COMISIA
EUROPEANĂ

Bruxelles, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Propunere de

DIRECTIVĂ A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148

(Text cu relevanță pentru SEE)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Motivele și obiectivele propunerii

Prezenta propunere face parte dintr-un pachet de măsuri menite să îmbunătățească și mai mult capacitatea de reziliență și capacitatea de răspuns la incidente ale entităților publice și private, ale autorităților competente și ale Uniunii în ansamblu în domeniul securității cibernetice și al protecției infrastructurilor critice. Propunerea reflectă prioritățile Comisiei de a pregăti Europa pentru era digitală și de a construi o economie capabilă să facă față provocărilor viitorului și aflată în serviciul cetățenilor. Securitatea cibernetică este o prioritate în răspunsul Comisiei la criza provocată de pandemia de COVID-19. Pachetul include o nouă strategie privind securitatea cibernetică, menită să consolideze autonomia strategică a Uniunii pentru a-și îmbunătăți reziliența și răspunsul colectiv și pentru a construi un internet deschis și global. Pachetul conține și o propunere de directivă privind reziliența operatorilor critici de servicii esențiale, care vizează atenuarea amenințărilor fizice la adresa acestor operatori.

Prezenta propunere se bazează pe Directiva (UE) 2016/1148 privind securitatea rețelelor și a sistemelor informatice (Directiva NIS) și abrogă această directivă, care este primul act legislativ privind securitatea cibernetică adoptat la nivelul UE. Propunerea prevede măsuri juridice de stimulare a nivelului general de securitate cibernetică în Uniune. Directiva NIS (1) a contribuit la îmbunătățirea capacităților în materie de securitate cibernetică la nivel național, solicitând statelor membre să adopte strategii naționale de securitate cibernetică și să desemneze autorități de securitate cibernetică; (2) a contribuit la intensificarea cooperării între statele membre la nivelul Uniunii prin înființarea a diferite foruri menite să faciliteze schimbul de informații strategice și operaționale; și (3) a îmbunătățit reziliența cibernetică a entităților publice și private în șapte sectoare specifice (energia, transporturile, sectorul bancar, infrastructurile piețelor financiare, asistența medicală, furnizarea și distribuția de apă potabilă și infrastructurile digitale) și în cadrul a trei servicii digitale (piețele online, motoarele de căutare online și serviciile de cloud computing), solicitând statelor membre să se asigure că operatorii de servicii esențiale și furnizorii de servicii digitale instituie cerințe în materie de securitate cibernetică și raportează incidentele.

Propunerea modernizează cadrul juridic existent, ținând seama de intensificarea digitalizării pieței interne în ultimii ani și de evoluția situației amenințărilor la adresa securității cibernetice. Ambele tendințe s-au amplificat de la începutul crizei provocate de pandemia de COVID-19. Propunerea abordează, de asemenea, o serie de deficiențe care au împiedicat valorificarea întregului potențial al Directivei NIS.

În pofida realizărilor sale notabile, Directiva NIS, care a pregătit terenul pentru o schimbare semnificativă de mentalitate în legătură cu abordarea instituțională și de reglementare a securității cibernetice în multe state membre, și-a dovedit și limitările. Transformarea digitală a societății (intensificată de criza provocată de pandemia de COVID-19) a extins situația amenințărilor și generează noi provocări care necesită răspunsuri adaptate și inovatoare. Numărul atacurilor cibernetice este în continuă creștere, atacurile, care sunt tot mai sofisticate, provenind dintr-o gamă largă de surse din interiorul și din afara UE.

În urma evaluării funcționării Directivei NIS, efectuată în scopul evaluării impactului, au fost identificate următoarele aspecte: (1) un nivel scăzut de reziliență cibernetică a întreprinderilor care își desfășoară activitatea în UE; (2) reziliență inconsecventă în toate statele membre și în toate sectoarele; și (3) un nivel scăzut de conștientizare comună a situației și lipsa unui răspuns comun în caz de criză. De exemplu, anumite spitale importante dintr-un stat membru nu intră în domeniul de aplicare al Directivei NIS și, prin urmare, nu sunt obligate să pună în

aplicare măsurile de securitate corespunzătoare, în timp ce, într-un alt stat membru, aproape fiecare furnizor de asistență medicală din țară trebuie să respecte cerințele de securitate NIS.

Fiind o inițiativă în cadrul Programului privind o reglementare adecvată și funcțională (REFIT), propunerea vizează reducerea sarcinii de reglementare pentru autoritățile competente și a costurilor de asigurare a conformității pentru entitățile publice și private. În special, acest lucru se realizează prin eliminarea obligației autorităților competente de a identifica operatorii de servicii esențiale și prin îmbunătățirea nivelului de armonizare a cerințelor de securitate și raportare pentru a facilita respectarea reglementărilor de către entitățile care furnizează servicii transfrontaliere. În același timp, autorităților competente li se vor atribui o serie de sarcini noi, inclusiv supravegherea entităților din sectoarele care nu sunt reglementate până în prezent de Directiva NIS.

- **Coerența cu dispozițiile existente în domeniul de politică vizat**

Prezenta propunere face parte dintr-un set mai larg de instrumente juridice existente și de inițiative viitoare adoptate la nivelul Uniunii care vizează creșterea nivelului de reziliență a entităților publice și private în fața amenințărilor.

În domeniul securității cibernetice, acestea sunt, în special, Directiva (UE) 2018/1972 de instituire a Codului european al comunicațiilor electronice (ale cărei dispoziții legate de securitatea cibernetică vor fi înlocuite de dispozițiile propunerii corespunzătoare) și Propunerea de regulament privind reziliența operațională digitală a sectorului financiar [COM(2020) 595 final], care va fi considerată drept *lex specialis* a propunerii corespunzătoare după intrarea în vigoare a celor două acte legislative.

În domeniul securității fizice, propunerea completează propunerea de directivă privind reziliența entităților critice, care revizuiește Directiva 2008/114/CE privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (Directiva ICE), care instituie, la nivelul Uniunii, un proces de identificare și desemnare a infrastructurilor critice europene și care stabilește o abordare pentru îmbunătățirea protecției acestora. În iulie 2020, Comisia a adoptat Strategia UE privind uniunea securității[1], care a recunoscut o creștere a interconectării și a interdependenței infrastructurilor fizice și digitale. Aceasta a subliniat necesitatea unei abordări mai coerente și mai consecvente între Directiva ICE și Directiva (UE) 2016/1148 privind măsurile menite să asigure un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

Prin urmare, propunerea este strâns aliniată la propunerea de directivă privind reziliența entităților critice, care vizează sporirea rezilienței entităților critice în fața amenințărilor fizice într-un număr mare de sectoare. Propunerea urmărește să asigure faptul că, în temeiul celor două acte legislative, autoritățile competente iau măsuri complementare și fac schimb de informații, dacă este necesar, în ceea ce privește reziliența cibernetică și non-cibernetică, și că, în special, operatorii critici din sectoarele considerate „esențiale” pentru fiecare propunere în parte fac, de asemenea, obiectul unor obligații cu caracter mai general de consolidare a rezilienței, cu accent pe riscurile non-cibernetice.

[1] COM(2020) 605 final.

- **Coerența cu alte politici ale Uniunii**

După cum se menționează în comunicarea intitulată „Conturarea viitorului digital al Europei”[2], este esențial ca Europa să valorifice toate beneficiile erei digitale și să își consolideze capacitatea industrială și de inovare, fără a transgresa însă limitele siguranței și ale eticii. Strategia europeană privind datele stabilește patru piloni – protecția datelor, drepturile fundamentale, siguranța și securitatea cibernetică – drept condiții prealabile esențiale pentru o societate autonomizată prin utilizarea datelor.

Într-o rezoluție din 12 martie 2019, Parlamentul European a invitat *„[...] Comisia să evalueze necesitatea de a se extinde domeniul de aplicare a Directivei NIS și la alte sectoare și servicii de importanță critică care nu sunt acoperite printr-o legislație specifică”*.[3] În concluziile sale din 9 iunie 2020, Consiliul a salutat *„[...] planurile Comisiei de a asigura norme coerente pentru operatorii de pe piață și de a facilita un schimb de informații sigur, solid și adecvat cu privire la amenințări, precum și la incidente, inclusiv prin intermediul unei revizuiri a Directivei privind securitatea rețelelor și a sistemelor informatice (Directiva NIS), pentru a căuta opțiuni de îmbunătățire a rezilienței cibernetice și răspunsuri mai eficace la atacurile cibernetice, în special asupra unor activități economice și societale esențiale, respectând în același timp competențele statelor membre, inclusiv responsabilitatea pentru securitatea lor națională.”*[4] În plus, actul juridic propus nu aduce atingere aplicării normelor în materie de concurență prevăzute în Tratatul privind funcționarea Uniunii Europene (TFUE).

Având în vedere că o parte semnificativă a amenințărilor la adresa securității cibernetice își au originea în afara UE, este necesară o abordare coerentă a cooperării internaționale. Prezenta directivă constituie un model de referință care trebuie promovat în contextul cooperării UE cu țările terțe, în special atunci când se acordă asistență tehnică externă.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

- **Temeiul juridic**

Temeiul juridic al Directivei NIS este articolul 114 din Tratatul privind funcționarea Uniunii Europene, al cărui obiectiv este instituirea și funcționarea pieței interne prin consolidarea măsurilor de apropiere a normelor naționale. Astfel cum a statuat Curtea de Justiție a UE în hotărârea sa în cauza C 58/08 Vodafone și alții, recurgerea la articolul 114 din TFUE este justificată în cazul în care între normele naționale există diferențe care au un efect direct asupra funcționării pieței interne. De asemenea, Curtea a statuat că, atunci când un act întemeiat pe articolul 114 TFUE a eliminat deja orice obstacol privind schimburile în domeniul pe care acesta îl armonizează, legiuitorul comunitar nu poate fi privat de posibilitatea de a adapta acest act în funcție de orice modificare a împrejurărilor sau de orice evoluție a cunoștințelor având în vedere sarcina care îi revine de a garanta protecția intereselor generale recunoscute de tratat. În sfârșit, Curtea a statuat că măsurile de apropiere prevăzute la articolul 114 din TFUE sunt menite să permită, în funcție de contextul general și de împrejurările specifice ale materiei care trebuie armonizată, o marjă de apreciere cu privire la cea mai adecvată tehnică de apropiere pentru a ajunge la rezultatul dorit. Actul juridic propus ar elimina obstacolele din calea instituirii și funcționării pieței interne și ar îmbunătăți funcționarea acesteia pentru entitățile esențiale și importante prin: stabilirea unor norme clare

[2] COM(2020) 67 final.
[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_RO.html
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/ro/pdf

general aplicabile privind domeniul de aplicare al Directivei NIS, armonizarea normelor aplicabile în domeniul gestionării riscurilor în materie de securitate cibernetică și al raportării incidentelor. Disparitățile actuale în acest domeniu, atât la nivel legislativ și de supraveghere, cât și la nivel național și la nivelul UE, reprezintă obstacole în calea pieței interne, deoarece entitățile care desfășoară activități transfrontaliere se confruntă cu cerințe de reglementare și/sau de aplicare diferite și, eventual, care se suprapun, în detrimentul exercitării libertăților lor de stabilire și de prestare de servicii. Normele diferite au, de asemenea, un impact negativ asupra condițiilor de concurență de pe piața internă în ceea ce privește entitățile de același tip din diferite state membre.

- **Subsidiaritatea (în cazul competențelor neexclusive)**

Reziliența în materie de securitate cibernetică în întreaga Uniune nu poate fi eficace dacă este abordată într-un mod disparat prin fragmentări naționale sau regionale. Directiva NIS a abordat parțial această deficiență, prin stabilirea unui cadru pentru securitatea rețelelor și a sistemelor informatice la nivel național și la nivelul Uniunii. Cu toate acestea, transpunerea și punerea sa în aplicare au evidențiat, de asemenea, deficiențele inerente și limitele anumitor dispoziții sau abordări, cum ar fi delimitarea neclară a domeniului de aplicare al directivei, ceea ce duce la diferențe semnificative în ceea ce privește amploarea și profunzimea intervenției *de facto* a UE la nivelul statelor membre. În plus, de la criza provocată de pandemia de COVID-19, economia europeană a devenit mai dependentă decât oricând de rețele și de sistemele informatice, iar sectoarele și serviciile sunt din ce în ce mai interconectate. Intervenția UE, care depășește măsurile actuale prevăzute de Directiva NIS, este justificată în principal de: (i) caracterul din ce în ce mai transfrontalier al amenințărilor și al provocărilor legate de NIS; (ii) potențialul acțiunii Uniunii de îmbunătățire și de facilitare a unor politici naționale eficace și coordonate; și (iii) contribuția acțiunilor concertate și colaborative în materie de politică la protecția eficace a protecției datelor și a vieții private.

- **Proporționalitatea**

Normele propuse în prezenta directivă nu depășesc ceea ce este necesar pentru îndeplinirea obiectivelor specifice în mod satisfăcător. Alinierea și raționalizarea preconizate ale măsurilor de securitate și ale obligațiilor de raportare au legătură cu solicitările statelor membre și ale întreprinderilor de îmbunătățire a cadrului actual.

Propunerea ține seama de practicile deja existente în statele membre. Un nivel sporit de protecție obținut prin intermediul unor astfel de cerințe raționalizate și coordonate este proporțional cu riscurile existente din ce în ce mai mari, inclusiv cu cele care prezintă un element transfrontalier; aceste cerințe sunt rezonabile și corespund, în general, interesului entităților implicate în asigurarea continuității și a calității serviciilor lor. Costurile pentru asigurarea cooperării sistematice între statele membre ar fi mici în comparație cu pierderile și daunele economice și societale cauzate de incidentele de securitate cibernetică. În plus, în urma consultărilor cu părțile interesate care au avut loc în contextul revizuirii Directivei NIS, inclusiv al rezultatelor consultării publice deschise și ale sondajelor specifice, rezultă că există sprijin pentru revizuirea Directivei NIS în conformitate cu orientările menționate mai sus.

- **Alegerea instrumentului**

Propunerea va raționaliza și mai mult obligațiile impuse întreprinderilor și va asigura un nivel mai ridicat de armonizare a acestora. În același timp, propunerea urmărește să ofere statelor membre flexibilitatea necesară pentru a ține seama de particularitățile naționale (de exemplu, posibilitatea de a identifica alte entități esențiale sau importante care depășesc nivelul de

referință stabilit de actul juridic). Prin urmare, viitorul instrument juridic ar trebui să fie o directivă, întrucât acest instrument juridic permite o armonizare îmbunătățită specifică, precum și un anumit grad de flexibilitate pentru autoritățile competente.

3. REZULTATE ALE EVALUĂRILOR *EX POST*, ALE CONSULTĂRILOR PĂRȚILOR INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

- **Evaluări *ex post*/verificări ale adecvării legislației existente**

Comisia a efectuat o evaluare a funcționării Directivei NIS[5], analizând relevanța, valoarea adăugată europeană, coerența, eficacitatea și eficiența acesteia. Principalele concluzii ale acestei analize sunt:

- Domeniul de aplicare al Directivei NIS este prea limitat în ceea ce privește sectoarele acoperite, în principal din cauza: (i) intensificării digitizării din ultimii ani și a unui grad mai ridicat de interconectare, (ii) faptului că domeniul de aplicare al Directivei NIS nu mai reflectă toate sectoarele digitalizate care furnizează servicii esențiale economiei și societății în ansamblu.
- Directiva NIS nu este suficient de clară în ceea ce privește domeniul de aplicare pentru operatorii de servicii esențiale, iar dispozițiile sale nu oferă suficientă claritate în ceea ce privește competența națională asupra furnizorilor de servicii digitale. Acest lucru a condus la o situație în care anumite tipuri de entități nu au fost identificate în toate statele membre și, prin urmare, nu sunt obligate să instituie măsuri de securitate și să raporteze incidentele.
- Directiva NIS a lăsat statelor membre o marjă largă de apreciere în ceea ce privește stabilirea cerințelor de raportare în materie de securitate și de incidente pentru operatorii de servicii esențiale (denumiți în continuare „OSE”). Evaluarea arată că, în unele cazuri, statele membre au pus în aplicare aceste cerințe în moduri foarte diferite, creând astfel o sarcină suplimentară pentru întreprinderile care își desfășoară activitatea în mai multe state membre.
- Regimul de supraveghere și de aplicare al Directivei NIS este ineficace. De exemplu, statele membre au fost foarte reticente față de aplicarea de sancțiuni entităților care nu pun în aplicare cerințele de securitate sau nu raportează incidentele. Acest lucru poate avea consecințe negative asupra rezilienței cibernetice a entităților individuale.
- Resursele financiare și umane pe care statele membre le alocă pentru îndeplinirea sarcinilor care le revin (cum ar fi identificarea sau supravegherea OSE) și, prin urmare, diferitele niveluri de maturitate în abordarea riscurilor de securitate cibernetică variază foarte mult. Acest lucru agravează și mai mult diferențele dintre statele membre în ceea ce privește reziliența cibernetică.
- Statele membre nu fac schimb sistematic de informații, iar acest lucru are consecințe negative, în special asupra eficacității măsurilor de securitate cibernetică și asupra nivelului de cunoaștere comună a situației la nivelul UE. Acest lucru este valabil și pentru schimbul de informații între entitățile private și pentru angajamentul dintre structurile de cooperare de la nivelul UE și entitățile private.

