul de risc prezentat pentru securitatea serviciilor digitale pe care le furnizează, ținând cont de importanța serviciilor lor pentru operațiunile altor întreprinderi din cadrul Uniunii. În practică, gradul de risc pentru operatorii de servicii esențiale, care sunt adesea de cea mai mare importanță pentru întreținerea unor activități societale și economice esențiale, este mai mare decât pentru furnizorii de servicii digitale. Prin urmare, cerințele de securitate pentru furnizorii de servicii digitale ar trebui să fie mai puțin stricte. Furnizorii de servicii digitale ar trebui să rămână liberi să adopte măsuri pe care le consideră adecvate pentru gestionarea riscurilor pentru securitatea rețelelor și sistemelor lor informatice. Ca urmare a naturii lor transfrontaliere, furnizorii de servicii digitale ar trebui să facă obiectul unei abordări mai armonizate la nivelul Uniunii. Actele de punere în aplicare ar trebui să faciliteze precizarea și aplicarea acestor măsuri.

(50) Deși fabricanții de echipamente și creatorii de programe informatice nu sunt operatori de servicii esențiale și nici furnizori de servicii digitale, produsele lor ameliorează securitatea rețelelor și a sistemelor informatice. Prin urmare, acestora le revine un rol important în a permite operatorilor de servicii esențiale și furnizorilor de servicii digitale să asigure securitatea rețelelor și a sistemelor lor informatice. Aceste echipamente și programe informatice fac deja obiectul normelor existente în materie de răspundere pentru produsele cu defect.

(51) Măsurile tehnice și organizatorice impuse operatorilor de servicii esențiale și furnizorilor de servicii digitale nu ar trebui să implice proiectarea, dezvoltarea sau fabricarea într-un anumit mod a unui anumit produs comercial al tehnologiei informației și comunicațiilor.

(52) Operatorii de servicii esențiale și furnizorii de servicii digitale ar trebui să asigure securitatea rețelelor și a sistemelor informatice pe care le utilizează. Acestea sunt în principal rețele și sisteme informatice private, gestionarea securității lor fiind efectuată de către personalul IT intern sau externalizată. Cerințele în materie de securitate și de notificare ar trebui să se aplice operatorilor de servicii esențiale și furnizorilor de servicii digitale relevanți, indiferent dacă aceștia asigură ei înșiși întreținerea propriilor rețele și sisteme informatice sau externalizează această activitate.

(53) Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra operatorilor de servicii esențiale și a furnizorilor de servicii digitale, cerințele ar trebui să fie proporționale cu riscurile la care este expusă rețeaua și sistemul informatic în cauză, ținând seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. În cazul furnizorilor de servicii digitale, aceste cerințe nu ar trebui să se aplice microîntreprinderilor și întreprinderilor mici.

(54) În cazul în care folosesc servicii oferite de furnizorii de servicii digitale, în special servicii de cloud computing, administrațiile publice din statele membre ar putea dori să solicite furnizorilor acestor servicii măsuri de securitate suplimentare față de cele pe care le-ar oferi în mod normal furnizorii de servicii digitale în conformitate cu cerințele prezentei directive. Administrațiile ar trebui să poată include aceste solicitări în cadrul obligațiilor contractuale.

(55) Definițiile piețelor online, motoarelor de căutare online și serviciilor de cloud computing din prezenta directivă servesc obiectivelor specifice ale prezentei directive și nu aduc atingere altor instrumente.

(56) Prezenta directivă nu ar trebui să împiedice statele membre să adopte măsuri la nivel național prin care să impună organismelor din sectorul public să asigure cerințe specifice de securitate atunci când contractează servicii de cloud computing. Orice astfel de măsuri la nivel național ar trebui să se aplice organismului din sectorul public și nu furnizorului de servicii de cloud computing.

(57) Ținând cont de diferențele fundamentale dintre operatorii de servicii esențiale, în special de legătura lor directă cu infrastructura fizică, și furnizorii de servicii digitale, în special natura transfrontalieră a acestora, prezenta directivă ar trebui să adopte o abordare diferențiată în legătură cu nivelul de armonizare în legătură cu aceste două grupuri de entități. Pentru operatorii de servicii esențiale, statele membre ar trebui să fie capabile să identifice operatorii relevanți și să impună cerințe mai stricte decât cele prevăzute de prezenta directivă. Statele membre nu ar trebui să identifice furnizorii de servicii digitale, deoarece prezenta directivă ar trebui să se aplice tuturor furnizorilor de servicii digitale din domeniul său de aplicare. În plus, prezenta directivă și actele de punere în aplicare adoptate în temeiul ei ar trebui să asigure un nivel ridicat de armonizare pentru furnizorii de servicii digitale în ceea ce privește cerințele de securitate și de notificare. Aceasta ar trebui să permită un tratament uniform al furnizorilor de servicii digitale în întreaga Uniune, proporțional cu natura acestora și cu gradul de risc cu care aceștia s-ar putea confrunta.

(58) Prezenta directivă nu ar trebui să împiedice statele membre să impună cerințe de securitate și de notificare entităților care nu sunt furnizori de servicii digitale în domeniul de aplicare al prezentei directive, fără a aduce atingere obligațiilor statelor membre în temeiul dreptului Uniunii.

(59) Autoritățile competente ar trebui să acorde atenția cuvenită menținerii unor canale informale și sigure pentru schimbul de informații. Anunțarea publică a incidentelor raportate autorităților competente ar trebui să găsească echilibrul cuvenit între interesul publicului de a fi informat cu privire la amenințări și eventualele daune comerciale sau de reputație pe care le pot suferi operatorii de servicii esențiale și furnizorii de servicii digitale care raportează incidente. Atunci când sunt puse în aplicare obligațiile de notificare, autoritățile competente și CSIRT ar trebui să acorde o atenție deosebită necesității de a păstra stricta confidențialitate a informațiilor despre vulnerabilitățile unui produs înainte de apariția unor soluții de securitate adecvate.

(60) Furnizorii de servicii digitale ar trebui să facă obiectul unor activități de supraveghere *ex post* lejere și bazate pe reacție, justificate de natura serviciilor și a operațiunilor lor. Prin urmare, respectiva autoritate competentă ar trebui să acționeze doar atunci când i se prezintă dovezi (de exemplu, chiar de către furnizorul de servicii digitale, de către o altă autoritate competentă, inclusiv o autoritate competentă a unui alt stat membru, sau de către un utilizator al serviciului) conform cărora furnizorul de servicii digitale nu se conformează cerințelor prezentei directive, în special în urma unui incident care a avut loc. Prin urmare, autorității competente nu ar trebui să-i revină nicio obligație generală de a supraveghea furnizorii de servicii digitale.

(61) Autoritățile competente ar trebui să dețină mijloacele necesare pentru a-și îndeplini atribuțiile, inclusiv competențele de a obține suficiente informații pentru a evalua nivelul securității rețelelor și a sistemelor informatice.

(62) Incidentele pot fi rezultatul activităților criminale, a căror prevenire, anchetare și urmărire penală este sprijinită prin coordonarea și cooperarea dintre operatorii de servicii esențiale, furnizorii de servicii digitale, autoritățile competente și autoritățile de aplicare a legii. În cazul în care un incident este suspectat că ar fi legat de activități criminale grave în temeiul dreptului Uniunii sau al dreptului intern, statele membre ar trebui să încurajeze operatorii de servicii esențiale și furnizorii de servicii digitale să raporteze autorităților de aplicare a legii incidentele suspecte de a fi de natură criminală gravă. După caz, este de dorit ca Centrul European de combatere a criminalității informatice (EC3) și ENISA să faciliteze coordonarea dintre autoritățile competente și autoritățile de aplicare a legii ale diferitelor state membre.

(63) În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente. În acest context, autoritățile competente și autoritățile de protecție a datelor ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante pentru abordarea oricăror cazuri de încălcare a securității datelor cu caracter personal în urma unor incidente.