[5] [Anexa 5 la evaluarea impactului]

- **Consultări cu părțile interesate**

Comisia a consultat o gamă largă de părți interesate. Statele membre și părțile interesate au fost invitate să participe la consultarea publică deschisă și la sondajele și atelierele organizate de Wavestone, CEPS și ICF, cu care Comisia a încheiat un contract pentru realizarea unui studiu în sprijinul revizuirii Directivei NIS. Printre părțile interesate consultate s-au numărat autorități competente, organisme ale Uniunii care se ocupă de securitatea cibernetică, operatori de servicii esențiale, furnizori de servicii digitale, entități care furnizează servicii care nu intră sub incidența actualei Directive NIS, asociații profesionale, organizații ale consumatorilor și cetățeni.

În plus, Comisia a fost în permanentă legătură cu autoritățile competente responsabile cu punerea în aplicare a Directivei NIS. Grupul de cooperare a acoperit în mare măsură diverse aspecte transversale și sectoriale legate de punerea în aplicare. În cele din urmă, în cursul vizitelor efectuate în 2019 și 2020 în statele membre în contextul aplicării Directivei NIS, Comisia a intervievat 154 de entități publice și private, precum și 117 autorități competente.

- **Opinii ale experților**

Comisia a contractat un consorțiu format din Wavestone, CEPS și ICF pentru a o sprijini în revizuirea Directivei NIS[6]. Contractantul nu numai că s-a adresat părților interesate direct afectate de Directiva NIS prin intermediul unor sondaje și ateliere specifice, ci s-a consultat și cu o gamă largă de experți în domeniul securității cibernetice, cum ar fi cercetătorii în domeniul securității cibernetice și profesioniștii din acest sector.

- **Evaluarea impactului**

Prezenta propunere este însoțită de o evaluare a impactului[7], care a fost prezentată Comitetului de control normativ (CAR) la 23 octombrie 2020 și care, la 20 noiembrie 2020, a primit un aviz pozitiv cu observații din partea CAR. CAR a recomandat îmbunătățiri în anumite domenii, astfel încât: (1) rolul efectelor de propagare transfrontalieră să fie mai bine reflectat în analiza problemei; (2) să se explice mai bine ce înseamnă că inițiativa se bucură de succes; (3) să se justifice în continuare lista opțiunilor de politică; (4) să se detalieze costurile măsurilor propuse. Evaluarea impactului a fost ajustată pentru a lua în calcul aceste puncte și observații mai detaliate formulate de CAR. Aceasta include acum explicații mai detaliate privind rolul efectelor de propagare transfrontalieră în domeniul securității cibernetice, o prezentare mai clară a modului în care poate fi măsurat succesul, o explicație mai detaliată a concepției și a logicii diferitelor opțiuni și acțiuni de politică luate în considerare în cadrul acestor opțiuni, o explicație mai detaliată a aspectelor analizate în legătură cu domeniul de aplicare sectorial al Directivei NIS și clarificări suplimentare cu privire la costuri.

Comisia a luat în considerare o serie de opțiuni de politică pentru îmbunătățirea cadrului juridic în domeniul rezilienței cibernetice și al răspunsului la incidente:

- „Nicio acțiune”: Directiva NIS rămâne neschimbată și nu se iau alte măsuri fără caracter legislativ pentru a aborda problemele identificate în evaluarea Directivei NIS.

---

6 Studiu în sprijinul revizuirii Directivei (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Directiva NIS) – nr. 2020-665. Wavestone, CEPS și ICF.

7 [**A se adăuga linkuri către documentul final și către fișa rezumat.**]

- Opțiunea 1: Nu au loc modificări la nivel legislativ. În schimb, Comisia emite recomandări și orientări (privind, de exemplu, identificarea operatorilor de servicii esențiale, cerințele de securitate, procedurile de notificare a incidentelor și supravegherea), după consultarea Grupului de cooperare, a Agenției UE pentru Securitate Cibernetică (ENISA) și, după caz, a rețelei echipelor de intervenție în caz de incidente de securitate informatică (CSIRT).
- Opțiunea 2: Această opțiune implică modificări specifice ale Directivei NIS, inclusiv o extindere a domeniului de aplicare și o serie de alte modificări care ar viza garantarea unor soluții imediate la problemele identificate, oferind mai multă claritate și o mai bună armonizare (cum ar fi dispozițiile de armonizare a pragurilor de identificare). Cu toate acestea, principalele elemente de bază, abordarea și justificarea Directivei NIS ar urma să rămână neschimbate.
- Opțiunea 3: Acest scenariu implică modificări sistemice și structurale ale Directivei NIS (prin adoptarea unei noi directive) care preconizează o schimbare fundamentală a abordării în ceea ce privește acoperirea unui segment mai larg al economiilor din întreaga Uniune, dar cu o supraveghere mai bine orientată, care să vizeze actori mari și esențiali. În plus, acest scenariu ar raționaliza obligațiile impuse întreprinderilor și ar asigura un nivel mai ridicat de armonizare a acestora, ar crea un cadru mai eficace pentru aspectele operaționale și ar stabili o bază clară pentru asumarea mai multor responsabilități comune și a răspunderii comune pentru diferitele părți interesate cu privire la măsurile de securitate cibernetică.

Evaluarea impactului concluzionează că opțiunea preferată este opțiunea 3 (și anume, modificări sistemice și structurale ale cadrului NIS). În ceea ce privește eficacitatea, opțiunea preferată ar determina în mod clar domeniul de aplicare al Directivei NIS, extins la o fracțiune mai reprezentativă a economiilor și a societăților din UE, precum și raționalizarea cerințelor, la care se adaugă un cadru mai bine definit de supraveghere și de asigurare a respectării legii, care ar viza îmbunătățirea nivelului de conformitate. Aceasta presupune, de asemenea, măsuri menite să îmbunătățească abordările în materie de elaborare a politicilor la nivelul statelor membre și să modifice paradigma acestora, promovând noi cadre pentru gestionarea riscurilor în relațiile cu furnizorii și comunicarea coordonată a vulnerabilităților. În același timp, opțiunea de politică preferată stabilește o bază clară pentru partajarea responsabilităților și a răspunderii și are în vedere mecanisme menite să promoveze o mai mare încredere între statele membre, atât la nivel de autorități, cât și la nivel de întreprinderi, stimulând schimbul de informații și asigurând o abordare mai operațională, cum ar fi asistența reciprocă și mecanismele de evaluare *inter pares*. Această opțiune ar oferi, de asemenea, un cadru UE de gestionare a crizelor, pornind de la rețeaua operațională a UE lansată recent, și ar asigura o mai mare implicare a ENISA, în cadrul mandatului său actual, în conturarea unei imagini de ansamblu exacte a situației securității cibernetice a Uniunii.

În ceea ce privește eficiența, deși opțiunea preferată ar presupune costuri suplimentare de asigurare a conformității și de asigurare a respectării legislației pentru întreprinderi și statele membre, aceasta ar conduce, de asemenea, la compromisuri și sinergii eficiente, cu cel mai bun potențial dintre toate opțiunile de politică analizate pentru a asigura un nivel sporit și consecvent de reziliență cibernetică a entităților-cheie din întreaga Uniune, ceea ce ar duce, în cele din urmă, la economii de costuri atât pentru întreprinderi, cât și pentru societate. Această opțiune de politică ar genera anumite sarcini administrative suplimentare și costuri de asigurare a conformității pentru autoritățile statelor membre. Totuși, în ansamblu, pe termen mediu și lung, aceasta ar aduce, de asemenea, beneficii substanțiale printr-o cooperare sporită între statele membre, inclusiv la nivel operațional, precum și prin stimularea – prin asistență reciprocă, mecanisme de evaluare *inter pares*, o mai bună imagine de ansamblu a

principalelor întreprinderi și o mai bună interacțiune cu acestea – unei creșteri globale a capacităților în materie de securitate cibernetică la nivel național și regional. Opțiunea de politică preferată ar asigura, totodată, în mare măsură coerența cu alte acte legislative, inițiative sau măsuri de politică, inclusiv cu *lex specialis* sectorială.

Modificarea gradului actual de pregătire în materie de securitate cibernetică la nivelul statelor membre și la nivelul întreprinderilor și al altor organizații ar putea duce la creșterea eficienței și la reducerea costurilor suplimentare generate de incidentele de securitate cibernetică.

- Pentru entitățile esențiale și importante, îmbunătățirea nivelului de pregătire în materie de securitate cibernetică ar putea avea ca rezultat atenuarea potențialelor pierderi de venituri cauzate de perturbări – inclusiv din cauza spionajului industrial – și ar putea reduce cheltuielile mari legate de o atenuare ad-hoc a amenințărilor. Este probabil ca aceste câștiguri să depășească costurile de investiții necesare. Reducerea fragmentării pieței interne ar contribui, de asemenea, la instituirea unor condiții de concurență mai echitabile între operatori.
- Pentru statele membre, aceasta ar însemna, de asemenea, o reducere a riscului creșterii cheltuielilor bugetare pentru atenuarea ad-hoc a amenințărilor și a costurilor suplimentare în cazul unor situații de urgență legate de incidente de securitate cibernetică.
- Pentru cetățeni, abordarea incidentelor de securitate cibernetică ar trebui să conducă la reducerea pierderii de venituri datorate perturbărilor economice.

Nivelurile crescute de securitate cibernetică în statele membre și capacitatea întreprinderilor și a autorităților de a reacționa rapid la un incident și de a atenua impactul acestuia vor conduce, cel mai probabil, la o creștere a încrederii generale a cetățenilor în economia digitală, ceea ce ar putea avea un impact pozitiv asupra creșterii economice și a investițiilor.

Creșterea nivelului general de securitate cibernetică ar putea conduce la o securitate globală sporită și la o funcționare fără întreruperi a serviciilor esențiale, care sunt critice pentru societate. Inițiativa poate avea, de asemenea, alte efecte sociale, cum ar fi reducerea nivelului criminalității informatice și al terorismului și îmbunătățirea protecției civile. Creșterea nivelului de pregătire cibernetică pentru întreprinderi și alte organizații poate preveni eventualele pierderi financiare cauzate de atacurile cibernetice și eventualele disponibilizări ale angajaților.

Creșterea nivelului general de securitate cibernetică ar putea duce, de asemenea, la prevenirea riscurilor/daunelor de mediu în cazul unui atac asupra unui serviciu esențial. Acest lucru ar putea fi valabil în special pentru sectorul energetic, sectorul aprovizionării cu apă și cel al distribuției de apă sau al transporturilor. Prin consolidarea capacităților în materie de securitate cibernetică, inițiativa ar putea duce la o mai bună utilizare a infrastructurilor și a serviciilor TIC de ultimă generație, care sunt, de altfel, mai durabile din punctul de vedere al mediului, precum și la înlocuirea infrastructurilor tradiționale ineficiente și mai puțin sigure. Se preconizează că acest lucru va contribui, de asemenea, la reducerea numărului de incidente cibernetice costisitoare, eliberând resursele disponibile pentru investiții durabile.

- **Adecvarea reglementărilor și simplificarea**

Propunerea prevede o excludere generală a microîntreprinderilor și a întreprinderilor mici din domeniul de aplicare al NIS și un regim mai puțin strict de supraveghere *ex post* aplicat unui număr mare de entități noi care intră în domeniul de aplicare revizuit (entitățile importante). Aceste măsuri vizează reducerea la minimum și echilibrarea sarcinii impuse întreprinderilor și

administrațiilor publice. În plus, propunerea înlocuiește sistemul complex de identificare pentru operatorii de servicii esențiale cu o obligație general aplicabilă și introduce un nivel mai ridicat de armonizare a obligațiilor în materie de securitate și raportare, ceea ce ar reduce sarcina de asigurare a conformității, în special pentru entitățile care furnizează servicii transfrontaliere.

Propunerea reduce la minimum costurile de conformare pentru IMM-uri, deoarece entităților li se cere să ia doar măsurile necesare pentru asigurarea unui nivel de securitate a rețelelor și a sistemelor informatice adecvat riscului prezentat.

- **Drepturile fundamentale**

UE se angajează să asigure standarde înalte de protecție a drepturilor fundamentale. Toate acordurile voluntare de schimb de informații între entități promovate de prezenta directivă ar fi încheiate în medii de încredere, cu respectarea deplină a normelor Uniunii în materie de protecție a datelor, în special a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului[8].

4. IMPLICAȚII BUGETARE

A se vedea fișa financiară

5. ALTE ELEMENTE

- **Planuri de implementare și măsuri de monitorizare, evaluare și raportare**

Propunerea include un plan general de monitorizare și evaluare a impactului asupra obiectivelor specifice, solicitând Comisiei să efectueze o revizuire la cel puțin [54 de luni] de la data intrării în vigoare și să prezinte Parlamentului European și Consiliului un raport cu principalele sale constatări.

Revizuirea urmează să se desfășoare în conformitate cu Orientările Comisiei privind o mai bună legiferare.

- **Explicație detaliată a dispozițiilor specifice ale propunerii**

Propunerea este structurată în jurul mai multor domenii de politică principale, care sunt interconectate și servesc scopului de îmbunătățire a nivelului securității cibernetice în Uniune.

Obiect și domeniu de aplicare (articolul 1 și articolul 2)

În special, directiva: (a) stabilește obligația statelor membre de a adopta o strategie națională de securitate cibernetică, de a desemna autoritățile naționale competente, punctele unice de contact și CSIRT; (b) prevede că statele membre stabilesc obligații de gestionare a riscurilor în materie de securitate cibernetică și de raportare pentru entitățile menționate ca entități esențiale în anexa I și pentru entitățile importante din anexa II; (c) prevede că statele membre stabilesc obligații privind schimbul de informații în materie de securitate cibernetică.

[8] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

Directiva se aplică anumitor entități esențiale publice sau private care își desfășoară activitatea în sectoarele enumerate în anexa I (energie, transporturi, sectorul bancar, infrastructuri ale pieței financiare, sănătate, apă potabilă, ape uzate, infrastructura digitală, administrație publică și spațiu) și anumite entități importante care își desfășoară activitatea în sectoarele enumerate în anexa II (servicii poștale și de curierat, gestionarea deșeurilor, fabricarea, producerea și distribuția de produse chimice, producția, prelucrarea și distribuția de alimente, producători și furnizori digitali). Microentitățile și entitățile mici în sensul Recomandării 2003/361/CE a Comisiei din 6 mai 2003 sunt excluse din domeniul de aplicare al directivei, cu excepția furnizorilor de rețele de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, a furnizorilor de servicii de încredere, a registrelor de nume de domenii de prim nivel (*Top-level domain name* – TLD) și a administrației publice, precum și a anumitor alte entități, cum ar fi furnizorul unic al unui serviciu într-un stat membru.

Cadrele naționale de securitate cibernetică (articolele 5-11)

Statele membre au obligația de a adopta o strategie națională în materie de securitate cibernetică care să definească obiectivele strategice și măsurile de politică și de reglementare adecvate în vederea atingerii și menținerii unui nivel ridicat de securitate cibernetică.

Directiva stabilește, de asemenea, un cadru pentru comunicarea coordonată a vulnerabilităților și solicită statelor membre să desemneze CSIRT care să acționeze ca intermediari de încredere și să faciliteze interacțiunea dintre entitățile raportoare și producătorii sau furnizorii de produse și de servicii TIC. ENISA are obligația de a institui și de a menține un registru european al vulnerabilităților pentru vulnerabilitățile descoperite.

Statele membre au obligația de a institui cadre naționale de gestionare a crizelor în materie de securitate cibernetică, printre altele prin desemnarea autorităților naționale competente responsabile cu gestionarea incidentelor și a crizelor de securitate cibernetică de mare amploare.

De asemenea, statele membre au obligația de a desemna una sau mai multe autorități naționale competente în materie de securitate cibernetică pentru sarcinile de supraveghere prevăzute în prezenta directivă și un punct unic național de contact în materie de securitate cibernetică (*single point of contact on cybersecurity* – SPOC) care să exercite o funcție de legătură pentru a asigura cooperarea transfrontalieră a autorităților statelor membre. Statele membre au, de asemenea, obligația de a desemna CSIRT.

Cooperare (articolele 12-16)

Directiva creează un grup de cooperare pentru a sprijini și facilita cooperarea strategică și schimbul de informații între statele membre și pentru a dezvolta încrederea. Directiva instituie, de asemenea, o rețea CSIRT pentru a contribui la dezvoltarea încrederii între statele membre și pentru a promova cooperarea operațională rapidă și eficace.

Se instituie o rețea europeană a Organizației de legătură în caz de crize cibernetice (EU-CyCLONe) care va sprijini gestionarea coordonată a incidentelor și a crizelor de securitate cibernetică de mare amploare și va asigura schimbul periodic de informații între statele membre și instituțiile UE.

ENISA trebuie să elaboreze, în cooperare cu Comisia, un raport bienal privind situația securității cibernetice în Uniune.

Comisia trebuie să instituie un sistem de evaluare *inter pares* care să permită evaluări *inter pares* periodice ale eficacității politicilor de securitate cibernetică ale statelor membre.

Gestionarea riscurilor în materie de securitate cibernetică și obligațiile de raportare (articolele 17-23)

Directiva impune statelor membre să prevadă ca organismele de conducere ale tuturor entităților care intră în domeniul său de aplicare să aprobe măsurile de gestionare a riscurilor în materie de securitate cibernetică luate de entitățile respective și să urmeze cursuri de formare specifice legate de securitatea cibernetică.

Statele membre trebuie să se asigure că entitățile care intră în domeniul de aplicare al directivei iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile în materie de securitate cibernetică la adresa securității rețelelor și a sistemelor informatice. De asemenea, acestea au obligația de a se asigura că entitățile notifică autorităților naționale competente sau CSIRT orice incident de securitate cibernetică care are un impact semnificativ asupra furnizării serviciului pe care îl furnizează.

Registrele TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD colectează și mențin date exacte și complete de înregistrare a numelor de domenii. În plus, astfel de entități sunt obligate să le ofere solicitanților legitimi de acces un acces eficient la datele de înregistrare a domeniilor.

Competență și înregistrare (articolele 24 și 25)

Ca regulă generală, entitățile esențiale și importante sunt considerate ca fiind sub jurisdicția statului membru în care își prestează serviciile. Cu toate acestea, se consideră că anumite tipuri de entități (furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date și furnizorii de rețele de distribuție de conținut, precum și anumiți furnizori digitali) se află sub jurisdicția statului membru în care își au sediul principal din Uniune. Scopul este de a se asigura că astfel de entități nu se confruntă cu o multitudine de cerințe juridice diferite, deoarece serviciile pe care le furnizează sunt, într-o foarte mare măsură, transfrontaliere. ENISA are obligația de a crea și de a menține un registru al entităților de acest tip.

Schimbul de informații (articolele 26 și 27)

Statele membre prevăd norme care le permit entităților să se implice în schimbul de informații privind securitatea cibernetică în cadrul unor acorduri specifice privind schimbul de informații în materie de securitate cibernetică, în conformitate cu articolul 101 din TFUE. În plus, statele membre le permit entităților care nu intră în domeniul de aplicare al prezentei directive să raporteze, în mod voluntar, incidentele semnificative, amenințările cibernetice sau incidentele evitate la limită.

Supraveghere și punere în aplicare (articolele 28-34)

Autoritățile competente au obligația de a supraveghea entitățile care intră în domeniul de aplicare al directivei și, în special, de a asigura că acestea respectă cerințele de securitate și de notificare a incidentelor. Directiva face distincția între un regim de supraveghere *ex ante* pentru entitățile esențiale și un regim de supraveghere *ex post* pentru entitățile importante, acestea din urmă solicitând autorităților competente să ia măsuri atunci când li se furnizează

dovezi sau indicii că o entitate importantă nu îndeplinește cerințele de securitate și de notificare a incidentelor.

Directiva prevede, de asemenea, că statele membre trebuie să impună amenzi administrative entităților esențiale și importante și definește anumite plafoane pentru amenzi.

Statele membre au obligația de a coopera și de a-și acorda asistență reciprocă, după caz, atunci când entitățile furnizează servicii în mai multe state membre sau când sediul principal al unei entități ori reprezentantul său se află într-un anumit stat membru, dar rețeaua și sistemele sale informatice sunt situate în unul sau mai multe alte state membre.

2020/0359 (COD)

Propunere de

DIRECTIVĂ A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ parlamentelor naționale,

având în vedere avizul Comitetului Economic și Social European[9],

având în vedere avizul Comitetului Regiunilor[10],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului[11] vizează consolidarea capacităților în materie de securitate cibernetică în întreaga Uniune, atenuarea amenințărilor la adresa rețelelor și a sistemelor informatice utilizate pentru a furniza servicii esențiale în sectoare-cheie și asigurarea continuității acestor servicii atunci când se confruntă cu incidente de securitate cibernetică, contribuind astfel la funcționarea eficace a economiei și a societății Uniunii.

(2) De la intrarea în vigoare a Directivei (UE) 2016/1148, s-au înregistrat progrese semnificative în ceea ce privește creșterea nivelului de reziliență a securității cibernetice în Uniune. Revizuirea directivei respective a arătat că aceasta a servit drept catalizator pentru abordarea instituțională și de reglementare a securității cibernetice în Uniune, deschizând calea pentru o schimbare semnificativă de mentalitate. Această directivă a asigurat finalizarea cadrelor naționale prin definirea strategiilor naționale de securitate cibernetică, prin stabilirea de capacități naționale și prin punerea în aplicare a măsurilor de reglementare care vizează infrastructurile esențiale și actorii identificați de fiecare stat membru. De asemenea, a contribuit la cooperarea la nivelul Uniunii prin instituirea Grupului de cooperare[12] și a unei rețele de echipe naționale de intervenție în caz de incidente de securitate informatică („rețeaua CSIRT”)[13]. În pofida

[9] JO C , , p. .

[10] JO C , , p. .

[11] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194/1, 19.7.2016, p. 1).

[12] Articolul 11 din Directiva (UE) 2016/1148.

[13] Articolul 12 din Directiva (UE) 2016/1148.

acestor realizări, revizuirea Directivei (UE) 2016/1148 a evidențiat deficiențe inerente care o împiedică să abordeze în mod eficace provocările contemporane și emergente în materie de securitate cibernetică.

(3) Rețelele și sistemele informatice reprezintă acum o componentă centrală a vieții de zi cu zi, odată cu transformarea digitală rapidă și interconectarea societății, inclusiv în cadrul schimburilor transfrontaliere. Această transformare a condus la o extindere a situației amenințărilor la adresa securității cibernetice, generând noi provocări, care necesită răspunsuri adaptate, coordonate și inovatoare în toate statele membre. Incidentele de securitate sunt tot mai numeroase, mai ample, mai sofisticate și cu un impact tot mai mare, acestea reprezentând o amenințare gravă la adresa funcționării rețelelor și a sistemelor informatice. Prin urmare, incidentele cibernetice pot să împiedice desfășurarea activităților economice pe piața internă, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei și societății Uniunii. Prin urmare, pregătirea și eficacitatea în materie de securitate cibernetică sunt acum mai importante ca niciodată pentru buna funcționare a pieței interne.

(4) Temeiul juridic al Directivei (UE) 1148/2016 este articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), al cărui obiectiv este instituirea și funcționarea pieței interne prin consolidarea măsurilor de apropiere a normelor naționale. Cerințele de securitate cibernetică impuse entităților care furnizează servicii sau activități relevante din punct de vedere economic variază considerabil de la un stat membru la altul în ceea ce privește tipul de cerință, nivelul lor de detaliere și metoda de supraveghere. Aceste disparități implică costuri suplimentare și creează dificultăți pentru întreprinderile care oferă bunuri sau servicii la nivel transfrontalier. Cerințele impuse de un stat membru care sunt diferite sau chiar în conflict cu cele impuse de un alt stat membru pot afecta în mod substanțial activitățile transfrontaliere respective. În plus, conceperea unor standarde de securitate cibernetică sub nivelul optim sau punerea în aplicare sub nivel optim a standardelor de securitate cibernetică într-un stat membru pot avea repercusiuni asupra nivelului de securitate cibernetică al altor state membre, în special în contextul schimburilor transfrontaliere intense. Revizuirea Directivei (UE) 2016/1148 a arătat că punerea sa în aplicare diferă foarte mult de la un stat membru la altul, inclusiv în ceea ce privește domeniul său de aplicare, a cărui delimitare a fost lăsată în mare măsură la latitudinea statelor membre. Directiva (UE) 2016/1148 a acordat, de asemenea, statelor membre o marjă de apreciere foarte largă în ceea ce privește punerea în aplicare a obligațiilor de raportare în materie de securitate și de raportare a incidentelor pe care le prevede aceasta. Prin urmare, aceste obligații au fost puse în aplicare în moduri foarte diferite la nivel național. Divergențe similare în ceea ce privește punerea în aplicare s-au înregistrat și în ceea ce privește dispozițiile directivei respective privind supravegherea și asigurarea respectării legislației.

(5) Toate aceste divergențe implică o fragmentare a pieței interne și pot avea un efect negativ asupra funcționării acesteia, afectând în special furnizarea transfrontalieră de servicii și nivelul de reziliență în materie de securitate cibernetică din cauza aplicării unor standarde diferite. Prezenta directivă urmărește să elimine divergențele importante dintre statele membre, în special prin stabilirea unor norme minime privind funcționarea unui cadru de reglementare coordonat, prin stabilirea unor mecanisme pentru cooperarea eficace între autoritățile responsabile din fiecare stat membru, prin actualizarea listei sectoarelor și a activităților care fac obiectul obligațiilor în materie de securitate cibernetică și prin instituirea unor căi de atac și sancțiuni eficace care

sunt esențiale pentru asigurarea eficace a respectării acestor obligații. Directiva (UE) 2016/1148 trebuie, prin urmare, abrogată și înlocuită cu prezenta directivă.

(6) Prezenta directivă nu aduce atingere posibilității de care dispun statele membre 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 legislația Uniunii. În conformitate cu articolul 346 din TFUE, niciun stat membru nu are obligația de a furniza informații a căror divulgare ar fi contrară intereselor esențiale ale siguranței sale publice. În acest context, sunt relevante normele naționale și cele ale Uniunii privind protecția informațiilor clasificate și acordurile de nedivulgare sau acordurile de nedivulgare informale, precum „Traffic Light Protocol”[14].

(7) Odată cu abrogarea Directivei (UE) 2016/1148, domeniul de aplicare ar trebui extins la mai multe sectoare economice, având în vedere considerentele 4-6. Sectoarele reglementate de Directiva (UE) 2016/1148 ar trebui, prin urmare, să fie extinse pentru a oferi o acoperire cuprinzătoare a sectoarelor și a serviciilor de importanță vitală pentru activitățile societale și economice esențiale din cadrul pieței interne. Normele nu ar trebui să fie diferite în funcție de statutul entităților: operatori de servicii esențiale sau furnizori de servicii digitale. Această diferențiere s-a dovedit a fi caducă, deoarece nu reflectă importanța reală a sectoarelor sau a serviciilor pentru activitățile sociale și economice de pe piața internă.

(8) În conformitate cu Directiva (UE) 2016/1148, statele membre au fost responsabile de stabilirea entităților care îndeplinesc criteriile pentru a fi considerate operatori de servicii esențiale („procesul de identificare”). Pentru a elimina divergențele mari dintre statele membre în această privință și pentru a asigura securitatea juridică în ceea ce privește cerințele de gestionare a riscurilor și obligațiile de raportare pentru toate entitățile relevante, ar trebui stabilit un criteriu uniform care să stabilească care sunt entitățile ce intră în domeniul de aplicare al prezentei directive. Acest criteriu ar trebui să constea în aplicarea regulii privind criteriul de dimensiune, conform căruia toate întreprinderile mijlocii și mari, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei[15], care își desfășoară activitatea în sectoarele reglementate de prezenta directivă sau furnizează tipul de servicii reglementate de aceasta intră în domeniul său de aplicare. Statele membre nu ar trebui să aibă obligația de a întocmi o listă a entităților care îndeplinesc acest criteriu general aplicabil în ceea ce privește dimensiunea.

(9) Cu toate acestea, entitățile mici sau microentitățile care îndeplinesc anumite criterii ce indică un rol-cheie pentru economiile sau societățile statelor membre sau pentru anumite sectoare sau tipuri de servicii ar trebui să intre, de asemenea, sub incidența prezentei directive. Statele membre ar trebui să fie responsabile de stabilirea unei liste a acestor entități și să o transmită Comisiei.

(10) Comisia, în cooperare cu Grupul de cooperare, poate emite orientări privind punerea în aplicare a criteriilor aplicabile microîntreprinderilor și întreprinderilor mici.

---

[14] Traffic Light Protocol (TLP) este un mijloc prin care cineva care face schimb de informații își informează publicul cu privire la eventualele limitări în răspândirea în continuare a acestor informații. Acest instrument este utilizat în aproape toate comunitățile CSIRT și în unele centre de schimb de informații și de analiză (ISAC).

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

(11) În funcție de sectorul în care își desfășoară activitatea sau de tipul de serviciu pe care îl furnizează, entitățile care intră în domeniul de aplicare al prezentei directive ar trebui clasificate în două categorii: esențiale și importante. Această clasificare ar trebui să țină seama de nivelul critic al sectorului sau al tipului de serviciu, precum și de nivelul de dependență al altor sectoare sau tipuri de servicii. Entitățile esențiale și cele importante ar trebui să fie supuse acelorași cerințe de gestionare a riscurilor și acelorași obligații de raportare. Regimurile de supraveghere și de sancționare corespunzătoare acestor două categorii de entități ar trebui diferențiate pentru a asigura un echilibru corect între cerințe și obligații, pe de o parte, și sarcina administrativă care decurge din supravegherea conformității, pe de altă parte.

(12) Legislația și instrumentele sectoriale pot contribui la asigurarea unor niveluri ridicate de securitate cibernetică, ținând seama pe deplin de particularitățile și de complexitatea acestor sectoare. În cazul în care un act juridic sectorial al Uniunii impune entităților esențiale sau importante să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică sau să notifice incidente ori amenințări cibernetice semnificative cu un efect cel puțin echivalent cu obligațiile prevăzute în prezenta directivă, ar trebui să se aplice dispozițiile sectoriale respective, inclusiv cele privind supravegherea și asigurarea respectării normelor. Comisia poate emite orientări cu privire la punerea în aplicare a *lex specialis*. Prezenta directivă nu împiedică adoptarea unor acte sectoriale suplimentare ale Uniunii care să abordeze măsurile de gestionare a riscurilor în materie de securitate cibernetică și notificările incidentelor. Aceasta nu aduce atingere competențelor de executare existente care i-au fost conferite Comisiei într-o serie de sectoare, inclusiv în domeniul transporturilor și în cel al energiei.

(13) În ceea ce privește entitățile din sectorul financiar, Regulamentul XXXX/XXXX al Parlamentului European și al Consiliului[16] ar trebui considerat un act juridic sectorial al Uniunii în legătură cu prezenta directivă. Dispozițiile Regulamentului XXXX/XXXX referitoare la măsurile de gestionare a riscurilor legate de tehnologia informației și comunicațiilor (TIC), la gestionarea incidentelor legate de TIC și, în special, la raportarea incidentelor, precum și cele referitoare la testarea rezilienței operaționale digitale, la acordurile privind schimbul de informații și la riscul asociat furnizorilor terți de servicii TIC ar trebui să se aplice în locul celor instituite în temeiul prezentei directive. Prin urmare, în cazul entităților financiare care intră sub incidența Regulamentului XXXX/XXXX, statele membre nu ar trebui să aplice dispozițiile prezentei directive privind obligațiile de gestionare și raportare a riscurilor în materie de securitate cibernetică, schimbul de informații, supravegherea și asigurarea respectării normelor. În același timp, este important ca, în temeiul prezentei directive, să se mențină o relație puternică cu sectorul financiar și să se facă un schimb de informații cu acesta. Astfel, în temeiul Regulamentului XXXX/XXXX, toate autoritățile de supraveghere financiară, autoritățile europene de supraveghere (AES) pentru sectorul financiar și autoritățile naționale competente în temeiul Regulamentului XXXX/XXXX pot participa la discuții strategice privind politicile și activitățile tehnice ale Grupului de cooperare, pot face schimb de informații și pot coopera cu punctele unice de contact desemnate în temeiul prezentei directive și cu CSIRT naționale. Autoritățile competente în temeiul Regulamentului XXXX/XXXX ar trebui să transmită detaliile incidentelor majore legate de TIC și punctelor unice de contact desemnate în temeiul prezentei directive. În plus, statele membre ar trebui să

[16] *[a se introduce titlul complet și referința de publicare în JO, atunci când acestea sunt cunoscute]*

includă în continuare sectorul financiar în strategiile lor de securitate cibernetică, iar CSIRT naționale pot acoperi sectorul financiar în activitățile lor.