(64) Jurisdicția cu privire la furnizorii de servicii digitale ar trebui să fie atribuită statului membru în care furnizorul de servicii digitale își are sediul principal în Uniune, care, în principiu, corespunde locului în care furnizorul își are sediul social în Uniune. Stabilirea implică exercitarea efectivă și reală a activității în cadrul unor acorduri stabile. Forma juridică a acestor acorduri, prin intermediul unei sucursale sau al unei filiale cu personalitate

juridică, nu este factorul determinant în această privință. Acest criteriu nu ar trebui să depindă de situarea fizică sau nu a rețelei și a sistemelor informatice în locul respectiv, prezența și utilizarea acestor sisteme neconstituind, prin ele însele, acest sediu principal și, prin urmare, nu este un criteriu de determinare a sediului principal.

(65) În cazul în care un furnizor de servicii digitale care nu este stabilit în Uniune oferă servicii în cadrul Uniunii, acesta ar trebui să desemneze un reprezentant. Pentru a determina dacă un astfel de furnizor de servicii digitale oferă servicii în cadrul Uniunii, ar trebui să se confirme că furnizorul de servicii digitale intenționează să ofere servicii persoanelor din unul sau mai multe state membre. Simpla accesibilitate în Uniune a unui site internet al furnizorului de servicii digitale sau al unui intermediar sau disponibilitatea unei adrese de e-mail și a altor date de contact, sau utilizarea unei limbi folosite în general în țara terță în care furnizorul de servicii digitale își are sediul, sunt 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 sau menționarea unor clienți sau utilizatori din Uniune pot conduce la concluzia că furnizorul de servicii digitale intenționează să ofere servicii în Uniune. Reprezentantul ar trebui să acționeze în numele furnizorului de servicii digitale, iar autoritățile competente sau CSIRT ar trebui să poată contacta reprezentantul. Reprezentantul ar trebui să fie desemnat explicit printr-un mandat scris al furnizorului de servicii digitale să acționeze în numele acestuia în privința obligațiilor care îi revin acestuia în temeiul prezentei directive, inclusiv raportarea incidentelor.

(66) Standardizarea cerințelor de securitate este un proces impulsionat de piață. Pentru a asigura o aplicare convergentă a standardelor de securitate, statele membre ar trebui să încurajeze respectarea standardelor indicate sau conformitatea cu acestea, în vederea garantării unui nivel ridicat de securitate al rețelelor și sistemelor informatice la nivelul Uniunii. ENISA ar trebui să asiste statele membre prin consiliere și orientări. În acest sens, ar putea fi util să se redacteze standarde armonizate în conformitate cu Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului ([1]).

(67) Entitățile care nu intră în domeniul de aplicare al prezentei directive pot suferi incidente care au un impact semnificativ asupra serviciilor pe care le furnizează. Atunci când consideră că este de interes public să notifice apariția acestor incidente, entitățile respective ar trebui să aibă posibilitatea să facă acest lucru voluntar. Aceste notificări ar trebui să fie tratate de autoritățile competente sau CSIRT în cazul în care aceasta nu constituie o sarcină disproporționată sau neavenită asupra statului membru în cauză.

(68) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentei directive, ar trebui să se confere Comisiei competențe de executare de a stabili acordurile procedurale necesare pentru funcționarea grupului de cooperare și cerințele privind securitatea și notificarea aplicabile furnizorilor de servicii digitale. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([2]). La adoptarea actelor de punere în aplicare legate de acordurile procedurale necesare pentru funcționarea grupului de cooperare, Comisia ar trebui să țină cont în cea mai mare măsură de avizul ENISA.

(69) La adoptarea de acte de punere în aplicare privind cerințele de securitate pentru furnizorii de servicii digitale, Comisia ar trebui să țină cont în cea mai mare măsură de avizul ENISA și ar trebui să consulte părțile interesate care se manifestă. De asemenea, Comisia este încurajată să țină cont de următoarele exemple: în ceea ce privește securitatea sistemelor și a instalațiilor: securitatea fizică și a mediului, securitatea aprovizionării, controlul accesului la rețea și la sistemele informatice și integritatea rețelelor și a sistemelor informatice; în ceea ce privește gestionarea incidentelor: proceduri de gestionare a incidentelor, capacitate de detectare a incidentelor, raportare a incidentelor și comunicare; în ceea ce privește gestionarea continuității activității: strategie de continuitate a activității și planuri de urgență, capacități de redresare în caz de dezastru; și, în ceea ce privește monitorizarea, auditarea și testarea: politici de monitorizare și înregistrare, planuri de urgență de exercițiu, testarea rețelelor și a sistemelor informatice, evaluări de securitate și monitorizarea conformității.

(70) În punerea în aplicare a prezentei directive, Comisia ar trebui să colaboreze, după caz, cu comitetele sectoriale relevante și cu organismele relevante instituite la nivelul Uniunii în domeniile reglementate de prezenta directivă.

([1]) 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).

([2]) 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).

(71) Comisia ar trebui să revizuiască periodic prezenta directivă, consultându-se cu părțile interesate, în special pentru a stabili dacă este necesară efectuarea unor modificări ca urmare a evoluției condițiilor societale, politice, tehnologice sau de piață.

(72) Schimbul de informații cu privire la riscuri și incidente desfășurat în cadrul grupului de cooperare și al rețelei CSIRT, precum și îndeplinirea cerințelor de notificare a incidentelor către autoritățile naționale competente sau CSIRT ar putea necesita prelucrarea datelor cu caracter personal. Prelucrarea acestora ar trebui să se conformeze Directivei 95/46/CE a Parlamentului European și a Consiliului ([1]) și Regulamentului (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([2]). În aplicarea prezentei directive, ar trebui să se aplice Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului ([3]).

(73) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 și a emis un aviz la 14 iunie 2013 ([4]).

(74) Deoarece obiectivul prezentei directive, și anume obținerea unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, nu poate fi realizat în măsură suficientă de către statele membre ci, datorită efectelor acțiunii, poate fi realizat mai bine la nivelul Uniunii, Uniunea poate adopta măsuri în conformitate cu principiul subsidiarității stabilit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității prevăzut la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru atingerea obiectivului respectiv.

(75) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, 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 în fața unei instanțe judecătorești și dreptul de a fi ascultat. Prezenta directivă ar trebui să fie pusă în aplicare în conformitate cu drepturile și principiile menționate,

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect și domeniu de aplicare

(1) Prezenta directivă stabilește măsuri în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în cadrul Uniunii, astfel încât să se îmbunătățească funcționarea pieței interne.

(2) În acest scop, prezenta directivă:

(a) stabilește pentru toate statele membre obligația de a adopta o strategie națională privind securitatea rețelelor și a sistemelor informatice;

(b) creează un grup de cooperare pentru a sprijini și facilita cooperarea strategică și schimbul de informații între statele membre și pentru a dezvolta încrederea între acestea;

(c) creează o rețea a echipelor de intervenție în caz de incidente de securitate informatică („rețeaua CSIRT”) pentru a contribui la dezvoltarea încrederii între statele membre și pentru a promova cooperarea operațională rapidă și eficace;

([1]) Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO L 281, 23.11.1995, p. 31).

([2]) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

([3]) Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

([4]) JO C 32, 4.2.2014, p. 19.

(d) stabilește cerințe de securitate și notificare pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale;

(e) stabilește pentru statele membre obligații de desemnare a autorităților competente la nivel național, a punctelor unice de contact și a CSIRT cu atribuții legate de securitatea rețelelor și a sistemelor informatice.

(3) Cerințele de securitate și notificare prevăzute de prezenta directivă nu se aplică nici întreprinderilor care fac obiectul cerințelor de la articolele 13a și 13b din Directiva 2002/21/CE, nici furnizorilor de servicii de încredere care fac obiectul cerințelor de la articolul 19 din Regulamentul (UE) nr. 910/2014.