(14) Având în vedere interconexiunile dintre securitatea cibernetică și securitatea fizică a entităților, ar trebui să se asigure o abordare coerentă între Directiva (UE) XXX/XXX a Parlamentului European și a Consiliului[17] și prezenta directivă. În acest scop, statele membre ar trebui să se asigure că, în temeiul Directivei (UE) XXX/XXX, entitățile critice și entitățile echivalente sunt considerate entități esențiale în temeiul prezentei directive. Statele membre ar trebui, de asemenea, să se asigure că strategiile lor în materie de securitate cibernetică oferă un cadru de politică pentru o coordonare consolidată între autoritatea competentă în temeiul prezentei directive și cea competentă în temeiul Directivei (UE) XXX/XXX în contextul schimbului de informații privind incidentele și amenințările cibernetice și al exercitării sarcinilor de supraveghere. Autoritățile competente în temeiul acestor două directive ar trebui să coopereze și să facă schimb de informații, în special în ceea ce privește identificarea entităților critice, amenințările cibernetice, riscurile de securitate cibernetică, incidentele care afectează entitățile critice, precum și cu privire la măsurile de securitate cibernetică adoptate de entitățile critice. La cererea autorităților competente în temeiul Directivei (UE) XXX/XXX, autorităților competente în temeiul prezentei directive ar trebui să li se permită să își exercite competențele de supraveghere și de asigurare a respectării legislației cu privire la o entitate esențială identificată ca fiind critică. Cele două tipuri de autorități ar trebui să coopereze și să facă schimb de informații în acest scop.

(15) Respectarea și menținerea unui sistem fiabil, rezilient și sigur de nume de domenii (DNS) este un factor-cheie pentru menținerea integrității internetului, esențial pentru funcționarea sa continuă și stabilă, de care depind economia digitală și societatea. Prin urmare, prezenta directivă ar trebui să se aplice tuturor furnizorilor de servicii DNS de-a lungul lanțului de rezoluție a DNS, inclusiv operatorilor de servere pentru numele primare, de servere cu nume de domeniu de prim nivel (TLD), de servere cu nume de utilizator autorizat pentru nume de domenii și de rezolvere recursive.

(16) Serviciile de cloud computing ar trebui să acopere serviciile care permit, la cerere, accesul larg de la distanță la un bazin elastic și redimensionabil de resurse informatice care pot fi puse în comun și distribuite. Noțiunea de „resurse informatice” include resurse precum rețelele, serverele sau alte infrastructuri, sistemele de operare, software-urile, stocarea, aplicațiile și serviciile. Modelele de implementare a cloud computingului ar trebui să includă tehnologiile de tip cloud private, comunitare, publice și hibride. Modelele de servicii și de implementare menționate anterior au același înțeles ca și termenii modelelor de servicii și de implementare definiți în standardul ISO/IEC 17788:2014. Capacitatea utilizatorului de cloud computing de a furniza în mod unilateral capacități de calcul autonome, cum ar fi ora serverului sau stocarea în rețea, fără nicio interacțiune umană din partea furnizorului de servicii de cloud computing, ar putea fi descrisă ca administrare la cerere. Termenul „acces larg la distanță” este utilizat pentru a descrie faptul că aceste capacități de cloud sunt furnizate prin rețea și accesate prin mecanisme care promovează utilizarea unor platforme eterogene, subțiri sau groase pentru clienți (inclusiv telefoane mobile, tablete, laptopuri, stații de lucru). Termenul „redimensionabil” se referă la resursele informatice care se alocă flexibil de către furnizorul de servicii cloud, indiferent de

[17] *[a se introduce titlul complet și referința de publicare în JO, atunci când acestea sunt cunoscute]*

poziția geografică a resurselor, pentru a administra fluctuațiile de cerere. Termenul „bazin elastic” se referă la acele resurse informatice care sunt atribuite și transferate în funcție de cerere, pentru a înmulți și a reduce rapid resursele disponibile în conformitate cu volumul 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. Termenul „distribuit” se referă la acele resurse informatice care sunt situate pe diferite calculatoare sau dispozitive în rețea și care comunică și se coordonează între ele prin transmiterea de mesaje.

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

(18) Este posibil ca serviciile oferite de furnizorii de servicii de centre de date să nu fie întotdeauna furnizate sub formă de servicii de cloud computing. În consecință, este posibil ca centrele de date să nu constituie întotdeauna o parte a infrastructurii de cloud computing. Pentru a gestiona toate riscurile la adresa securității rețelelor și a sistemelor informatice, prezenta directivă ar trebui să vizeze și furnizorii de astfel de servicii de centre de date care nu sunt servicii de cloud computing. În sensul prezentei directive, termenul „serviciu de centru de date” ar trebui să includă furnizarea unui serviciu care cuprinde structuri sau grupuri de structuri dedicate instalării centralizate, interconectării și funcționării tehnologiei informației și a echipamentelor de rețea care furnizează servicii de stocare, prelucrare și transport de date, împreună cu toate instalațiile și infrastructurile de distribuție a energiei electrice și de control al mediului. Termenul „serviciu de centre de date” nu se aplică centrelor de date interne, corporative deținute și operate în scopuri proprii entității în cauză.

(19) Furnizorii de servicii poștale în sensul Directivei 97/67/CE a Parlamentului European și a Consiliului[18], precum și furnizorii de servicii de curierat și curierat rapid ar trebui să facă obiectul prezentei directive în cazul în care asigură cel puțin una dintre etapele lanțului de distribuție poștală, în special ridicarea, sortarea sau distribuția, inclusiv serviciile de preluare. Serviciile de transport care nu sunt efectuate împreună cu una dintre aceste etape nu ar trebui să intre în domeniul de aplicare al serviciilor poștale.

(20) Aceste interdependențe din ce în ce mai mari sunt rezultatul unei rețele din ce în ce mai transfrontaliere și interdependente de furnizare de servicii care utilizează infrastructuri-cheie din întreaga Uniune în sectoare precum energia, transporturile, infrastructura digitală, apa potabilă și apele uzate, sănătatea, anumite aspecte ale administrației publice, precum și spațiul, în măsura în care furnizarea anumitor servicii în funcție de infrastructurile terestre care sunt deținute, gestionate și exploatate fie de statele membre, fie de părți private, nu acoperă, prin urmare, infrastructurile deținute, gestionate sau exploatate de Uniune sau în numele acesteia, ca parte a programelor sale spațiale. Aceste interdependențe înseamnă că orice perturbare, chiar dacă inițial este limitată la o singură entitate sau la un singur sector, poate avea efecte în cascadă

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

în sens mai larg, ceea ce ar putea avea efecte negative de amploare și de lungă durată asupra furnizării de servicii pe piața internă. Pandemia de COVID-19 a demonstrat vulnerabilitatea societăților noastre, care sunt din ce în ce mai interdependente în fața riscurilor cu probabilitate redusă de producere.

(21) 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, 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 entităților importante în temeiul prezentei directive. Statele membre ar trebui să fie capabile să atribuie acest rol unei autorități existente.

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

(23) Autoritățile competente sau CSIRT-urile ar trebui să primească de la entități notificări ale incidentelor într-un mod eficace și eficient. Punctele unice de contact ar trebui să aibă sarcina de a transmite notificările incidentelor către punctele unice de contact ale altor state membre afectate. La nivelul autorităților statelor membre, pentru a asigura un punct de intrare unic în fiecare stat membru, punctele unice de contact ar trebui să fie, de asemenea, destinatarii informațiilor relevante privind incidentele referitoare la entități din sectorul financiar, furnizate de autoritățile competente în temeiul Regulamentului XXXX/XXXX, pe care ar trebui să le poată transmite, după caz, autorităților naționale competente relevante sau CSIRT în temeiul prezentei directive.

(24) 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. În vederea consolidării relației de încredere dintre entități și CSIRT, în cazurile în care o echipă CSIRT face parte din autoritatea competentă, statele membre ar trebui să aibă în vedere separarea funcțională între sarcinile operaționale furnizate de CSIRT, în special în ceea ce privește schimbul de informații și sprijinul acordat entităților, și activitățile de supraveghere ale autorităților competente.

(25) În ceea ce privește datele cu caracter personal, CSIRT ar trebui să poată furniza, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[19], în ceea ce privește datele cu caracter personal, în numele și la cererea unei entități în temeiul prezentei directive, o scanare proactivă a rețelei și a sistemelor informatice utilizate pentru furnizarea serviciilor lor. Statele membre ar trebui să

[19] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

vizeze asigurarea unui nivel egal al capacităților tehnice pentru toate CSIRT-urile sectoriale. Statele membre pot solicita asistența Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) la dezvoltarea echipelor CSIRT naționale.

(26) 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.

(27) În conformitate cu anexa la Recomandarea (UE) 2017/1584 a Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare („Blueprint”)[20], un incident de mare anvergură ar trebui să însemne un incident cu un impact semnificativ asupra a cel puțin două state membre sau care provoacă o perturbare ce depășește capacitatea unui stat membru de a reacționa la acesta. În funcție de cauza și de impactul lor, incidentele de mare amploare pot escalada și se pot transforma în crize de sine stătătoare, care să împiedice buna funcționare a pieței interne. Având în vedere domeniul larg de aplicare și, în cele mai multe cazuri, natura transfrontalieră a unor astfel de incidente, statele membre și instituțiile, organele și agențiile relevante ale Uniunii ar trebui să coopereze la nivel tehnic, operațional și politic pentru a coordona în mod corespunzător răspunsul în întreaga Uniune.

(28) Întrucât exploatarea vulnerabilităților din cadrul rețelelor și al sistemelor informatice poate provoca perturbări și prejudicii semnificative, identificarea și remedierea rapidă a acestor vulnerabilități reprezintă un factor important în reducerea riscului de securitate cibernetică. Entitățile care dezvoltă astfel de sisteme ar trebui, prin urmare, să stabilească proceduri adecvate de gestionare a vulnerabilităților atunci când acestea sunt descoperite. Întrucât vulnerabilitățile sunt adesea descoperite și raportate (divulgate) de părți terțe (entități raportoare), producătorul ori furnizorul de produse sau servicii TIC ar trebui, de asemenea, să instituie procedurile necesare pentru a primi de la terți informații privind vulnerabilitatea. În acest sens, standardele internaționale ISO/IEC 30111 și ISO/IEC 29417 oferă orientări privind gestionarea vulnerabilităților și, respectiv, divulgarea vulnerabilităților. În ceea ce privește divulgarea vulnerabilităților, coordonarea dintre entitățile raportoare și producătorii ori furnizorii de produse sau servicii TIC este deosebit de importantă. Divulgarea coordonată a vulnerabilităților presupune un proces structurat prin care vulnerabilitățile sunt raportate organizațiilor într-un mod care să permită organizației să diagnosticheze și să remedieze vulnerabilitățile înainte ca informațiile detaliate privind vulnerabilitățile să fie divulgate terților sau publicului. Divulgarea coordonată a vulnerabilităților ar trebui să includă, de asemenea, coordonarea dintre entitatea raportoare și organizație în ceea ce privește calendarul de remediere și publicare a vulnerabilităților.

(29) Prin urmare, statele membre ar trebui să ia măsuri pentru a facilita divulgarea coordonată a vulnerabilităților prin stabilirea unei politici naționale relevante. În acest sens, statele membre ar trebui să desemneze o echipă CSIRT care să preia rolul de „coordonator”, acționând ca intermediar între entitățile raportoare și producătorii ori furnizorii de produse sau servicii TIC, dacă este necesar. Sarcinile coordonatorului CSIRT ar trebui să includă, în special, identificarea și contactarea entităților vizate, sprijinirea entităților raportoare, negocierea calendarelor de divulgare și gestionarea vulnerabilităților care afectează mai multe organizații (divulgarea vulnerabilităților mai multor părți). Atunci când vulnerabilitățile afectează mai mulți producători ori

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

furnizori de produse sau servicii TIC stabiliți în mai multe state membre, CSIRT desemnate din fiecare dintre statele membre afectate ar trebui să coopereze în cadrul rețelei CSIRT.

(30) Accesul la informații corecte și în timp util cu privire la vulnerabilitățile care afectează produsele și serviciile TIC contribuie la o mai bună gestionare a riscurilor în materie de securitate cibernetică. În această privință, sursele de informații accesibile publicului cu privire la vulnerabilități reprezintă un instrument important atât pentru entități și utilizatorii acestora, cât și pentru autoritățile naționale competente și CSIRT. Din acest motiv, ENISA ar trebui să creeze un registru al vulnerabilităților în care entitățile esențiale și importante și furnizorii acestora, precum și entitățile care nu intră în domeniul de aplicare al prezentei directive pot, în mod voluntar, să divulge vulnerabilitățile și să furnizeze informații privind vulnerabilitățile, astfel încât utilizatorii să ia măsuri de atenuare adecvate.

(31) Deși există registre ale vulnerabilităților sau baze de date similare, acestea sunt găzduite și întreținute de entități care nu sunt stabilite în Uniune. Un registru european al vulnerabilităților gestionat de ENISA ar oferi o mai mare transparență în ceea ce privește procesul de publicare înainte de dezvăluirea oficială a vulnerabilității, precum și reziliența în caz de perturbări sau întreruperi ale furnizării de servicii similare. Pentru a evita dublarea eforturilor și pentru a căuta complementaritatea în măsura posibilului, ENISA ar trebui să analizeze posibilitatea de a încheia acorduri de cooperare structurată cu registre similare în jurisdicții din țări terțe.

(32) Grupul de cooperare ar trebui să stabilească, o dată la doi ani, un program de lucru care să includă acțiunile ce urmează să fie întreprinse de grup în vederea punerii în aplicare a obiectivelor și sarcinilor sale. Calendarul primului program adoptat în temeiul prezentei directive ar trebui să fie aliniat la calendarul ultimului program adoptat în temeiul Directivei (UE) 2016/1148, pentru a se evita eventualele perturbări ale activității grupului.

(33) Atunci când elaborează documente de orientare, Grupul de cooperare ar trebui ca, în mod consecvent, să identifice soluțiile și experiențele naționale, să evalueze impactul rezultatelor Grupului de cooperare asupra abordărilor naționale, să discute provocările legate de punerea în aplicare și să formuleze recomandări specifice care să fie abordate printr-o mai bună punere în aplicare a normelor existente.

(34) Grupul de cooperare ar trebui să rămână un forum flexibil, care să poată reacționa la prioritățile și provocările noi și în schimbare în materie de politici, ținând seama, în același timp, de disponibilitatea resurselor. Acesta ar trebui să organizeze reuniuni comune periodice cu părțile interesate relevante din sectorul privat din întreaga Uniune pentru a discuta activitățile pe care le desfășoară grupul și pentru a colecta informații cu privire la provocările emergente în materie de politici. Pentru a consolida cooperarea la nivelul Uniunii, grupul ar trebui să invite să participe la lucrările sale organismele și agențiile Uniunii implicate în politica de securitate cibernetică, cum ar fi Centrul european de combatere a criminalității informatice (EC3), Agenția Uniunii Europene pentru Siguranța Aviației (AESA) și Agenția Uniunii Europene pentru Programul spațial (EUSPA).

(35) Autoritățile competente și CSIRT ar trebui să aibă posibilitatea să participe la programe de schimb pentru funcționari din alte state membre în vederea îmbunătățirii cooperării. Autoritățile competente ar trebui să ia măsurile necesare ca funcționari din alte state membre să poată juca un rol efectiv în activitățile autorității competente gazdă.

(36) Dacă este posibil, Uniunea ar trebui să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaționale cu țări terțe sau organizații internaționale, care să permită și să organizeze participarea acestora la anumite activități ale Grupului de cooperare și ale rețelei CSIRT. Astfel de acorduri ar trebui să asigure o protecție adecvată a datelor.