(4) Prezenta directivă se aplică fără a aduce atingere Directivei 2008/114/CE a Consiliului ([1]) și Directivelor 2011/93/UE ([2]) și 2013/40/UE ([3]) ale Parlamentului European și ale Consiliului.

(5) Fără a aduce atingere articolului 346 din TFUE, informațiile confidențiale în conformitate cu normele Uniunii și cu cele naționale, precum cele privind secretul comercial, fac obiectul schimbului de informații cu Comisia și cu alte autorități relevante numai dacă acest lucru este necesar pentru aplicarea prezentei directive. Informațiile care fac obiectul schimbului se limitează la informații relevante și proporționale cu scopul urmărit. Acest schimb de informații păstrează confidențialitatea informațiilor respective și protejează securitatea și interesele comerciale ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale.

(6) Prezenta directivă nu aduce atingere acțiunilor întreprinse de statele membre pentru salvgardarea funcțiilor lor esențiale de stat, în special pentru salvgardarea securității naționale, inclusiv acțiuni de protejare a informațiilor a căror divulgare este considerată de statele membre contrară intereselor esențiale ale securității lor, precum și pentru menținerea legii și ordinii, în special pentru a permite investigarea, detectarea și urmărirea penală a infracțiunilor.

(7) În cazul în care un act juridic al Uniunii specific unui sector obligă operatorii de servicii esențiale sau furnizorii de servicii digitale să asigure securitatea rețelelor și sistemelor lor informatice sau să notifice incidentele, cu condiția ca aceste cerințe să aibă un efect cel puțin echivalent cu obligațiile prevăzute în prezenta directivă, se aplică respectivele dispoziții ale actului juridic al Uniunii specific sectorului în cauză.

Articolul 2

Prelucrarea datelor cu caracter personal

(1) Prelucrarea datelor cu caracter personal în temeiul prezentei directive se efectuează în conformitate cu Directiva 95/46/CE.

(2) Prelucrarea datelor cu caracter personal de către instituțiile și organele Uniunii în temeiul prezentei directive are loc în conformitate cu Regulamentul (CE) nr. 45/2001.

Articolul 3

Armonizarea minimă

Fără a aduce atingere articolului 16 alineatul (10) și obligațiilor lor în temeiul dreptului Uniunii, statele membre pot să adopte sau să mențină dispoziții în vederea obținerii unui nivel mai ridicat de securitate a rețelelor și a sistemelor informatice.

([1]) Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (JO L 345, 23.12.2008, p. 75).

([2]) 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).

([3]) 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).

Articolul 4

Definiții

În sensul prezentei directive, se aplică următoarele definiții:

1. „rețea și sistem informatic” înseamnă:

   (a) o rețea de comunicații electronice în sensul articolului 2 litera (a) din Directiva 2002/21/CE;

   (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, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate sau transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

3. „strategie națională privind securitatea rețelelor și a sistemelor informatice” înseamnă un cadru care furnizează obiective și priorități strategice privind securitatea rețelelor și a sistemelor informatice la nivel național;

4. „operator de servicii esențiale” înseamnă o entitate publică sau privată de tipul menționat în anexa II care îndeplinește criteriile prevăzute la articolul 5 alineatul (2);

5. „serviciu digital” înseamnă un serviciu în sensul articolului 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului ([1]) care este de un tip enumerat în anexa III;

6. „furnizor de servicii digitale” înseamnă orice persoană juridică care furnizează un serviciu digital;

7. „incident” înseamnă orice eveniment care are un efect real negativ asupra securității rețelelor și a sistemelor informatice;

8. „administrarea incidentului” înseamnă toate procedurile utilizate pentru detectarea, analiza și limitarea unui incident și răspunsul la acesta;

9. „risc” înseamnă orice circumstanță sau eveniment ce poate fi identificat în mod rezonabil care are un efect potențial negativ asupra securității rețelelor și a sistemelor informatice;

10. „reprezentant” înseamnă orice persoană fizică sau juridică stabilită în Uniune desemnată explicit să acționeze în numele unui furnizor de servicii digitale nestabilit în Uniune, căreia i se poate adresa autoritatea competentă națională sau CSIRT în locul furnizorului de servicii digitale în ceea ce privește obligațiile furnizorului de servicii digitale în temeiul prezentei directive;

11. „standard” înseamnă un standard în sensul articolului 2 punctul 1 din Regulamentul (UE) nr. 1025/2012;

12. „specificație” înseamnă o specificație tehnică în sensul articolului 2 punctul 4 din Regulamentul (UE) nr. 1025/2012;

13. „internet exchange point (IXP)” înseamnă o facilitate a rețelei care permite interconectarea a mai mult de două sisteme autonome independente, în special în scopul facilitării schimbului de trafic de internet; un IXP furnizează interconectare doar pentru sisteme autonome; un IXP 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;

14. „domain name system (DNS)” înseamnă un sistem de atribuire de nume distribuite ierarhic într-o rețea în care se efectuează căutări de nume de domenii;

([1]) 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).

15. „furnizor de servicii DNS” înseamnă o entitate care furnizează servicii DNS pe internet;

16. „registru de nume de domenii Top-level” înseamnă o entitate care administrează și operează înregistrarea de nume de domenii de internet într-un domeniu Top-level (TLD) specific;

17. „piață online” înseamnă un serviciu digital care permite consumatorilor și/sau comercianților, astfel cum sunt definiți la articolul 4 alineatul (1) litera (a) și, respectiv, la articolul 4 alineatul (1) litera (b) din Directiva 2013/11/UE a Parlamentului European și a Consiliului ([1]), să încheie online vânzări sau contracte de servicii cu comercianți fie pe site-ul internet al pieței online, fie pe site-ul internet al unui comerciant care utilizează servicii informatice furnizate de piața online;

18. „motor de căutare online” înseamnă un serviciu digital care permite utilizatorilor să caute, în principiu, în toate site-urile internet sau site-urile internet într-o anumită limbă pe baza unei interogații privind orice subiect sub forma unui cuvânt, a unei fraze sau a unei alte informații-cheie și care revine cu linkuri în care se pot găsi informații legate de conținutul căutat;

19. „serviciu de cloud computing” înseamnă un serviciu digital care permite accesul la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun.

Articolul 5

Identificarea operatorilor de servicii esențiale

(1) Până la 9 noiembrie 2018, pentru fiecare sector și subsector menționat în anexa II, statele membre identifică operatorii de servicii esențiale care au un sediu pe teritoriul lor.

(2) Criteriile pentru identificarea furnizorilor de servicii esențiale menționați la articolul 4 punctul 4 sunt următoarele:

(a) o entitate furnizează un serviciu esențial pentru susținerea activităților societale și/sau economice de cea mai mare importanță;

(b) furnizarea serviciului respectiv depinde de rețea și de sistemele informatice; și

(c) un incident ar avea efecte perturbatoare semnificative asupra furnizării serviciului.

(3) În sensul alineatului (1), fiecare stat membru stabilește o listă a serviciilor menționate la alineatul (2) litera (a).

(4) În sensul alineatului (1), atunci când o entitate furnizează un serviciu menționat la alineatul (2) litera (a) în două sau mai multe state membre, statele membre respective se consultă reciproc. Consultarea respectivă are loc înainte de adoptarea unei decizii privind identificarea.

(5) Statele membre, periodic și cel puțin la fiecare doi ani de la 9 mai 2018, revizuiesc și, după caz, actualizează lista operatorilor de servicii esențiale identificați.

(6) Rolul grupului de cooperare este, în conformitate cu atribuțiile menționate la articolul 11, să sprijine statele membre în adoptarea unei abordări coerente în procesul de identificare a operatorilor de servicii esențiale.