(37) Statele membre ar trebui să contribuie la instituirea cadrului UE de răspuns la crizele de securitate cibernetică prevăzut în Recomandarea (UE) 2017/1584 prin intermediul rețelelor de cooperare existente, în special prin rețeaua Organizației de legătură în caz de criză cibernetică (EU-CyCLONe), rețeaua CSIRT și Grupul de cooperare. EU-CyCLONe și rețeaua CSIRT ar trebui să coopereze pe baza modalităților procedurale care definesc modalitățile acestei cooperări. Regulamentul de procedură al EU-CyCLONe ar trebui să precizeze în detaliu modalitățile prin care ar trebui să funcționeze rețeaua, inclusiv, dar fără a se limita la acestea, rolurile, modurile de cooperare, interacțiunile cu alți actori relevanți și modelele pentru schimbul de informații, precum și mijloacele de comunicare. Pentru gestionarea crizelor la nivelul Uniunii, părțile relevante ar trebui să se bazeze pe mecanismul integrat pentru un răspuns politic la crize (IPCR). În acest scop, Comisia ar trebui să utilizeze procesul ARGUS de coordonare transsectorială la nivel înalt în situații de criză. În cazul în care criza are o importantă dimensiune externă sau de politică de securitate și apărare comună (PSAC), ar trebui activat mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă (SEAE).

(38) În sensul prezentei directive, termenul „risc” ar trebui să se refere la potențialele pierderi sau perturbări cauzate de un incident de securitate cibernetică și ar trebui exprimat ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului respectiv.

(39) În sensul prezentei directive, termenul „incident evitat la limită” ar trebui să se refere la un eveniment care ar fi putut cauza prejudicii, dar care a cărui desfășurare până la capăt a fost împiedicată cu succes.

(40) Măsurile de gestionare a riscurilor ar trebui să includă 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 ar trebui să cuprindă securitatea datelor stocate, transmise și prelucrate.

(41) Pentru a se evita impunerea unei sarcini financiare și administrative disproporționate asupra entităților esențiale și importante, cerințele de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri.

(42) Entitățile esențiale și importante ar trebui să asigure securitatea rețelelor și a sistemelor informatice pe care le utilizează pentru a-și desfășura activitatea. Acestea sunt în principal rețele și sisteme informatice private, gestionarea securității lor fiind efectuată de către personalul IT intern sau externalizată. Cerințele de raportare și de gestionare a riscurilor în materie de securitate cibernetică în temeiul prezentei directive ar trebui să se aplice entităților esențiale și importante relevante, indiferent dacă acestea efectuează la nivel intern întreținerea rețelelor și a sistemelor lor informatice sau dacă le externalizează.

(43) Abordarea riscurilor în materie de securitate cibernetică care decurg din lanțul de aprovizionare al unei entități și din relația acesteia cu furnizorii săi este deosebit de

importantă, având în vedere prevalența incidentelor în care entitățile au căzut victime atacurilor cibernetice și în care actori răuvoitori au fost în măsură să compromită securitatea rețelelor și a sistemelor informatice ale unei entități prin exploatarea vulnerabilităților care afectează produsele și serviciile părții terțe. Prin urmare, entitățile ar trebui să evalueze și să țină seama de calitatea generală a produselor și de practicile în materie de securitate cibernetică ale furnizorilor și ale prestatorilor lor de servicii, inclusiv de procedurile lor de dezvoltare sigure.

(44) În rândul furnizorilor de servicii, furnizorii de servicii de securitate administrați (*managed security services providers* – MSSP) în domenii precum răspunsul în caz de incidente, testele de penetrare, auditurile de securitate și consultanța joacă un rol deosebit de important în sprijinirea entităților în eforturile lor de a detecta și de a reacționa la incidente. Totuși, și aceste MSSP-uri au fost ținte ale atacurilor cibernetice și, prin integrarea lor strânsă în operațiunile operatorilor, prezintă un risc deosebit în materie de securitate cibernetică. Prin urmare, entitățile ar trebui să dea dovadă de o diligență sporită în selectarea unui MSSP.

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

(46) Pentru a aborda în continuare principalele riscuri din cadrul lanțului de aprovizionare și pentru a oferi asistență entităților care își desfășoară activitatea în sectoarele reglementate de prezenta directivă în gestionarea adecvată a riscurilor în materie de securitate cibernetică legate de lanțul de aprovizionare și de furnizori, Grupul de cooperare, la care participă autoritățile naționale relevante, ar trebui să efectueze, în cooperare cu Comisia și ENISA, evaluări sectoriale coordonate ale riscurilor la nivelul lanțului de aprovizionare, astfel cum s-a procedat deja în cazul rețelelor 5G ca urmare a Recomandării (UE) 2019/534 privind securitatea cibernetică a rețelelor 5G[21], cu scopul de a identifica, pentru fiecare sector în parte, care sunt serviciile, sistemele sau produsele TIC critice, amenințările și vulnerabilitățile relevante.

(47) Evaluările riscurilor din cadrul lanțului de aprovizionare, având în vedere caracteristicile sectorului în cauză, ar trebui să țină seama atât de factori tehnici, cât și, după caz, de factori fără caracter tehnic, inclusiv de cei definiți în Recomandarea (UE) 2019/534, în evaluarea coordonată la nivelul UE a riscurilor legate de securitatea rețelelor 5G și în setul de instrumente al UE privind securitatea cibernetică 5G convenit de Grupul de cooperare. Pentru a identifica lanțurile de aprovizionare care ar trebui să facă obiectul unei evaluări coordonate a riscurilor, ar trebui să se țină seama de următoarele criterii: (i) în ce măsură entitățile esențiale și importante utilizează și se bazează pe servicii, sisteme sau produse TIC critice specifice; (ii) relevanța serviciilor,

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

a sistemelor sau a produselor TIC critice specifice pentru îndeplinirea funcțiilor critice sau sensibile, printre care se numără și prelucrarea datelor cu caracter personal; (iii) disponibilitatea unor servicii, sisteme sau produse TIC alternative; (iv) reziliența întregului lanț de aprovizionare cu servicii, sisteme sau produse TIC împotriva evenimentelor perturbatoare și (v) pentru serviciile, sistemele sau produsele TIC emergente, potențiala lor importanță pentru activitățile pe care le vor desfășura entitățile în viitor.

(48) Pentru a raționaliza obligațiile juridice impuse furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului și furnizorilor de servicii de asigurare a încrederii în ceea ce privește securitatea rețelelor și a sistemelor lor informatice, precum și pentru a permite acestor entități și autorităților competente ale acestora să beneficieze de cadrul juridic instituit prin prezenta directivă (inclusiv desemnarea CSIRT responsabile de gestionarea riscurilor și de administrarea incidentelor, participarea autorităților și a organismelor competente la lucrările grupului de cooperare și ale rețelei CSIRT), acestea ar trebui incluse în domeniul de aplicare al prezentei directive. Prin urmare, dispozițiile corespunzătoare prevăzute în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului[22] și în Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului[23] referitoare la impunerea obligației de securitate și de notificare pentru aceste tipuri de entități ar trebui abrogate. Normele privind obligațiile de raportare nu ar trebui să aducă atingere nici Regulamentului (UE) 2016/679, nici Directivei 2002/58/CE a Parlamentului European și a Consiliului[24].

(49) După caz și pentru a evita perturbările inutile, orientările naționale existente și legislația națională adoptată pentru transpunerea normelor referitoare la măsurile de securitate prevăzute la articolul 40 alineatul (1) din Directiva (UE) 2018/1972, precum și a cerințelor de la articolul 40 alineatul (2) din această directivă privind parametrii referitori la importanța unui incident ar trebui utilizate în continuare de către autoritățile competente responsabile cu supravegherea și asigurarea aplicării în sensul prezentei directive.

(50) Având în vedere importanța crescândă a serviciilor de comunicații interpersonale care nu se bazează pe numere, este necesar să se asigure că aceste servicii fac, de asemenea, obiectul unor cerințe corespunzătoare în materie de securitate, în conformitate cu natura lor specifică și cu importanța lor economică. Furnizorii unor astfel de servicii ar trebui, prin urmare, să asigure și un nivel de securitate a rețelelor și a sistemelor informatice adecvat riscului prezentat. Având în vedere faptul că furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere nu exercită în mod normal un control efectiv asupra transmiterii semnalelor în rețea, gradul de risc aferent unor astfel de servicii poate fi considerat, în unele privințe, mai redus decât în cazul serviciilor tradiționale de comunicații electronice. Același lucru este valabil și pentru serviciile de comunicații interpersonale care utilizează numere și care nu exercită un control efectiv asupra transmiterii semnalului.

---

22 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).

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

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

(51) Piața internă depinde mai mult decât oricând de funcționarea internetului. Aproape toate serviciile entităților esențiale și importante depind de serviciile furnizate pe internet. Pentru a asigura furnizarea fără probleme a serviciilor asigurate de entități esențiale și importante, este important ca rețelele publice de comunicații electronice, cum ar fi, de exemplu, magistralele de internet sau cablurile de comunicații submarine, să dispună de măsuri adecvate în materie de securitate cibernetică și să raporteze incidentele legate de aceasta.

(52) După caz, entitățile ar trebui să își informeze destinatarii serviciilor cu privire la amenințări specifice și semnificative, precum și cu privire la măsurile pe care le pot lua pentru a atenua riscurile pentru ei înșiși. Cerința de a informa destinatarii cu privire la astfel de amenințări nu ar trebui să scutească entitățile de obligația de a lua, pe cheltuiala proprie, măsuri adecvate și imediate pentru a preveni sau remedia orice amenințare cibernetică și pentru a restabili nivelul normal de securitate al serviciului. Furnizarea unor astfel de informații privind amenințările la adresa securității destinatarilor ar trebui să fie gratuită.

(53) În special, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului ar trebui să îi informeze pe destinatarii serviciilor cu privire la amenințările cibernetice specifice și semnificative și cu privire la măsurile pe care le pot lua pentru a-și proteja securitatea comunicațiilor, de exemplu prin folosirea unor anumite tipuri de software sau de tehnologii de criptare.

(54) Pentru a se garanta securitatea rețelelor și a serviciilor de comunicații electronice, ar trebui promovată utilizarea criptării, în special a criptării de la un capăt la altul și, dacă este necesar, acest tip de criptare ar trebui să fie obligatoriu pentru furnizorii de astfel de servicii și rețele, în conformitate cu principiile securității și protecției vieții private în mod implicit și începând cu momentul conceperii, în sensul articolului 18. Utilizarea criptării de la un capăt la altul ar trebui să fie reconciliată cu competențele statelor membre de a asigura protecția intereselor lor esențiale în materie de securitate și de siguranță publică și de a permite investigarea, depistarea și urmărirea penală a infracțiunilor în conformitate cu dreptul Uniunii. Soluțiile pentru accesul legal la informații în comunicațiile criptate de la un capăt la altul ar trebui să mențină eficacitatea criptării în ceea ce privește protecția vieții private și securitatea comunicațiilor, oferind, în același timp, un răspuns eficace la criminalitate.

(55) Prezenta directivă stabilește o abordare în două etape a raportării incidentelor pentru a se ajunge la un echilibru adecvat între, pe de o parte, raportarea rapidă care contribuie la atenuarea unei eventuale răspândiri a incidentelor și le permite entităților să solicite sprijin și, pe de altă parte, raportarea aprofundată, care permite extragerea unor învățăminte valoroase din incidentele individuale și îmbunătățește în timp reziliența întreprinderilor individuale și a unor sectoare întregi la amenințările cibernetice. Atunci când entitățile descoperă că a aut loc un incident, acestea ar trebui să aibă obligația de a transmite o notificare inițială în termen de 24 de ore, urmată de un raport final în termen de cel mult o lună de la incidentul respectiv. Notificarea inițială ar trebui să includă numai informațiile strict necesare pentru a informa autoritățile competente cu privire la incident și pentru a putea solicita asistență, dacă este necesar. O astfel de notificare, după caz, ar trebui să indice dacă incidentul pare să fie cauzat de acțiuni ilegale sau răuvoitoare. Statele membre ar trebui să se asigure că cerința de transmitere a acestei notificări inițiale nu deviază resursele entității raportoare de la activitățile legate de administrarea incidentelor care ar trebui să aibă prioritate. Pentru a preveni și mai mult situațiile în care obligațiile de raportare a incidentelor fie deviază resursele de la gestionarea răspunsului la incidente, fie compromit eforturile depuse de

entități în acest sens, statele membre ar trebui să prevadă, de asemenea, că, în cazuri justificate în mod corespunzător și cu acordul autorităților competente sau al CSIRT, entitatea în cauză se poate abate de la termenul de 24 de ore pentru notificarea inițială și de o lună pentru raportul final.

(56) Entitățile esențiale și importante se află adesea într-o situație în care, din cauza caracteristicilor sale, un anumit incident trebuie raportat mai multor autorități ca urmare a obligațiilor de notificare incluse în diferite instrumente juridice. Astfel de cazuri creează sarcini suplimentare și pot conduce, de asemenea, la incertitudini în ceea ce privește formatul unor asemenea notificări și procedurile aferente acestora. Având în vedere cele de mai sus și în scopul simplificării raportării incidentelor de securitate, statele membre ar trebui să instituie un *punct de intrare unic* pentru toate notificările efectuate în temeiul prezentei directive și, de asemenea, în temeiul altor acte legislative ale Uniunii, cum ar fi Regulamentul (UE) 2016/679 și Directiva 2002/58/CE. ENISA, în cooperare cu Grupul de cooperare, ar trebui să instituie modele comune de notificare prin intermediul unor orientări care să simplifice și să raționalizeze informațiile de raportare solicitate de dreptul Uniunii și să reducă sarcinile impuse întreprinderilor.

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

(58) În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente. În acest context, autoritățile competente ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante cu autoritățile de protecție a datelor și cu autoritățile de supraveghere, în temeiul Directivei 2002/58/CE.

(59) Menținerea unor baze de date exacte și complete conținând numele de domenii și datele de înregistrare (așa-numitele „date WHOIS”) și furnizarea unui acces legal la astfel de date sunt aspecte esențiale pentru a asigura securitatea, stabilitatea și reziliența DNS, sistem care, la rândul său, contribuie la un nivel comun ridicat de securitate cibernetică în Uniune. Atunci când prelucrarea include date cu caracter personal, această prelucrare respectă legislația Uniunii în materie de protecție a datelor.

(60) Disponibilitatea și accesibilitatea în timp util a acestor date pentru autoritățile publice, inclusiv pentru autoritățile competente în temeiul dreptului Uniunii sau al dreptului intern pentru prevenirea, investigarea sau urmărirea penală a infracțiunilor, CERT, CSIRT și, în ceea ce privește datele clienților lor, pentru furnizorii de rețele și servicii de comunicații electronice și pentru furnizorii de tehnologii și servicii de securitate cibernetică care acționează în numele clienților respectivi, sunt aspecte esențiale pentru prevenirea și combaterea abuzurilor din sistemul de nume de domenii, în special pentru prevenirea, detectarea și combaterea incidentelor de securitate cibernetică. Acest tip de acces ar trebui să respecte legislația Uniunii în materie de protecție a datelor în măsura în care este legat de date cu caracter personal.

(61) Pentru a asigura disponibilitatea unor date exacte și complete de înregistrare a numelor de domeniu, registrele TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD (operatorii de registru) ar trebui să colecteze și să garanteze integritatea și disponibilitatea datelor de înregistrare a numelor de domenii. În special, registrele TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD ar trebui să stabilească politici și proceduri pentru colectarea și păstrarea unor date de înregistrare exacte și complete, precum și pentru prevenirea și corectarea datelor de înregistrare inexacte, în conformitate cu normele Uniunii privind protecția datelor.

(62) Registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii ar trebui să pună la dispoziția publicului date de înregistrare a numelor de domenii care nu intră în domeniul de aplicare al normelor Uniunii privind protecția datelor, cum ar fi datele care se referă la persoanele juridice[25]. Registrele TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD ar trebui, de asemenea, să le permită solicitanților legitimi de acces, în conformitate cu legislația Uniunii privind protecția datelor, accesul legal la date specifice de înregistrare a numelor de domenii privind persoanele fizice. Statele membre ar trebui să se asigure că registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii răspund fără întârzieri nejustificate solicitărilor de divulgare a datelor de înregistrare a numelor de domenii formulate de solicitanții legitimi de acces. Registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii ar trebui să stabilească politici și proceduri pentru publicarea și divulgarea datelor de înregistrare, inclusiv acorduri privind nivelul serviciilor pentru a trata cererile de acces din partea solicitanților legitimi de acces. Procedura de acces poate include, de asemenea, utilizarea unei interfețe, a unui portal sau a unui alt instrument tehnic, scopul fiind furnizarea unui sistem eficient de solicitare și accesare a datelor de înregistrare. În vederea promovării unor practici armonizate pe piața internă, Comisia poate adopta orientări cu privire la aceste proceduri fără a aduce atingere competențelor Comitetului european pentru protecția datelor.

(63) Toate entitățile esențiale și importante vizate de prezenta directivă sunt considerate ca fiind sub jurisdicția statului membru în care își prestează serviciile. În cazul în care entitatea furnizează servicii în mai multe state membre, aceasta ar trebui să intre sub jurisdicția separată și concurentă a fiecăruia dintre aceste state membre. Autoritățile competente din aceste state membre ar trebui să coopereze, să își ofere asistență reciprocă și, după caz, să întreprindă acțiuni comune de supraveghere.

(64) Pentru a ține seama de caracterul transfrontalier al serviciilor și al operațiunilor furnizorilor de servicii DNS, ale registrelor de nume TLD, ale furnizorilor de rețele de distribuție de conținut, ale furnizorilor de servicii de cloud computing, ale furnizorilor de servicii de centre de date și ale furnizorilor digitali, un singur stat membru ar trebui să aibă jurisdicție asupra acestor entități. Competența ar trebui să fie atribuită statului membru în care entitatea respectivă își are sediul principal în Uniune. Criteriul stabilirii în sensul prezentei directive implică exercitarea efectivă a activității prin intermediul unor înțelegeri stabile. Forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul

[25] Considerentul 14 din REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI prevede: „Prezentul regulament nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice.”

determinant în această privință. Respectarea acestui criteriu nu ar trebui să depindă de localizarea fizică a rețelei și a sistemelor informatice într-un anumit loc; prezența și utilizarea unor astfel de sisteme nu constituie, în sine, un astfel de sediu principal și, prin urmare, nu sunt criterii decisive pentru stabilirea sediului principal. Sediul principal ar trebui să fie locul în care sunt luate deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică în Uniune. Aceasta va corespunde, de regulă, locului în care se află administrația centrală a întreprinderilor din Uniune. În cazul în care astfel de decizii nu sunt luate în Uniune, se consideră că sediul principal se află în statul membru în care entitatea are sediul cu cel mai mare număr de angajați din Uniune. În cazul în care serviciile sunt prestate de un grup de întreprinderi, sediul principal al întreprinderii care exercită controlul ar trebui considerat drept sediul principal al grupului de întreprinderi.

(65) În cazurile în care un furnizor de servicii DNS, un registru al numelor TLD, un furnizor de rețea de livrare de conținut, un furnizor de servicii de cloud computing, un furnizor de servicii de centru de date sau un furnizor digital care nu este stabilit în Uniune oferă servicii în cadrul Uniunii, acesta ar trebui să desemneze un reprezentant. Pentru a determina dacă o astfel de entitate 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 entității sau al unui intermediar ori disponibilitatea unei adrese de e-mail și a altor date de contact sau utilizarea unei limbi folosite în general în țara terță în care își are sediul entitatea 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 ori menționarea unor clienți sau utilizatori din Uniune pot conduce la concluzia că entitatea intenționează să ofere servicii în Uniune. Reprezentantul ar trebui să acționeze în numele entității, iar autoritățile competente sau CSIRT ar trebui să poată contacta reprezentantul. Reprezentantul ar trebui să fie desemnat explicit printr-un mandat scris al entității pentru a acționa în numele acesteia în privința obligațiilor care îi revin acesteia în temeiul prezentei directive, inclusiv în privința raportării incidentelor.

(66) În cazul în care se face schimb de informații considerate clasificate în conformitate cu legislația națională sau a Uniunii ori astfel de informații sunt raportate sau partajate în alt mod în temeiul dispozițiilor prezentei directive, ar trebui să se aplice normele specifice corespunzătoare privind tratarea informațiilor clasificate.

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

(68) Entitățile ar trebui încurajate să își valorifice în mod colectiv cunoștințele individuale și experiența practică la nivel strategic, tactic și operațional, pentru a-și consolida capacitățile de evaluare și de monitorizare a amenințărilor cibernetice, de apărare împotriva acestora și de răspuns în mod adecvat la asemenea amenințări. Prin urmare,

este necesar să se permită apariția, la nivelul Uniunii, a unor mecanisme de schimb voluntar de informații. În acest scop, statele membre ar trebui să sprijine și să încurajeze în mod activ și entitățile relevante care nu intră în domeniul de aplicare al prezentei directive să participe la astfel de mecanisme de schimb de informații. Mecanismele respective ar trebui să se desfășoare în deplină conformitate cu normele Uniunii în materie de concurență, precum și cu normele Uniunii în materie de protecție a datelor.

(69) Prelucrarea datelor cu caracter personal, în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor de către entități, autorități publice, CERT, CSIRT și furnizorii de tehnologii și servicii de securitate ar trebui să constituie un interes legitim al operatorului de date în cauză, astfel cum se menționează în Regulamentul (UE) 2016/679. Aceasta ar trebui să includă măsuri legate de prevenirea, detectarea, analizarea și combaterea incidentelor, măsuri de sensibilizare cu privire la amenințările cibernetice specifice, schimbul de informații în contextul remedierii vulnerabilității și al divulgării coordonate, precum și schimbul voluntar de informații cu privire la incidentele respective, precum și la amenințările și vulnerabilitățile cibernetice, indicatori de compromis, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare. Astfel de măsuri pot necesita prelucrarea următoarelor tipuri de date cu caracter personal: adrese IP, localizatoare uniforme de resurse (URL), nume de domenii și adrese de e-mail.

(70) Pentru a consolida competențele și acțiunile de supraveghere care contribuie la asigurarea respectării efective, prezenta directivă ar trebui să prevadă o listă minimă de acțiuni și mijloace de supraveghere prin care autoritățile competente să poată supraveghea entitățile esențiale și importante. În plus, prezenta directivă ar trebui să stabilească o diferențiere între regimul de supraveghere al entităților esențiale și cel al entităților importante, în vederea asigurării unui echilibru echitabil al obligațiilor atât pentru entități, cât și pentru autoritățile competente. Astfel, entitățile esențiale ar trebui să facă obiectul unui regim de supraveghere complet (*ex ante* și *ex post*), în timp ce entitățile importante ar trebui să facă obiectul unui regim de supraveghere moderat, doar *ex post*. Pentru cele din urmă, acest lucru înseamnă că entitățile importante nu ar trebui să documenteze în mod sistematic respectarea cerințelor de gestionare a riscurilor în materie de securitate cibernetică, în timp ce autoritățile competente ar trebui să pună în aplicare o abordare reactivă *ex post* a supravegherii și, prin urmare, să nu aibă o obligație generală de a supraveghea entitățile respective.

(71) Pentru ca asigurarea respectării să fie eficace, ar trebui stabilită o listă minimă de sancțiuni administrative pentru încălcarea obligațiilor de gestionare a riscurilor de securitate cibernetică și de raportare prevăzute în prezenta directivă, stabilind un cadru clar și coerent pentru astfel de sancțiuni în întreaga Uniune. Ar trebui să se țină seama în mod corespunzător de natura, gravitatea și durata încălcării, de daunele reale cauzate sau de pierderile suferite ori de daunele sau pierderile potențiale care ar fi putut fi declanșate, de caracterul intenționat sau din neglijență al încălcării, de acțiunile întreprinse pentru a preveni sau a atenua prejudiciul și/sau pierderile suferite, de gradul de responsabilitate sau de orice încălcare anterioară relevantă, de gradul de cooperare cu autoritatea competentă și de orice alt factor agravant sau atenuant. Impunerea de sancțiuni, inclusiv de amenzi administrative, ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene, inclusiv al unei protecții judiciare eficiente și al unui proces echitabil.

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

(73) În cazul în care amenzile administrative sunt impuse unei întreprinderi, acest termen ar trebui înțeles ca fiind o întreprindere în conformitate cu articolele 101 și 102 din TFUE în aceste scopuri. În cazul în care se impun amenzi administrative unor persoane care nu sunt întreprinderi, autoritatea de supraveghere ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al amenzii. Competența de a stabili dacă și în ce măsură autoritățile publice ar trebui să facă obiectul unor amenzi administrative ar trebui să revină statelor membre. Impunerea unei amenzi administrative nu afectează exercitarea altor competențe de către autoritățile competente sau aplicarea altor sancțiuni prevăzute în normele naționale de transpunere a prezentei directive.

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

(75) În cazul în care prezenta directivă nu armonizează sancțiunile administrative sau în alte cazuri, acolo unde este necesar, de exemplu în cazul unor încălcări grave ale obligațiilor prevăzute în prezenta directivă, statele membre ar trebui să pună în aplicare un sistem care să prevadă sancțiuni eficace, proporționale și disuasive. Natura unor astfel de sancțiuni, penale sau administrative, ar trebui stabilită în legislația statelor membre.

(76) Pentru a consolida și mai mult eficacitatea și caracterul disuasiv al sancțiunilor aplicabile în cazul încălcării obligațiilor prevăzute în temeiul prezentei directive, autoritățile competente ar trebui să fie împuternicite să aplice sancțiuni constând în suspendarea unei certificări sau a unei autorizații privind o parte din serviciile furnizate de o entitate esențială sau toate aceste servicii și impunerea unei interdicții temporare de a exercita funcții de conducere de către o persoană fizică. Având în vedere gravitatea și impactul lor asupra activităților entităților și, în cele din urmă, asupra consumatorilor acestora, aceste sancțiuni ar trebui aplicate numai proporțional cu gravitatea încălcării și ținând seama de circumstanțele specifice fiecărui caz, inclusiv de caracterul intenționat sau din neglijență al încălcării, de măsurile luate pentru a preveni sau a atenua prejudiciul și/sau de pierderile suferite. Astfel de sancțiuni ar trebui aplicate doar în ultimă instanță, adică numai după ce celelalte măsuri relevante de asigurare a respectării legislației prevăzute de prezenta directivă au fost epuizate și numai până în momentul în care entitățile cărora li se aplică iau măsurile necesare pentru a remedia deficiențele sau pentru a se conforma cerințelor autorității competente pentru care au fost aplicate aceste sancțiuni. Impunerea unor astfel de sancțiuni face obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene, inclusiv protecția jurisdicțională efectivă, respectarea garanțiilor procedurale, prezumția de nevinovăție și dreptul la apărare.

(77) Prezenta directivă ar trebui să stabilească norme de cooperare între autoritățile competente și autoritățile de supraveghere în conformitate cu

Regulamentul (UE) 2016/679 pentru tratarea cazurilor de încălcare a normelor în materie de date cu caracter personal.

(78) Prezenta directivă ar trebui să vizeze asigurarea unui nivel ridicat de responsabilitate pentru măsurile de gestionare a riscurilor în materie de securitate cibernetică și pentru obligațiile de raportare la nivelul organizațiilor. Din aceste motive, organele de conducere ale entităților care intră în domeniul de aplicare al prezentei directive ar trebui să aprobe măsurile privind riscurile la adresa securității cibernetice și să supravegheze punerea lor în aplicare.

(79) Ar trebui introdus un mecanism de evaluare *inter pares*, care să permită evaluarea de către experții desemnați de statele membre a punerii în aplicare a politicilor în materie de securitate cibernetică, inclusiv a nivelului capacităților și al resurselor de care dispun statele membre.

(80) Pentru a ține seama de noile amenințări cibernetice, de evoluțiile tehnologice sau de specificitățile sectoriale, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei în ceea ce privește elementele legate de măsurile de gestionare a riscurilor impuse de prezenta directivă. Comisia ar trebui, de asemenea, să fie împuternicită să adopte acte delegate pentru a stabili ce categorii de entități esențiale au obligația de a obține un certificat și în temeiul căror sisteme europene specifice de certificare a securității cibernetice. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare[26]. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(81) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a dispozițiilor relevante ale prezentei directive în ceea ce privește dispozițiile procedurale necesare pentru funcționarea grupului de cooperare, elementele tehnice legate de măsurile de gestionare a riscurilor sau tipul de informații, formatul și procedura de notificare a incidentelor, Comisiei ar trebui să i se confere competențe de executare. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[27].

(82) 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.

(83) Întrucât obiectivul prezentei directive, și anume obținerea unui nivel comun ridicat de securitate cibernetică în Uniune, nu poate fi suficient realizat 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

[26] JO L 123, 12.5.2016, p. 1.

[27] 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).

proporționalității prevăzut la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru atingerea obiectivului respectiv.

(84) 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

1. Prezenta directivă stabilește măsuri în vederea asigurării unui nivel comun ridicat de securitate cibernetică în Uniune.

2. În acest scop, prezenta directivă:

(a) stabilește obligațiile statelor membre de a adopta strategii naționale de securitate cibernetică, de a desemna autorități naționale competente, puncte unice de contact și echipe de intervenție în caz de incidente de securitate informatică (CSIRT);

(b) stabilește obligațiile de gestionare și de raportare a riscurilor în materie de securitate cibernetică pentru entitățile de tipul celor menționate ca fiind entități esențiale în anexa I și entități importante în anexa II;

(c) stabilește obligații privind schimbul de informații în materie de securitate cibernetică.

Articolul 2

Domeniul de aplicare

1. Prezenta directivă se aplică entităților publice și private de tipul celor menționate ca fiind entități esențiale în anexa I și entități importante în anexa II. Prezenta directivă nu se aplică entităților care se califică drept microîntreprinderi și întreprinderi mici în sensul Recomandării 2003/361/CE a Comisiei[28].

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

2. Cu toate acestea, indiferent de dimensiunea lor, prezenta directivă se aplică, de asemenea, entităților menționate în anexele I și II, în cazul în care:

(b) serviciile sunt furnizate de una dintre următoarele entități:

(i) rețelele publice de comunicații electronice sau serviciile de comunicații electronice accesibile publicului menționate la punctul 8 din anexa I;

(ii) prestatorii de servicii de încredere menționați la punctul 8 din anexa I;

(iii) registrele de nume de domenii de prim nivel și furnizorii de servicii de sistem de nume de domenii (DNS) menționați la punctul 8 din anexa I;

(b) entitatea este o entitate a administrației publice, astfel cum este definită la articolul 4 punctul 23;

(c) entitatea este singurul furnizor al unui serviciu într-un stat membru;

(d) o eventuală perturbare a serviciului furnizat de entitate ar putea avea un impact asupra siguranței publice, a securității publice sau a sănătății publice;

(e) o eventuală perturbare a serviciului furnizat de entitate ar putea genera riscuri sistemice, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier;

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

(g) entitatea este identificată ca fiind o entitate critică în temeiul Directivei (UE) XXXX/XXXX a Parlamentului European și a Consiliului[29] [Directiva privind reziliența entităților critice] sau o entitate echivalentă cu o entitate critică în temeiul articolului 7 din directiva respectivă.

Statele membre întocmesc o listă a entităților identificate în temeiul literelor (b) - (f) și o transmit Comisiei până la [6 luni de la termenul de transpunere]. Statele membre revizuiesc lista în mod regulat și, ulterior, cel puțin o dată la doi ani și, dacă este cazul, o actualizează.

3. Prezenta directivă nu aduce atingere competențelor statelor membre în ceea ce privește menținerea securității publice, a apărării și a securității naționale în conformitate cu dreptul Uniunii.

4. Prezenta directivă se aplică fără a aduce atingere Directivei 2008/114/CE a Consiliului[30] și Directivelor 2011/93/UE[31] și 2013/40/UE[32] ale Parlamentului European și ale Consiliului.

---

29 *[a se introduce titlul complet și referința de publicare în JO, atunci când acestea vor fi cunoscute]*

30 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).

31 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).

32 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).

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. Schimbul de informații păstrează confidențialitatea informațiilor respective și protejează securitatea și interesele comerciale ale entităților esențiale sau importante.

6. În cazul în care dispozițiile actelor specifice fiecărui sector din dreptul Uniunii impun entităților esențiale sau importante fie să adopte măsuri de gestionare a riscurilor în materie de securitate cibernetică, fie să notifice incidentele sau amenințările cibernetice semnificative, iar cerințele respective au un efect cel puțin echivalent cu efectul obligațiilor prevăzute în prezenta directivă, nu se aplică dispozițiile relevante ale prezentei directive, așadar nici dispozițiile privind supravegherea și asigurarea respectării legislației, prevăzute în capitolul VI.

Articolul 3

Armonizarea minimă

Fără a aduce atingere celorlalte obligații care le revin în temeiul dreptului Uniunii, statele membre pot, în conformitate cu prezenta directivă, să adopte sau să mențină dispoziții care să asigure un nivel mai ridicat de securitate cibernetică.