(7) În sensul revizuirii menționate la articolul 23 și până la 9 noiembrie 2018 și apoi la fiecare doi ani, statele membre transmit Comisiei informațiile necesare pentru ca aceasta să poată evalua punerea în aplicare a prezentei directive, în special coerența abordărilor de către statele membre a identificării operatorilor de servicii esențiale. Aceste informații includ cel puțin următoarele:

(a) măsuri naționale care permit identificarea operatorilor de servicii esențiale;

([1]) Directiva 2013/11/UE a Parlamentului European și a Consiliului din 21 mai 2013 privind soluționarea alternativă a litigiilor în materie de consum și de modificare a Regulamentului (CE) nr. 2006/2004 și a Directivei 2009/22/CE (Directiva privind SAL în materie de consum) (JO L 165, 18.6.2013, p. 63).

(b) lista serviciilor menționate la alineatul (3);

(c) numărul operatorilor de servicii esențiale identificați pentru fiecare sector menționat în anexa II și o indicație a importanței lor în legătură cu sectorul respectiv;

(d) limite, atunci când acestea există, pentru determinarea nivelului relevant de furnizare, în raport cu numărul de utilizatori care se bazează pe serviciul respectiv astfel cum se prevede la articolul 6 alineatul (1) litera (a) sau cu importanța operatorului de servicii esențiale respectiv astfel cum se prevede la articolul 6 alineatul (1) litera (f).

Pentru a contribui la furnizarea de informații comparabile, Comisia, ținând cont în cea mai mare măsură de avizul ENISA, poate adopta orientări tehnice adecvate privind parametrii informației menționați la prezentul alineat.

Articolul 6

Efect perturbator semnificativ

(1) La determinarea importanței unui efect perturbator menționat la articolul 5 alineatul (2) litera (c), statele membre țin cont cel puțin de următorii factori transsectoriali:

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

(b) dependența altor sectoare menționate în anexa II de serviciul furnizat de entitatea în cauză;

(c) impactul pe care l-ar putea avea incidentele, în ceea ce privește intensitatea și durata, asupra activităților economice și societale sau asupra siguranței publice;

(d) cota de piață a entității în cauză;

(e) distribuția geografică în ceea ce privește zona care ar putea fi afectată de un incident;

(f) importanța entității pentru menținerea unui nivel suficient al serviciului, ținând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv.

(2) Pentru a stabili dacă un incident ar avea un efect perturbator semnificativ, statele membre țin cont, după caz, de factorii specifici fiecărui sector.

CAPITOLUL II

CADRELE NAȚIONALE DE SECURITATE A REȚELELOR ȘI A SISTEMELOR INFORMATICE

Articolul 7

Strategia națională privind securitatea rețelelor și a sistemelor informatice

(1) Fiecare stat membru adoptă o strategie națională privind securitatea rețelelor și a sistemelor informatice care definește obiectivele strategice și măsurile politice și de reglementare adecvate, în vederea obținerii și menținerii unui nivel ridicat de securitate a rețelelor și a sistemelor informatice, și care acoperă cel puțin sectoarele menționate în anexa II și serviciile menționate în anexa III. Strategia națională privind securitatea rețelelor și a sistemelor informatice se referă, în special, la următoarele aspecte:

(a) obiectivele și prioritățile strategiei naționale privind securitatea rețelelor și a sistemelor informatice;

(b) un cadru de guvernanță pentru realizarea obiectivelor și a priorităților strategiei naționale privind securitatea rețelelor și a sistemelor informatice, care să includă rolurile și responsabilitățile organismelor guvernamentale și ale altor actori relevanți;

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

(d) indicarea programelor de instruire, sensibilizare și formare legate de strategia națională privind securitatea rețelelor și a sistemelor informatice;

(e) indicarea planurilor de cercetare și dezvoltare legate de strategia națională privind securitatea rețelelor și a sistemelor informatice;

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

(g) o listă a diferiților actori implicați în punerea în aplicare a strategiei naționale privind securitatea rețelelor și a sistemelor informatice.

(2) Statele membre pot solicita asistența ENISA la elaborarea strategiilor naționale privind securitatea rețelelor și a sistemelor informatice.

(3) Statele membre comunică strategiile lor naționale privind securitatea rețelelor și a sistemelor informatice Comisiei în termen de trei luni de la adoptarea lor. Din această comunicare, statele membre pot exclude elemente ale strategiei care au legătură cu securitatea națională.

Articolul 8

Autoritățile competente la nivel național și punctul unic de contact

(1) Fiecare stat membru desemnează una sau mai multe autorități competente la nivel național privind securitatea rețelelor și a sistemelor informatice („autoritatea competentă”) care acoperă cel puțin sectoarele menționate în anexa II și serviciile menționate în anexa III. Statele membre pot atribui acest rol unei autorități sau unor autorități existente.

(2) Autoritățile competente monitorizează aplicarea prezentei directive la nivel național.

(3) Fiecare stat membru desemnează un punct unic de contact național privind securitatea rețelelor și a sistemelor informatice („punct unic de contact”). Statele membre pot atribui acest rol unei autorități existente. În cazul în care un stat membru desemnează o singură autoritate competentă, aceasta servește, de asemenea, ca punct unic de contact.

(4) Punctul unic de contact exercită o funcție de legătură pentru asigurarea cooperării transfrontaliere a autorităților statului membru și cu autoritățile relevante din alte state membre, precum și cu grupul de cooperare menționat la articolul 11 și rețeaua CSIRT menționată la articolul 12.

(5) Statele membre se asigură că autoritățile 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. Statele membre asigură cooperarea eficace, eficientă și sigură a reprezentanților desemnați în grupul de cooperare.

(6) Autoritățile competente și punctul unic de contact se consultă și cooperează, după caz și în conformitate cu dreptul intern, cu autoritățile naționale de aplicare a legii și cu autoritățile naționale de protecție a datelor relevante.

(7) Fiecare stat membru notifică fără întârziere Comisiei desemnarea autorității competente și a punctului unic de contact, atribuțiile acestora și orice modificări ulterioare ale acestora. Fiecare stat membru face publică desemnarea autorității competente și a punctului unic de contact. Comisia publică lista punctelor unice de contact desemnate.

Articolul 9

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

(1) Fiecare stat membru desemnează una sau mai multe echipe CSIRT care respectă cerințele stabilite în anexa I punctul 1 și care acoperă cel puțin sectoarele menționate în anexa II și serviciile menționate în anexa III, responsabile pentru administrarea riscurilor și a incidentelor în conformitate cu o procedură bine definită. O echipă CSIRT poate fi înființată în cadrul unei autorități competente.

(2) Statele membre se asigură că echipele CSIRT dispun de resurse adecvate pentru a-și îndeplini efectiv atribuțiile stabilite în anexa I punctul 2.

Statele membre asigură cooperarea efectivă, eficientă și sigură a propriilor echipe CSIRT în cadrul rețelei CSIRT menționate la articolul 12.

(3) Statele membre se asigură că echipele lor CSIRT au acces la o infrastructură de comunicare și informații adecvată, sigură și rezilientă la nivel național.

(4) Statele membre informează Comisia cu privire la misiunea, precum și la principalele elemente ale procedurilor de administrare a incidentelor folosite de echipele CSIRT.

(5) Statele membre pot solicita asistența ENISA la dezvoltarea echipelor CSIRT naționale.

Articolul 10

Cooperarea la nivel național

(1) Atunci când sunt separate, autoritatea competentă, punctul unic de contact și echipele CSIRT ale aceluiași stat membru cooperează cu privire la îndeplinirea obligațiilor ce le revin în temeiul prezentei directive.

(2) Statele membre se asigură că fie autoritățile competente, fie echipele CSIRT primesc notificările incidentelor transmise în conformitate cu prezenta directivă. În cazul în care un stat membru decide ca echipele CSIRT să nu primească notificări, se acordă acestora, în măsura necesară pentru a-și îndeplini atribuțiile, acces la datele privind incidentele notificate de operatorii de servicii esențiale în conformitate cu articolul 14 alineatele (3) și (5) sau de furnizorii de servicii digitale în conformitate cu articolul 16 alineatele (3) și (6).

(3) Statele membre se asigură că autoritățile competente sau CSIRT informează punctele unice de contact despre notificările incidentelor transmise în conformitate cu prezenta directivă.

Până la 9 august 2018 și, ulterior, în fiecare an, punctul unic de contact transmite grupului de cooperare un raport de sinteză privind notificările primite, care include numărul de notificări și natura incidentelor notificate, precum și acțiunile întreprinse în conformitate cu articolul 14 alineatele (3) și (5) și cu articolul 16 alineatele (3) și (6).

CAPITOLUL III

COOPERARE

Articolul 11

Grupul de cooperare

(1) Se stabilește un grup de cooperare, pentru a sprijini și pentru a facilita cooperarea strategică și schimbul de informații între statele membre, pentru a consolida încrederea și în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

Grupul de cooperare își îndeplinește atribuțiile pe baza programelor bienale de lucru, astfel cum sunt menționate la alineatul (3) al doilea paragraf.

(2) Grupul de cooperare se compune din reprezentanți ai statelor membre, ai Comisiei și ai ENISA.

După caz, grupul de cooperare poate invita să participe la lucrările sale reprezentanți ai părților interesate relevante.

Comisia asigură secretariatul.

(3) Grupului de cooperare îi revin următoarele atribuții:

(a) furnizează orientări strategice pentru activitățile rețelei CSIRT stabilite în temeiul articolului 12;

(b) participă la schimbul de bune practici privind schimbul de informații legate de notificarea incidentelor menționată la articolul 14 alineatele (3) și (5) și la articolul 16 alineatele (3) și (6);

(c) participă la schimbul de bune practici între statele membre și, în colaborare cu ENISA, asistă statele membre la consolidarea capacității în securitatea rețelelor și a sistemelor informatice;

(d) discută despre capacitățile și nivelul de pregătire ale statelor membre și, pe bază de voluntariat, evaluează strategiile naționale privind securitatea rețelelor și a sistemelor informatice și eficacitatea echipelor CSIRT și identifică cele mai bune practici;

(e) participă la schimbul de informații și de bune practici privind sensibilizarea și formarea;

(f) participă la schimbul de informații și de bune practici privind cercetarea și dezvoltarea legate de securitatea rețelelor și a sistemelor informatice;

(g) după caz, participă la schimbul de experiență privind aspecte legate de securitatea rețelelor și a sistemelor informatice cu instituții, organe, oficii și agenții relevante ale Uniunii;

(h) discută standardele și specificațiile menționate la articolul 19 cu reprezentanți ai organizațiilor de standardizare europene relevante;

(i) colectează informații referitoare la bunele practici privind riscurile și incidentele;

(j) examinează anual rapoartele de sinteză menționate la articolul 10 alineatul (3) al doilea paragraf;

(k) discută despre lucrările efectuate în legătură cu exercițiile privind securitatea rețelelor și a sistemelor informatice, programele educative și formarea, inclusiv lucrările ENISA;

(l) cu asistența ENISA, participă la schimbul de bune practici privind identificarea operatorilor de servicii esențiale de către statele membre, inclusiv în legătură cu dependența transfrontalieră legată de riscuri și incidente de securitate;

(m) discută modalități de raportare a notificărilor de incidente menționate la articolele 14 și 16.

Până la 9 februarie 2018 și, ulterior, la fiecare doi ani, Grupul de cooperare stabilește un program de activitate cu privire la acțiunile care urmează să fie întreprinse pentru punerea în aplicare a obiectivelor și atribuțiilor sale, care să fie în conformitate cu obiectivele prezentei directive;

(4) În scopul revizuirii menționate la articolul 23, grupul de cooperare întocmește până la 9 august 2018 și, ulterior, la fiecare 18 luni, un raport de evaluare a experienței câștigate prin cooperarea strategică realizată în temeiul prezentului articol.

(5) Comisia adoptă acte de punere în aplicare prin care se stabilesc acordurile procedurale necesare pentru funcționarea grupului de cooperare. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 22 alineatul (2).

În sensul primului paragraf, Comisia transmite primul proiect de act de punere în aplicare până la 9 februarie 2017 comitetului menționat la articolul 22 alineatul (1).

Articolul 12

Rețeaua CSIRT

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

(2) Rețeaua CSIRT se compune din reprezentanți ai echipelor CSIRT ale statelor membre și ai CERT-UE. Comisia participă la rețeaua CSIRT în calitate de observator. ENISA asigură secretariatul și sprijină activ cooperarea între echipele CSIRT.

(3) Rețelei CSIRT îi revin următoarele atribuții:

(a) participă la schimbul de informații privind serviciile, operațiunile și capacitățile de cooperare ale echipelor CSIRT;

(b) la cererea reprezentantului unei echipe CSIRT a unui stat membru potențial afectat de un incident, schimbă și discută informații sensibile fără caracter comercial legate de incidentul respectiv și de riscurile asociate; cu toate acestea, orice echipă CSIRT a unui stat membru poate refuza să contribuie la discuția respectivă dacă există riscul de a se prejudicia anchetarea incidentului;

(c) participă la schimbul de informații și pune la dispoziție în mod voluntar informații fără caracter confidențial privind incidente individuale;

(d) la cererea reprezentantului unei echipe CSIRT dintr-un stat membru, discută și, după caz, identifică un răspuns coordonat la un incident care a fost identificat în jurisdicția respectivului stat membru;

(e) acordă statelor membre sprijin în abordarea incidentelor transfrontaliere pe baza asistenței reciproce voluntare a acestora;

(f) discută, explorează și identifică noi forme de cooperare operațională, inclusiv în legătură cu:

(i) categorii de riscuri și incidente;

(ii) alertele timpurii;

(iii) asistența reciprocă;

(iv) principii și modalități de coordonare, atunci când statele membre răspund la riscuri și incidente transfrontaliere;

(g) informează grupul de cooperare cu privire la activitățile sale și cu privire la noi forme de cooperare operațională discutate în conformitate cu litera (f) și solicită orientări aferente acestora;

(h) discută lecțiile învățate din exercițiile care privesc securitatea rețelelor și sistemelor informatice, inclusiv din cele organizate de ENISA;

(i) la cererea unei anumite echipe CSIRT, discută despre capacitățile și nivelul de pregătire al aceleiași echipe CSIRT;

(j) emite orientări pentru a facilita convergența practicilor operaționale în ceea ce privește aplicarea dispozițiilor prezentului articol privind cooperarea operațională.

(4) În scopul revizuirii menționate la articolul 23, rețeaua CSIRT întocmește până la 9 august 2018 și, ulterior, la fiecare 18 luni, un raport de evaluare a experienței câștigate prin cooperarea operațională realizată în temeiul prezentului articol, inclusiv concluzii și recomandări. Raportul se transmite, de asemenea, grupului de cooperare.

(5) Rețeaua CSIRT își stabilește propriul regulament de procedură.

Articolul 13

Cooperarea internațională

Uniunea poate încheia, 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. Aceste acorduri țin seama de necesitatea de a se asigura o protecție adecvată a datelor.

CAPITOLUL IV

SECURITATEA REȚELELOR ȘI A SISTEMELOR INFORMATICE ALE OPERATORILOR DE SERVICII ESENȚIALE

Articolul 14

Cerințe de securitate și notificarea incidentelor

(1) Statele membre se asigură că operatorii de servicii esențiale iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care le utilizează în activitățile lor. Ținând seama de cele mai avansate cunoștințe în domeniu, măsurile respective asigură un nivel de securitate a rețelelor și a sistemelor informatice adecvat riscului existent.