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 alineatul (1) din Directiva (UE) 2018/1972;

(b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale;

(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, transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

(3) „securitate cibernetică” înseamnă securitate cibernetică în sensul articolului 2 alineatul (1) din Regulamentul (UE) nr. 2019/881 al Parlamentului European și al Consiliului[33];

(4) „strategie națională de securitate cibernetică” înseamnă un cadru coerent al unui stat membru care prevede obiective și priorități strategice privind securitatea rețelelor și a sistemelor informatice în statul membru respectiv;

(5) „incident” înseamnă orice eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor conexe oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora;

(6) „administrarea incidentelor” înseamnă toate acțiunile și procedurile care vizează detectarea, analizarea și limitarea unui incident, precum și răspunsul la acesta;

(7) „amenințare cibernetică” înseamnă o amenințare cibernetică în sensul articolului 2 punctul 8 din Regulamentul (UE) 2019/881;

(8) „vulnerabilitate” înseamnă un punct slab, o susceptibilitate sau o deficiență a unui activ, sistem, proces sau control care poate fi exploatată de o amenințare cibernetică;

(9) „reprezentant” înseamnă orice persoană fizică sau juridică stabilită în Uniune care este desemnată în mod explicit să acționeze în numele i) unui furnizor de servicii DNS, al unui registru de nume de domenii de prim nivel (TLD), al unui furnizor de servicii de cloud computing, al unui furnizor de servicii de centre de date, al unui furnizor de rețele de furnizare de conținut, astfel cum se menționează la punctul 8 din anexa I sau ii) al entităților menționate la punctul 6 din anexa II care nu sunt stabilite în Uniune, căreia i se poate adresa o autoritate națională competentă sau o CSIRT în locul entității în ceea ce privește obligațiile entității respective în temeiul prezentei directive;

(10) „standard” înseamnă un standard în sensul articolului 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[34];

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

(12) „internet exchange point (IXP)” înseamnă o structură de rețea care permite interconectarea a mai mult de două rețele independente (sisteme autonome), 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 o pereche oarecare de sisteme autonome participante și nici nu modifică sau afectează într-un alt mod acest trafic;

---

[33] Regulamentul (UE) nr. 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

[34] 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).

(13) „sistem de nume de domenii (DNS)” înseamnă un sistem ierarhic și distribuit de atribuire de nume care le permite utilizatorilor finali să acceseze servicii și resurse pe internet;

(14) „furnizor de servicii DNS” înseamnă o entitate care furnizează servicii de rezoluție a numelor de domenii recursive sau cu autoritate utilizatorilor finali de internet și altor furnizori de servicii DNS;

(15) „registru de nume de domenii de prim nivel” înseamnă o entitate căreia i s-a delegat un anumit domeniu de prim nivel (*top–level domain* –TLD) și care este responsabilă cu administrarea TLD-ului, inclusiv cu înregistrarea numelor de domenii în cadrul TLD-ului și cu exploatarea tehnică a TLD-ului, în special cu exploatarea serverelor sale de nume, cu întreținerea bazelor sale de date și cu distribuirea fișierelor zonale TLD între serverele de nume;

(16) „serviciu digital” înseamnă un serviciu în sensul articolului 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului [35];

(17) „piață online” înseamnă un serviciu digital în sensul articolului 2 litera (n) din Directiva 2005/29/CE a Parlamentului European și a Consiliului[36];

(18) „motor de căutare online” înseamnă un serviciu digital în sensul articolului 2 alineatul (5) din Regulamentul (UE) 2019/1150 al Parlamentului European și al Consiliului[37];

(19) „serviciu de cloud computing” înseamnă un serviciu digital care permite administrarea la cerere și accesul amplu la distanță la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun și distribuite;

(20) „serviciu de centre de date” înseamnă un serviciu care cuprinde structuri sau grupuri de structuri dedicate găzduirii, interconectării și exploatării centralizate a tehnologiei informației și a echipamentelor de rețea care furnizează servicii de stocare, prelucrare și transport de date, împreună cu toate instalațiile și infrastructurile de distribuție a energiei electrice și de control al mediului;

(21) „rețea de furnizare de conținut” înseamnă o rețea de servere distribuite geografic cu scopul de a asigura o disponibilitate ridicată, accesibilitate sau furnizare rapidă de conținut digital și servicii către utilizatorii de internet în numele furnizorilor de conținut și de servicii;

(22) „platformă de servicii de socializare în rețea” înseamnă o platformă care le permite utilizatorilor finali să se conecteze, să partajeze, să descopere și să comunice între ei prin intermediul mai multor dispozitive, în special prin chat, postări, materiale video și recomandări;

---

35 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).

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

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

(23) „entitate a administrației publice” înseamnă o entitate dintr-un stat membru care îndeplinește următoarele criterii:

(a) a fost înființată în scopul satisfacerii unor nevoi de interes general și nu are caracter industrial sau comercial;

(b) are personalitate juridică;

(c) este finanțată, în cea mai mare parte, de stat, de autoritatea regională sau de alte organisme de drept public; sau face obiectul unui control de gestiune din partea autorităților sau a organismelor respective; sau are un consiliu de administrație, de conducere sau de supraveghere ai cărui membri sunt desemnați în proporție de peste 50 % de stat, de autoritățile regionale sau de alte organisme de drept public;

(d) are competența de a adresa persoanelor fizice sau juridice decizii administrative sau de reglementare care le afectează drepturile în ceea ce privește circulația transfrontalieră a persoanelor, mărfurilor, serviciilor sau capitalurilor.

Sunt excluse entitățile administrației publice care desfășoară activități în domeniul securității publice, al aplicării legii, al apărării sau al securității naționale.

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

(25) „entitate esențială” înseamnă orice entitate de tipul celor menționate ca fiind entități esențiale în anexa I;

(26) „entitate importantă” înseamnă orice entitate de tipul celor menționate ca fiind entități importante în anexa II.

CAPITOLUL II

Cadre de reglementare coordonate în materie de securitate cibernetică

Articolul 5
Strategia națională de securitate cibernetică

1. Fiecare stat membru adoptă o strategie națională de securitate cibernetică care definește obiectivele strategice și măsurile de politică și de reglementare adecvate, în vederea atingerii și menținerii unui nivel ridicat de securitate cibernetică. Strategia națională de securitate cibernetică include, în special, următoarele elemente:

(a) o definire a obiectivelor și a priorităților strategiei statelor membre privind securitatea cibernetică;

(b) un cadru de guvernanță pentru realizarea acestor obiective și priorități, inclusiv politicile menționate la alineatul (2) și rolurile și responsabilitățile organismelor și ale entităților publice, precum și ale altor actori relevanți;

(c) o evaluare menită să identifice activele și riscurile în materie de securitate cibernetică relevante din statul membru respectiv;

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

(e) o listă a diferitelor autorități și a diferiților actori care participă la punerea în aplicare a strategiei naționale de securitate cibernetică;

(f) un cadru de politică menit să asigure o mai bună coordonare între autoritățile competente în temeiul prezentei directive și al Directivei (UE) XXXX/XXXX a Parlamentului European și a Consiliului[38] [Directiva privind reziliența entităților critice] în scopul schimbului de informații privind incidentele și amenințările cibernetice și al exercitării sarcinilor de supraveghere.

2. În cadrul strategiei naționale de securitate cibernetică, statele membre adoptă în special următoarele politici:

(a) o politică ce abordează securitatea cibernetică în lanțul de aprovizionare pentru produsele și serviciile TIC utilizate de entitățile esențiale și importante pentru furnizarea serviciilor lor;

(b) orientări privind includerea și specificarea cerințelor legate de securitatea cibernetică pentru produsele și serviciile TIC în cadrul achizițiilor publice;

(c) o politică de promovare și facilitare a divulgării coordonate a vulnerabilităților în sensul articolului 6;

(d) o politică legată de menținerea disponibilității și a integrității generale a nucleului public al internetului deschis;

(e) o politică de promovare și dezvoltare a inițiativelor privind competențele, sensibilizarea și cercetarea și dezvoltarea în materie de securitate cibernetică;

(f) o politică de sprijinire a instituțiilor academice și de cercetare în vederea dezvoltării unor instrumente de securitate cibernetică și a unei infrastructuri de rețea securizate;

(g) o politică, proceduri relevante și instrumente adecvate de schimb de informații care să sprijine schimbul voluntar de informații în materie de securitate cibernetică între întreprinderi, în conformitate cu dreptul Uniunii;

(h) o politică care răspunde nevoilor specifice ale IMM-urilor, în special ale celor excluse din domeniul de aplicare al prezentei directive, în ceea ce privește orientările și sprijinul pentru îmbunătățirea rezilienței acestora la amenințările la adresa securității cibernetice.

3. Statele membre notifică Comisiei strategiile lor naționale de securitate cibernetică în termen de trei luni de la adoptarea acestora. Statele membre pot exclude din notificare anumite informații în cazul și în măsura în care acest lucru este strict necesar pentru menținerea securității naționale.

4. Statele membre își evaluează strategiile naționale de securitate cibernetică cel puțin o dată la patru ani pe baza indicatorilor-cheie de performanță și, dacă este necesar, le modifică. Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) sprijină statele membre, la cerere, în elaborarea unei strategii naționale și a unor indicatori-cheie de performanță pentru evaluarea strategiei.

[38] *[a se introduce titlul complet și referința de publicare în JO, atunci când acestea vor fi cunoscute]*

Articolul 6

Divulgarea coordonată a vulnerabilităților și registrul european al vulnerabilităților

1. Fiecare stat membru desemnează una dintre echipele sale CSIRT, astfel cum se menționează la articolul 9, drept coordonator în scopul divulgării coordonate a vulnerabilităților. CSIRT desemnată acționează ca intermediar de încredere, facilitând, dacă este necesar, interacțiunea dintre entitatea raportoare și producătorul sau furnizorul de produse TIC sau servicii TIC. În cazul în care vulnerabilitatea raportată vizează mai mulți producători sau furnizori de produse TIC sau de servicii TIC din Uniune, CSIRT desemnată din fiecare stat membru în cauză cooperează cu rețeaua CSIRT.

2. ENISA creează și menține un registru european al vulnerabilităților. În acest scop, ENISA instituie și menține sisteme, politici și proceduri de informare adecvate, în special pentru a permite entităților importante și esențiale și furnizorilor acestora de rețele și sisteme informatice să divulge și să înregistreze vulnerabilitățile prezente în produsele TIC sau serviciile TIC, precum și să ofere acces tuturor părților interesate la informațiile privind vulnerabilitățile conținute în registru. Registrul include, în special, informații care descriu vulnerabilitatea, produsul TIC sau serviciile TIC afectate și gravitatea vulnerabilității în ceea ce privește circumstanțele în care aceasta poate fi exploatată, disponibilitatea unor corecții conexe și, dacă astfel de corecții nu sunt disponibile, orientări adresate utilizatorilor de produse și servicii vulnerabile cu privire la modul în care pot fi atenuate riscurile care rezultă din vulnerabilitățile divulgate.

Articolul 7

Cadrele naționale de gestionare a crizelor în materie de securitate cibernetică

1. Fiecare stat membru desemnează una sau mai multe autorități competente responsabile cu gestionarea incidentelor și a crizelor de mare amploare. Statele membre se asigură că autoritățile competente dispun de resurse adecvate pentru a îndeplini, în mod eficace și eficient, sarcinile care le-au fost încredințate.

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

3. Fiecare stat membru adoptă un plan național de răspuns la incidente și crize de securitate cibernetică în care sunt stabilite obiective și modalități de gestionare a incidentelor și a crizelor de securitate cibernetică de mare amploare. Planul stabilește, în special, următoarele:

   (a) obiectivele măsurilor și ale activităților naționale de pregătire;

   (b) sarcinile și responsabilitățile autorităților naționale competente;

   (c) procedurile de gestionare a crizelor și canalele de schimb de informații;

   (d) măsurile de pregătire, inclusiv exerciții și activități de formare;

   (e) părțile interesate relevante din sectorul public și privat și infrastructura implicată;

(f) procedurile și mecanismele naționale dintre autoritățile și organismele naționale relevante menite să asigure participarea efectivă a statului membru la gestionarea coordonată a incidentelor și a crizelor de securitate cibernetică de mare amploare la nivelul Uniunii și sprijinul acordat de acesta.

4. Statele membre comunică Comisiei desemnarea autorităților lor competente menționate la alineatul (1) și își prezintă planurile naționale de răspuns la incidente și crize în materie de securitate cibernetică, astfel cum se menționează la alineatul (3), în termen de trei luni de la desemnarea autorităților și adoptarea planurilor respective. Statele membre pot exclude din plan anumite informații în cazul și în măsura în care acest lucru este strict necesar pentru securitatea lor națională.

Articolul 8

Autoritățile naționale competente și punctele unice de contact

1. Fiecare stat membru desemnează una sau mai multe autorități competente responsabile cu securitatea cibernetică și cu sarcinile de supraveghere menționate în capitolul VI din prezenta directivă. Statele membre pot desemna în acest scop o autoritate existentă sau autorități existente.

2. Autoritățile competente menționate la alineatul (1) monitorizează aplicarea prezentei directive la nivel național.

3. Fiecare stat membru desemnează un punct unic de contact național în materie de securitate cibernetică („punct unic de contact”). În cazul în care un stat membru desemnează o singură autoritate competentă, aceasta servește, de asemenea, drept punct unic de contact pentru statul membru respectiv.

4. Fiecare punct unic de contact exercită o funcție de legătură menită să asigure cooperarea transfrontalieră a autorităților din statul său membru cu autoritățile relevante din alte state membre și să asigure cooperarea transsectorială cu alte autorități naționale competente din statul său membru.

5. Statele membre se asigură că autoritățile competente menționate la alineatul (1) și punctele unice de contact dispun de resurse adecvate pentru a-și îndeplini în mod eficace și eficient sarcinile care le-au fost atribuite și a realiza astfel obiectivele prezentei directive. Statele membre asigură cooperarea eficace, eficientă și sigură a reprezentanților desemnați în grupul de cooperare menționat la articolul 12.

6. Fiecare stat membru notifică fără întârzieri nejustificate Comisiei desemnarea autorității competente menționate la alineatul (1) și a punctului unic de contact menționat la alineatul (3), sarcinile acestora și orice modificare ulterioară a acestora. Fiecare stat membru face publică desemnarea lor. 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 la articolul 10 alineatul (1) și care acoperă cel puțin sectoarele, subsectoarele sau entitățile menționate în anexele I și II; acestea sunt responsabile de administrarea incidentelor în conformitate cu o procedură bine definită. O echipă

CSIRT poate fi înființată în cadrul unei autorități competente menționate la articolul 8.

2. Statele membre se asigură că fiecare echipă CSIRT dispune de resurse adecvate pentru a-și îndeplini efectiv sarcinile stabilite la articolul 10 alineatul (2).

3. Statele membre se asigură că fiecare echipă CSIRT dispune de o infrastructură de comunicare și de informații adecvată, sigură și reziliență pentru a face schimb de informații cu entitățile esențiale și importante și cu alte părți interesate relevante. În acest scop, statele membre se asigură că echipele CSIRT contribuie la implementarea unor instrumente securizate de schimb de informații.

4. Echipele CSIRT cooperează și, după caz, fac schimb de informații relevante în conformitate cu articolul 26 cu comunități sectoriale sau transsectoriale de încredere formate din entități esențiale și importante.

5. Echipele CSIRT participă la evaluările *inter pares* organizate în conformitate cu articolul 16.

6. Statele membre asigură cooperarea efectivă, eficientă și sigură a propriilor echipe CSIRT în cadrul rețelei CSIRT menționate la articolul 13.

7. Statele membre comunică fără întârzieri nejustificate Comisiei echipele CSIRT desemnate în conformitate cu alineatul (1), coordonatorul CSIRT desemnat în conformitate cu articolul 6 alineatul (1) și sarcinile acestora prevăzute în legătură cu entitățile menționate în anexele I și II.

8. Statele membre pot solicita asistența ENISA pentru instituirea echipelor CSIRT naționale.

Articolul 10

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

1. Echipele CSIRT trebuie să respecte următoarele cerințe:

   (a) echipele CSIRT asigură o disponibilitate ridicată a serviciilor lor de comunicații, evitând punctele unice de defecțiune și dispun de mai multe mijloace pentru a fi contactate și pentru a contacta alte entități în orice moment. Echipele CSIRT specifică în mod clar canalele de comunicare și le aduc la cunoștința utilizatorilor și a partenerilor de cooperare;

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

   (c) echipele CSIRT dispun de un sistem adecvat de gestionare și rutare a cererilor, în special în vederea facilitării eficace și eficiente a transferurilor;

   (d) echipele CSIRT dispun de personal adecvat pentru a asigura o disponibilitate permanentă;

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

   (f) echipele CSIRT au posibilitatea de a participa la rețele internaționale de cooperare.

2. Echipelor CSIRT le revin următoarele sarcini:

(a) monitorizarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor la nivel național;

(b) asigurarea unor mecanisme de avertizare timpurii, alerte, anunțuri și diseminare de informații către entitățile esențiale și importante, precum și către alte părți interesate relevante cu privire la amenințările cibernetice, vulnerabilități și incidente;

(c) răspunsul la incidente;

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

(e) furnizarea, la cererea unei entități, a unei scanări proactive a rețelei și a sistemelor informatice utilizate pentru furnizarea serviciilor lor;

(f) participarea la rețeaua CSIRT și furnizarea de asistență reciprocă altor membri ai rețelei, la cererea acestora.