(2) Statele membre se asigură că operatorii de servicii esențiale iau măsuri adecvate pentru a preveni și pentru a minimiza impactul incidentelor care afectează securitatea rețelelor și a sistemelor informatice utilizate pentru furnizarea acestor servicii esențiale, cu scopul de a asigura continuitatea serviciilor respective.

(3) Statele membre se asigură că operatorii de servicii esențiale notifică autorității competente sau echipelor CSIRT, fără întârzieri nejustificate, incidentele care au un impact semnificativ asupra continuității serviciilor esențiale pe care le furnizează. Notificările includ informații care să permită autorității competente sau echipelor CSIRT să stabilească orice impact transfrontalier al incidentului. Notificarea nu expune partea care notifică unei răspunderi sporite.

(4) Pentru a determina importanța impactului unui incident, se ține cont în mod special de următorii parametri:

(a) numărul de utilizatori afectați de perturbarea serviciului esențial;

(b) durata incidentului;

(c) distribuția geografică în ceea ce privește zona afectată de incident.

(5) Pe baza informațiilor furnizate de operatorul de servicii esențiale în notificarea sa, autoritatea competentă sau echipa CSIRT informează celălalt (celelalte) stat(e) membru (membre) afectat(e) dacă incidentul are un impact semnificativ asupra continuității serviciilor esențiale în statul (statele) membru (membre) respectiv(e). Astfel, autoritatea competentă sau echipa CSIRT, în conformitate cu dreptul Uniunii sau cu legislația națională conformă cu dreptul Uniunii, apără interesele de securitate și comerciale ale operatorului de servicii esențiale, precum și confidențialitatea informațiilor furnizate în notificare.

Atunci când circumstanțele o permit, autoritatea competentă sau echipa CSIRT furnizează operatorului de servicii esențiale care a făcut notificarea informații relevante în ceea ce privește acțiunile ulterioare notificării, de exemplu informații care ar putea sprijini administrarea eficace a incidentului.

La cererea autorității competente sau a echipei CSIRT, punctul unic de contact transmite notificările menționate la primul paragraf punctelor unice de contact din alte state membre afectate.

(6) După consultarea operatorului de servicii esențiale care a făcut notificarea, autoritatea competentă sau echipa CSIRT poate informa publicul cu privire la anumite incidente, în legătură cu care este necesară sensibilizarea publicului pentru a se preveni un incident sau pentru a se administra un incident în curs.

(7) Autoritățile competente care acționează împreună în cadrul grupului de cooperare pot elabora și adopta orientări privind circumstanțele în care operatorii de servicii esențiale sunt obligați să notifice incidente, inclusiv privind parametrii pentru stabilirea importanței impactului unui incident, astfel cum se menționează la alineatul (4).

Articolul 15

Punere în aplicare și executare

(1) Statele membre se asigură că autoritățile competente dețin competențele și mijloacele necesare pentru a evalua măsura în care operatorii de servicii esențiale se conformează obligațiilor care le revin în temeiul articolului 14, precum și efectele acesteia asupra securității rețelelor și a sistemelor informatice.

(2) Statele membre garantează că autoritățile competente dețin competențele și mijloacele pentru a solicita operatorilor de servicii esențiale să furnizeze:

(a) informațiile necesare pentru evaluarea securității rețelelor și a sistemelor lor informatice, inclusiv politicile de securitate documentate;

(b) dovezi privind punerea efectivă în aplicare a politicilor de securitate, precum rezultatele unui audit de securitate realizat de autoritatea competentă sau de un auditor calificat și, în acest din urmă caz, să pună la dispoziția autorității competente rezultatele auditului, inclusiv probele pe care se bazează acesta.

Atunci când solicită astfel de informații sau dovezi, autoritatea competentă menționează scopul solicitării și precizează informațiile necesare.

(3) În urma evaluării informațiilor sau a rezultatelor auditurilor de securitate menționate la alineatul (2), autoritatea competentă poate emite instrucțiuni obligatorii pentru operatorii de servicii esențiale pentru ca aceștia să remedieze deficiențele constatate.

(4) Autoritatea competentă lucrează în strânsă cooperare cu autoritățile de protecție a datelor în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal.

CAPITOLUL V

SECURITATEA REȚELELOR ȘI A SISTEMELOR INFORMATICE ALE FURNIZORILOR DE SERVICII DIGITALE

Articolul 16

Cerințe de securitate și notificarea incidentelor

(1) Statele membre se asigură că furnizorii de servicii digitale identifică și iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care le utilizează în contextul oferirii de servicii menționate în anexa III pe teritoriul Uniunii. Ținând seama de cele mai avansate cunoștințe în domeniu, măsurile respective asigură un nivel de securitate a rețelelor și a sistemelor informatice adecvat riscului existent și țin cont de următoarele elemente:

(a) securitatea sistemelor și a instalațiilor;

(b) gestionarea incidentelor;

(c) gestionarea continuității activității;

(d) monitorizarea, auditarea și testarea;

(e) conformitatea cu standardele internaționale.

(2) Statele membre garantează luarea de către furnizorii de servicii digitale a unor măsuri de prevenire și de minimalizare a impactului incidentelor care afectează securitatea rețelelor și a sistemelor informatice în legătură cu serviciile menționate în anexa III care sunt oferite pe teritoriul Uniunii, în vederea asigurării continuității serviciilor respective.

(3) Statele membre garantează că furnizorii de servicii digitale notifică, fără întârziere nejustificată, autorității competente sau echipei CSIRT orice incident care are un impact substanțial asupra furnizării unui serviciu astfel cum se menționează în anexa III pe care îl oferă pe teritoriul Uniunii. Notificările includ informații care să ofere autorității competente sau echipei CSIRT posibilitatea de a stabili importanța oricărui impact transfrontalier. Notificarea nu expune partea care notifică unei răspunderi sporite.

(4) Pentru a determina dacă impactul unui incident este important, se ține cont în mod special de următorii parametri:

(a) numărul de utilizatori afectați de incident, în special utilizatori care se bazează pe serviciu pentru furnizarea propriilor servicii;

(b) durata incidentului;

(c) distribuția geografică în ceea ce privește zona afectată de incident;

(d) amploarea perturbării funcționării serviciului;

(e) amploarea impactului asupra activităților economice și societale.

Obligația de a notifica un incident se aplică doar în cazul în care furnizorul de servicii digitale are acces la informațiile necesare pentru a evalua impactul unui incident asupra parametrilor menționați la primul paragraf.

(5) În cazul în care un operator de servicii esențiale se bazează pe un terț furnizor de servicii digitale pentru furnizarea unui serviciu care este esențial pentru întreținerea unor activități societale și economice de cea mai mare importanță, operatorul respectiv notifică orice impact semnificativ asupra continuității serviciilor esențiale din cauza unui incident care afectează furnizorul de servicii digitale.

(6) După caz, dar mai ales dacă incidentul menționat la alineatul (3) implică două sau mai multe state membre, autoritatea competentă sau echipa CSIRT informează alte state membre afectate. Autoritățile competente, echipele CSIRT și punctele unice de contact, în conformitate cu dreptul Uniunii sau cu legislația națională conformă cu dreptul Uniunii, păstrează interesele de securitate și comerciale ale furnizorului de servicii digitale, precum și confidențialitatea informațiilor furnizate.

(7) După consultarea furnizorului de servicii digitale în cauză, autoritatea competentă sau echipa CSIRT și, după caz, autoritățile sau echipele CSIRT ale altor state membre vizate pot informa publicul cu privire la incidente individuale sau pot solicita furnizorului de servicii digitale să facă acest lucru, în cazul în care sensibilizarea publicului este necesară pentru prevenirea unui incident sau pentru administrarea unui incident în curs sau în cazul în care divulgarea incidentului este de interes public în alt fel.

(8) Comisia adoptă acte de punere în aplicare în scopul de a preciza elementele menționate la alineatul (1) și parametrii enumerați la alineatul (4) din prezentul articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 22 alineatul (2) până la 9 august 2017.

(9) Comisia adoptă acte de punere în aplicare prin care se stabilesc formatele și procedurile aplicabile cerințelor de notificare. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 22 alineatul (2).

(10) Fără a aduce atingere articolului 1 alineatul (6), statele membre nu impun furnizorilor de servicii digitale nicio altă cerință de securitate sau de notificare.

(11) Capitolul V nu se aplică microîntreprinderilor și întreprinderilor mici, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei ([1]).

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

Articolul 17

Punere în aplicare și executare

(1) Statele membre se asigură că autoritățile competente acționează, dacă este necesar, prin măsuri de supraveghere *ex post*, atunci când primesc dovezi conform cărora un furnizor de servicii digitale nu îndeplinește cerințele specificate la articolul 16. Aceste dovezi pot fi transmise de o autoritate competentă a unui alt stat membru în care se furnizează serviciul.

(2) În sensul alineatului (1), autoritățile competente au competențele și mijloacele necesare pentru a solicita furnizorilor de servicii digitale:

(a) să furnizeze informațiile necesare pentru evaluarea securității rețelelor și a sistemelor lor informatice, inclusiv politicile de securitate documentate;

(b) să remedieze orice neîndeplinire a cerințelor specificate la articolul 16.

(3) Dacă un furnizor de servicii digitale își are sediul principal sau un reprezentant într-un stat membru, dar rețelele și sistemele sale informatice sunt situate într-unul sau mai multe alte state membre, autoritatea competentă a statului membru în care se află sediul principal sau reprezentantul și autoritățile competente ale acelor alte state membre cooperează și își oferă asistență reciprocă, după caz. Această asistență și cooperare poate cuprinde schimburi de informații între autoritățile competente în cauză și solicitări de a se lua măsurile de supraveghere menționate la alineatul (2).

Articolul 18

Jurisdicție și teritorialitate

(1) În sensul prezentei directive, un furnizor de servicii digitale se consideră sub jurisdicția statului membru în care își are sediul principal. Se consideră că un furnizor de servicii digitale își are sediul principal într-un stat membru în cazul în care sediul său social se află în statul membru respectiv.

(2) Un furnizor de servicii digitale care nu este stabilit în Uniune, dar oferă servicii astfel cum se menționează în anexa III pe teritoriul Uniunii desemnează un reprezentant în Uniune. Reprezentantul se stabilește într-unul dintre statele membre în care se oferă serviciile. Furnizorul de servicii digitale se consideră sub jurisdicția statului membru în care este stabilit reprezentantul.

(3) Desemnarea de către furnizorul de servicii digitale a unui reprezentant nu aduce atingere acțiunilor în justiție care ar putea fi inițiate împotriva furnizorului de servicii digitale însuși.

CAPITOLUL VI

STANDARDIZAREA ȘI NOTIFICAREA VOLUNTARĂ

Articolul 19

Standardizarea

(1) Pentru promovarea aplicării convergente a articolului 14 alineatele (1) și (2) și a articolului 16 alineatele (1) și (2), statele membre, fără a impune sau a discrimina în favoarea utilizării unui anumit tip de tehnologie, încurajează utilizarea standardelor și specificațiilor europene sau a celor acceptate la nivel internațional relevante pentru securitatea rețelelor și a sistemelor informatice.

(2) ENISA, în colaborare cu statele membre, 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 ale statelor membre, care ar permite reglementarea acestor domenii.

Articolul 20

Notificarea voluntară

(1) Fără a aduce atingere articolului 3, entitățile care nu au fost identificate drept operatori de servicii esențiale și nu sunt furnizori de servicii digitale pot notifica voluntar incidente care au un impact semnificativ asupra continuității serviciilor pe care le furnizează.

(2) La tratarea notificărilor, statele membre acționează în conformitate cu procedura stabilită la articolul 14. Statele membre pot trata notificările obligatorii cu prioritate față de notificările voluntare. Notificările voluntare se tratează doar atunci când această prelucrare nu constituie o sarcină disproporționată sau neavenită asupra statului membru în cauză.

Notificarea voluntară nu impune entității notificatoare nicio obligație care nu i-ar fi revenit dacă nu ar fi făcut notificarea.

CAPITOLUL VII

DISPOZIȚII FINALE

Articolul 21

Sancțiuni

Statele membre stabilesc regimul sancțiunilor aplicabile în cazurile de încălcare a dispozițiilor de drept intern adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a asigura punerea în aplicare a acestora. Sancțiunile prevăzute sunt eficace, proporționale și disuasive. Statele membre notifică aceste norme și aceste măsuri Comisiei până la 9 mai 2018 și notifică acesteia, fără întârziere, orice modificare ulterioară a acestora.

Articolul 22

Procedura comitetului

(1) Comisia este asistată de Comitetul pentru securitatea rețelelor și a sistemelor informatice. Comitetul respectiv reprezintă un comitet în sensul Regulamentului (UE) nr. 182/2011.

(2) Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

Articolul 23

Revizuire

(1) Până la 9 mai 2019, Comisia transmite Parlamentului European și Consiliului un raport de evaluare a coerenței abordării adoptate de statele membre în procesul de identificare a operatorilor de servicii esențiale.

(2) Comisia revizuiește periodic funcționarea prezentei directive și prezintă un raport Parlamentului European și Consiliului. 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. În revizuirea sa, Comisia evaluează și listele prevăzute în anexele II și III, precum și coerența identificării operatorilor de servicii esențiale și a serviciilor din sectoarele menționate în anexa II. Primul raport se transmite până la 9 mai 2021.

Articolul 24

Măsuri tranzitorii

(1) Fără a aduce atingere articolului 25 și pentru a oferi statelor membre posibilități suplimentare de cooperare adecvată pe parcursul perioadei de transpunere, grupul de cooperare și rețeaua CSIRT încep să își îndeplinească atribuțiile stabilite la articolul 11 alineatul (3) și respectiv la articolul 12 alineatul (3) până la 9 februarie 2017.

(2) În perioada cuprinsă între 9 februarie 2017 și 9 noiembrie 2018 și în vederea sprijinirii statelor membre în adoptarea unei abordări coerente a procesului de identificare a operatorilor de servicii esențiale, grupul de cooperare discută despre procesul, substanța, tipul măsurilor naționale care permit identificarea operatorilor de servicii esențiale în cadrul unui sector specific în conformitate cu criteriile stabilite la articolele 5 și 6. De asemenea, grupul de cooperare discută, la cererea unui stat membru, proiecte specifice de măsuri naționale ale statului membru respectiv, care să permită identificarea operatorilor de servicii esențiale în cadrul unui anumit sector, în conformitate cu criteriile stabilite la articolele 5 și 6.

(3) Până la 9 februarie 2017 și în scopul prezentului articol, statele membre asigură reprezentarea adecvată în grupul de cooperare și în rețeaua CSIRT.

Articolul 25

Transpunere

(1) Statele membre adoptă și publică până la 9 mai 2018 actele cu putere de lege și actele administrative necesare pentru a se conforma prezentei directive. Statele membre comunică fără întârziere Comisiei textul acestor acte.

Acestea aplică măsurile respective începând cu 10 mai 2018.

Atunci când statele membre adoptă actele respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o astfel de trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

(2) Statele membre comunică Comisiei textul principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.

Articolul 26

Intrare în vigoare

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

Articolul 27

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Strasbourg, 6 iulie 2016.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
M. SCHULZ	I. KORČOK

ANEXA I

CERINȚE ȘI ATRIBUȚII ALE ECHIPEI DE INTERVENȚIE ÎN CAZ DE INCIDENTE DE SECURITATE INFORMATICĂ (CSIRT)

Cerințele și atribuțiile echipei CSIRT sunt definite în mod adecvat și clar pe baza unei politici și/sau a unei reglementări naționale. Acestea includ următoarele:

1. Cerințe pentru echipa CSIRT

   (a) Echipa CSIRT asigură o disponibilitate ridicată a serviciilor sale de comunicații, evitând punctele unice de defecțiune și dispunând de mai multe mijloace pentru a fi contactată și pentru a contacta alte entități în orice moment. În plus, canalele de comunicare trebuie să fie clar specificate și bine cunoscute bazei sale de utilizatori și partenerilor de cooperare.

   (b) Localurile echipei CSIRT și sistemele informatice de suport sunt situate pe amplasamente securizate.

   (c) Continuitatea activităților:

      (i) echipa CSIRT dispune de un sistem adecvat de gestionare și rutare a cererilor, cu scopul de a facilita transferurile;

      (ii) echipa CSIRT dispune de personal adecvat pentru a asigura o disponibilitate permanentă;

      (iii) echipa CSIRT se bazează pe o infrastructură a cărei continuitate este asigurată. În acest scop se pun la dispoziție sisteme redundante și spațiu de lucru de rezervă.

   (d) Echipa CSIRT are posibilitatea de a participa, după dorință, la rețele internaționale de cooperare.

2. Atribuțiile echipei CSIRT

   (a) Atribuțiile echipei CSIRT includ cel puțin următoarele:

      (i) monitorizarea incidentelor la nivel național;

      (ii) asigurarea de avertizări timpurii, alerte, anunțuri și diseminare de informații privind riscurile și incidentele pentru părțile interesate relevante;

      (iii) răspunsul la incidente;

      (iv) furnizarea de analize dinamice de risc și de incident și sensibilizare situațională;

      (v) participarea la rețeaua CSIRT.

   (b) Echipa CSIRT stabilește relații de cooperare cu sectorul privat.

   (c) Pentru a facilita cooperarea, echipa CSIRT promovează adoptarea și utilizarea unor practici comune sau standardizate pentru:

      (i) procedurile de administrare a incidentelor și a riscurilor;

      (ii) sistemele de clasificare a incidentelor, riscurilor și informațiilor.

ANEXA II

TIPURI DE ENTITĂȚI ÎN SENSUL ARTICOLULUI 4 PUNCTUL 4

Sectorul	Subsectorul	Tipul de entitate
1. Energie	(a) Electricitate	— Întreprinderi din domeniul energiei electrice, astfel cum sunt definite la articolul 2 punctul 35 din Directiva 2009/72/CE a Parlamentului European și a Consiliului20 ([1]), care îndeplinește funcția de „furnizare", astfel cum este definită la articolul 2 punctul 19 din directiva respectivă
		— Operatori de distribuție, astfel cum sunt definiți la articolul 2 punctul 6 din Directiva 2009/72/CE
		— Operatori de transport și de sistem, astfel cum sunt definiți la articolul 2 punctul 4 din Directiva 2009/72/CE
	(b) Petrol	— Operatori de conducte de transport al petrolului
		— Operatori ai instalațiilor de producție, de rafinare și de tratare a petrolului, de depozitare și de transport
	(c) Gaze naturale	— Întreprinderi de furnizare, astfel cum sunt definite la articolul 2 punctul 8 din Directiva 2009/73/CE a Parlamentului European și a Consiliului21 ([2])
		— Operatori de distribuție, astfel cum sunt definiți la articolul 2 punctul 6 din Directiva 2009/73/CE
		— Operatori de transport și de sistem, astfel cum sunt definiți la articolul 2 punctul 4 din Directiva 2009/73/CE
		— Operatori de înmagazinare, astfel cum sunt definiți la articolul 2 punctul 10 din Directiva 2009/73/CE
		— Operatori de sistem GNL, astfel cum este definit la articolul 2 punctul 12 din Directiva 2009/73/CE
		— Întreprinderi din sectorul gazelor naturale, astfel cum este definită la articolul 2 punctul 1 din Directiva 2009/73/CE
		— Operatori de instalație de rafinare și de tratare a gazelor naturale
2. Transport	(a) Transport aerian	— Transportatori aerieni, astfel cum sunt definiți la articolul 3 punctul 4 din Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului ([3])
		— Organe de administrare a aeroportului, astfel cum sunt definite la articolul 2 punctul 2 din Directiva 2009/12/CE a Parlamentului European și a Consiliului23 ([4]), aeroporturi, 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 ([5]), precum și entități care operează instalații auxiliare în cadrul aeroporturilor.

Sectorul	Subsectorul	Tipul de entitate
		— Operatori 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 ([6])
	(b) Transport feroviar	— Administratori de infrastructuri, astfel cum sunt definiți la articolul 3 punctul 2 din Directiva 2012/34/UE a Parlamentului European și a Consiliului ([7])
		— Întreprinderi feroviare, astfel cum sunt definite la articolul 3 punctul 1 din Directiva 2012/34/UE, inclusiv operatori ai unor infrastructuri de servicii, astfel cum sunt definiți la articolul 3 punctul 12 din Directiva 2012/34/UE
	(c) Transport pe apă	— Companii 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 ([8]), fără a include navele individuale operate de companiile respective
		— Organe de gestionare a porturilor, astfel cum sunt definite la articolul 3 punctul 1 din Directiva 2005/65/CE a Parlamentului European și a Consiliului ([9]), inclusiv instalațiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004 și entitățile care operează lucrări și echipamente în cadrul porturilor
		— Operatori de servicii de trafic naval, astfel cum sunt definite la articolul 3 litera (o) din Directiva 2002/59/CE a Parlamentului European și a Consiliului ([10])
	(d) Transport rutier	— Autorități rutiere, astfel cum sunt definite la articolul 2 punctul 12 din Regulamentul delegat (UE) 2015/962 al Comisiei ([11]) responsabile pentru controlul gestionării traficului
		— Operatori 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 ([12])
3. Sectorul bancar		Instituții de credit, astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului ([13])
4. Infrastructuri ale pieței financiare		— Operatori de locuri de tranzacționare, astfel cum sunt definite la articolul 4 punctul 24 din Directiva 2014/65/UE a Parlamentului European și a Consiliului ([14])
		— Contrapartide centrale, astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului ([15])
5. Sectorul sănătății	Instituții de asistență medicală (inclusiv spitale și clinici private)	Furnizori de servicii medicale, astfel cum sunt definiți la articolul 3 litera (g) din Directiva 2011/24/UE a Parlamentului European și a Consiliului ([16])

Sectorul	Subsectorul	Tipul de entitate
6. Furnizarea și distribuirea de apă potabilă		Furnizori și distribuitori de „apă destinată consumului uman”, astfel cum este definită la articolul 2 punctul 1 litera (a) din Directiva 98/83/CE a Consiliului ([17]), excluzând distribuitorii pentru care distribuția de apă destinată consumului uman reprezintă doar o parte din activitatea lor generală de distribuție a altor produse de bază și produse care nu sunt considerate servicii esențiale.
7. Infrastructură digitală		— IXP
		— DNS
		— TLD

([1]) Directiva 2009/72/CE a Parlamentului European și a Consiliului din 13 iulie 2009 privind normele comune pentru piața internă a energiei electrice și de abrogare a Directivei 2003/54/CE (JO L 211, 14.8.2009, p. 55).
([2]) 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).
([3]) 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).
([4]) 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).
([5]) 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).
([6]) 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).
([7]) 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).
([8]) 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).
([9]) 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).
([10]) 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).
([11]) 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).
([12]) 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).
([13]) Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și societățile de investiții și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).
([14]) 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).
([15]) 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).
([16]) 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).
([17]) Directiva 98/83/CE a Consiliului din 3 noiembrie 1998 privind calitatea apei destinate consumului uman (JO L 330, 5.12.1998, p. 32).

ANEXA III

TIPURI DE SERVICII DIGITALE ÎN SENSUL ARTICOLULUI 4 PUNCTUL 5

1. Piață online
2. Motor de căutare online
3. Serviciu de cloud computing