3. Echipele CSIRT stabilesc relații de cooperare cu actorii relevanți din sectorul privat, în vederea unei mai bune îndepliniri a obiectivelor directivei.

4. Pentru a facilita cooperarea, echipele CSIRT promovează adoptarea și utilizarea unor practici, sisteme de clasificare și taxonomii comune sau standardizate în legătură cu următoarele:

(a) procedurile de administrare a incidentelor;

(b) gestionarea crizelor în materie de securitate cibernetică;

(c) divulgarea coordonată a vulnerabilităților.

Articolul 11

Cooperarea la nivel național

1. Atunci când sunt separate, autoritățile competente menționate la articolul 8, punctul unic de contact și echipele (echipa) CSIRT ale aceluiași stat membru cooperează între ele pentru îndeplinirea obligațiilor ce le revin în temeiul prezentei directive.

2. Statele membre se asigură că fie autoritățile lor competente, fie echipele lor CSIRT primesc notificări privind incidentele, amenințările cibernetice semnificative și incidentele evitate la limită comunicate în temeiul prezentei directive. În cazul în care un stat membru decide ca echipele sale CSIRT să nu primească notificări, acestora li se acordă, în măsura necesară pentru a-și îndeplini atribuțiile, acces la datele privind incidentele notificate de entitățile esențiale sau importante, în temeiul articolului 20.

3. Fiecare stat membru se asigură că autoritățile sale competente sau echipele sale CSIRT informează punctul său unic de contact cu privire la notificările privind incidentele, amenințările cibernetice semnificative și incidentele evitate la limită comunicate în temeiul prezentei directive.

4. În măsura în care este necesar pentru a îndeplini în mod eficace sarcinile și obligațiile prevăzute în prezenta directivă, statele membre asigură o cooperare adecvată între autoritățile competente și punctele unice de contact și autoritățile de aplicare a legii, autoritățile pentru protecția datelor și autoritățile responsabile cu

infrastructura critică în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] și autoritățile financiare naționale desemnate în conformitate cu Regulamentul (UE) XXXX/XXXX al Parlamentului European și al Consiliului[39] [Regulamentul DORA] din statul membru respectiv.

5. Statele membre se asigură că autoritățile lor competente furnizează periodic informații autorităților competente desemnate în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] cu privire la riscurile de securitate cibernetică, amenințările cibernetice și incidentele care afectează entitățile esențiale identificate ca fiind critice sau ca entități echivalente cu entitățile critice, în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice], precum și cu privire la măsurile luate de autoritățile competente ca răspuns la aceste riscuri și incidente.

CAPITOLUL III

Cooperare

Articolul 12
Grupul de cooperare

1. Pentru a sprijini și a facilita cooperarea strategică și schimbul de informații între statele membre în domeniul aplicării directivei, se instituie un grup de cooperare.

2. Grupul de cooperare își îndeplinește sarcinile pe baza programelor bienale de lucru menționate la alineatul (6).

3. Grupul de cooperare este format din reprezentanți ai statelor membre, ai Comisiei și ai ENISA. Serviciul European de Acțiune Externă participă la activitățile grupului de cooperare în calitate de observator. Autoritățile europene de supraveghere (AES) în conformitate cu articolul 17 alineatul (5) litera (c) din Regulamentul (UE) XXXX/XXXX [Regulamentul DORA] pot participa la activitățile grupului de cooperare.

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

   Comisia asigură secretariatul.

4. Grupului de cooperare îi revin următoarele sarcini:

   (a) furnizarea de orientări autorităților competente în legătură cu transpunerea și punerea în aplicare a prezentei directive;

   (b) schimbul de bune practici și de informații în legătură cu punerea în aplicare a prezentei directive, inclusiv în ceea ce privește amenințările cibernetice, incidentele, vulnerabilitățile, incidentele evitate la limită, inițiativele de sensibilizare, cursurile de formare, exercițiile și competențele, consolidarea capacităților, precum și standardele și specificațiile tehnice;

[39] *[a se introduce titlul complet și referința de publicare în JO, atunci când acestea vor fi cunoscute]*

(c) schimbul de opinii și cooperarea cu Comisia cu privire la inițiativele emergente de politică în materie de securitate cibernetică;

(d) schimbul de opinii și cooperarea cu Comisia cu privire la proiectele de acte de punere în aplicare sau acte delegate ale Comisiei adoptate în temeiul prezentei directive;

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

(f) discutarea rapoartelor privind evaluarea *inter pares* menționate la articolul 16 alineatul (7);

(g) discutarea rezultatelor activităților de supraveghere comună în cazurile transfrontaliere, astfel cum se menționează la articolul 34;

(h) furnizarea de orientări strategice rețelei CSIRT cu privire la aspecte emergente specifice;

(i) contribuția la capacitățile în materie de securitate cibernetică în întreaga Uniune prin facilitarea schimbului de funcționari naționali prin intermediul unui program de consolidare a capacităților care implică personal din cadrul autorităților competente ale statelor membre sau al CSIRT;

(j) organizarea de reuniuni comune periodice cu părțile interesate relevante din sectorul privat din întreaga Uniune pentru a discuta activitățile pe care le desfășoară grupul și pentru a colecta informații cu privire la noile dificultăți în materie de politici;

(k) discutarea activității desfășurate în legătură cu exercițiile de securitate cibernetică, inclusiv a activității desfășurate de ENISA.

5. Grupul de cooperare poate solicita rețelei CSIRT un raport tehnic pe anumite teme.

6. Până la ...[24 de luni de la data intrării în vigoare a prezentei directive] și, ulterior, o dată la doi ani, grupul de cooperare stabilește un program de lucru cu privire la acțiunile care urmează să fie întreprinse pentru punerea în aplicare a obiectivelor și a sarcinilor sale. Calendarul primului program adoptat în temeiul prezentei directive este aliniat la calendarul ultimului program adoptat în temeiul Directivei (UE) 2016/1148.

7. Comisia poate adopta acte de punere în aplicare prin care se stabilesc acordurile procedurale necesare pentru funcționarea grupului de cooperare. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 37 alineatul (2).

8. Grupul de cooperare se reunește periodic și cel puțin o dată pe an cu Grupul privind reziliența entităților critice instituit în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] pentru a promova cooperarea strategică și schimbul de informații.

Articolul 13

Rețeaua CSIRT

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

2. Rețeaua CSIRT este formată 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 sarcini:

   (a) schimbul de informații privind capacitățile CSIRT;

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

   (c) la cererea unui reprezentant al rețelei CSIRT care ar putea fi afectat de un incident, schimbul de informații și discutarea informațiilor cu privire la incidentul respectiv și la amenințările cibernetice, riscurile și vulnerabilitățile conexe;

   (d) la cererea unui reprezentant al rețelei CSIRT, discutarea și, după caz, punerea în aplicare a unui răspuns coordonat la un incident care a fost identificat în jurisdicția statului membru respectiv;

   (e) furnizarea de sprijin statelor membre în abordarea incidentelor transfrontaliere în temeiul prezentei directive;

   (f) cooperarea și furnizarea de asistență echipelor CSIRT desemnate menționate la articolul 6 în ceea ce privește gestionarea divulgării coordonate multipartite a vulnerabilităților care afectează mai mulți producători sau furnizori de produse TIC, servicii TIC și procese TIC stabiliți în diferite state membre;

   (g) discutarea și identificarea de noi forme de cooperare operațională, inclusiv în legătură cu:

      (i) categoriile de amenințări cibernetice și incidente;

      (ii) alertele timpurii;

      (iii) asistența reciprocă;

      (iv) principiile și modalitățile de coordonare, ca răspuns la riscuri și incidente transfrontaliere;

      (v) contribuția la planul național de răspuns la incidente și crize de securitate cibernetică menționat la articolul 7 alineatul (3);

   (h) informarea grupului de cooperare cu privire la activitățile sale și cu privire la noi forme de cooperare operațională discutate în temeiul literei (g) și, după caz, solicitarea de orientări în acest sens;

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

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

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

(l) discutarea rapoartelor privind evaluarea *inter pares* menționate la articolul 16 alineatul (7);

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

4. În scopul revizuirii menționate la articolul 35 și în termen de [24 de luni de la data intrării în vigoare a prezentei directive] și, ulterior, la fiecare doi ani, rețeaua CSIRT evaluează progresele înregistrate în ceea ce privește cooperarea operațională și întocmește un raport. Raportul formulează, în special, concluzii cu privire la rezultatele evaluărilor *inter pares* menționate la articolul 16, efectuate în legătură cu echipele CSIRT naționale, inclusiv concluzii și recomandări, în temeiul articolului respectiv. Raportul se transmite, de asemenea, grupului de cooperare.

5. Rețeaua CSIRT își adoptă propriul regulament de procedură.

Articolul 14

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

1. Pentru a sprijini gestionarea coordonată, la nivel operațional, a incidentelor și a crizelor de securitate cibernetică de mare amploare și pentru a asigura schimbul periodic de informații între statele membre și instituțiile, organele și agențiile Uniunii, se înființează Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (UE - CyCLONe).

2. UE - CyCLONe este formată din reprezentanți ai autorităților de gestionare a crizelor din statele membre desemnați în conformitate cu articolul 7, reprezentanți ai Comisiei și ai ENISA. ENISA asigură secretariatul rețelei și sprijină schimbul securizat de informații.

3. UE - CyCLONe are următoarele sarcini:

(a) consolidarea nivelului de pregătire pentru gestionarea incidentelor și a crizelor de mare amploare;

(b) dezvoltarea unei conștientizări comune a situației, în ceea ce privește evenimentele relevante în materie de securitate cibernetică;

(c) coordonarea gestionării incidentelor și a crizelor de mare amploare și sprijinirea procesului decizional la nivel politic în legătură cu astfel de incidente și crize;

(d) discutarea planurilor naționale de răspuns la incidente și crize în materie de securitate cibernetică menționate la articolul 7 alineatul (2).

4. UE-CyCLONe își adoptă regulamentul de procedură.

5. UE-CyCLONe prezintă periodic rapoarte grupului de cooperare cu privire la amenințările, incidentele și tendințele cibernetice, concentrându-se în special pe impactul acestora asupra entităților esențiale și importante.

6. UE-CyCLONe cooperează cu rețeaua CSIRT pe baza modalităților procedurale convenite.

Articolul 15

Raportul privind situația în materie de securitate cibernetică în Uniune

1. ENISA elaborează, în cooperare cu Comisia, un raport bienal privind situația în materie de securitate cibernetică în Uniune. Raportul include, în special, o evaluare a următoarelor elemente:

   (a) dezvoltarea capacităților în materie de securitate cibernetică în întreaga Uniune;

   (b) resursele tehnice, financiare și umane de care dispun autoritățile competente și politicile în materie de securitate cibernetică, precum și punerea în aplicare a măsurilor de supraveghere și a acțiunilor de asigurare a respectării legislației în lumina rezultatelor evaluărilor *inter pares* menționate la articolul 16;

   (c) un indice de securitate cibernetică care să prevadă o evaluare globală a nivelului de maturitate al capacităților în materie de securitate cibernetică.

2. Raportul include recomandări de politică specifice pentru îmbunătățirea nivelului de securitate cibernetică în întreaga Uniune și un rezumat al constatărilor pentru perioada respectivă incluse în rapoartele UE privind situația tehnică în materie de securitate cibernetică ale agenției, emise de ENISA în conformitate cu articolul 7 alineatul (6) din Regulamentul (UE) 2019/881.

Articolul 16

Evaluări *inter pares*

1. După consultarea grupului de cooperare și a ENISA și în termen de cel mult 18 luni de la intrarea în vigoare a prezentei directive, Comisia stabilește metodologia și conținutul unui sistem de evaluare *inter pares* pentru evaluarea eficacității politicilor de securitate cibernetică ale statelor membre. Evaluările sunt efectuate de experți tehnici în materie de securitate cibernetică din alte state membre decât cel care face obiectul evaluării și acoperă cel puțin următoarele elemente:

   (i) eficacitatea punerii în aplicare a cerințelor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare menționate la articolele 18 și 20;

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

   (iii) capacitățile operaționale și eficacitatea echipelor CSIRT;

   (iv) eficacitatea asistenței reciproce menționate la articolul 34;

   (v) eficacitatea cadrului privind schimbul de informații, menționat la articolul 26 din prezenta directivă.

2. Metodologia include criterii obiective, nediscriminatorii, echitabile și transparente pe baza cărora statele membre desemnează experți eligibili pentru efectuarea evaluărilor

inter pares. ENISA și Comisia desemnează experți care să participe în calitate de observatori la evaluările *inter pares*. Comisia, sprijinită de ENISA, stabilește, în cadrul metodologiei menționate la alineatul (1), un sistem obiectiv, nediscriminatoriu, echitabil și transparent de selecție și alocare aleatorie a experților pentru fiecare evaluare *inter pares*.

3. Aspectele organizatorice ale evaluărilor *inter pares* sunt decise de Comisie, cu sprijinul ENISA, și, în urma consultării grupului de cooperare, se bazează pe criteriile definite în metodologia menționată la alineatul (1). Evaluările *inter pares* analizează aspectele menționate la alineatul (1) pentru toate statele membre și toate sectoarele, inclusiv anumite aspecte specifice unuia sau mai multor state membre sau unuia sau mai multor sectoare.

4. Evaluările *inter pares* implică vizite la fața locului efective sau virtuale și schimburi *ex situ*. Având în vedere principiul bunei cooperări, statele membre care fac obiectul evaluării le furnizează experților desemnați informațiile solicitate necesare pentru analizarea aspectelor evaluate. Orice informație obținută prin intermediul procesului de evaluare *inter pares* este utilizată exclusiv în acest scop. Experții care participă la evaluarea *inter pares* nu divulgă terților nicio informație sensibilă sau confidențială obținută în cursul evaluării respective.

5. Odată evaluate într-un stat membru, aceleași aspecte nu fac obiectul unei noi evaluări *inter pares* în statul membru respectiv timp de doi ani de la încheierea evaluării *inter pares*, cu excepția cazului în care Comisia decide altfel, în urma consultării ENISA și a grupului de cooperare.

6. Statele membre se asigură că orice risc de conflict de interese în ceea ce privește experții desemnați este dezvăluit celorlalte state membre, Comisiei și ENISA fără întârzieri nejustificate.

7. Experții care participă la evaluări *inter pares* elaborează rapoarte cu privire la constatările și concluziile evaluărilor. Rapoartele sunt prezentate Comisiei, grupului de cooperare, rețelei CSIRT și ENISA. Rapoartele se discută în cadrul grupului de cooperare și al rețelei CSIRT. Rapoartele se pot publica pe site-ul web dedicat al grupului de cooperare.

CAPITOLUL IV

Gestionarea riscurilor în materie de securitate cibernetică și obligațiile de raportare

SECȚIUNEA I

Gestionarea și raportarea riscurilor în materie de securitate cibernetică

Articolul 17

Guvernanța

1. Statele membre se asigură că organele de conducere ale entităților esențiale și importante aprobă măsurile de gestionare a riscurilor în materie de securitate

cibernetică luate de entitățile respective pentru a se conforma articolului 18, supraveghează punerea în aplicare a acestora și sunt responsabile pentru nerespectarea de către entități a obligațiilor care le revin în temeiul prezentului articol.

2. Statele membre se asigură că membrii organului de conducere urmează, în mod regulat, cursuri de formare specifice pentru a dobândi suficiente cunoștințe și competențe în vederea identificării și a evaluării riscurilor și a practicilor de gestionare în materie de securitate cibernetică, precum și a impactului acestora asupra operațiunilor pe care le desfășoară entitatea.

Articolul 18

Măsuri de gestionare a riscurilor în materie de securitate cibernetică

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

2. Măsurile menționate la alineatul (1) includ cel puțin următoarele:

   (a) analiza riscurilor și politicile de securitate a sistemelor informatice;

   (b) administrarea incidentelor (prevenirea și detectarea incidentelor și răspunsul la acestea);

   (c) continuitatea activității și gestionarea crizelor;

   (d) securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile dintre fiecare entitate și prestatorii sau furnizorii săi de servicii, cum ar fi furnizorii de servicii de stocare și prelucrare a datelor sau de servicii de securitate gestionate;

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

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

   (g) utilizarea criptografiei și a criptării.

3. Statele membre se asigură că, atunci când au în vedere luarea măsurilor adecvate menționate la alineatul (2) litera (d), entitățile iau în considerare vulnerabilitățile specifice fiecărui prestator și furnizor de servicii, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale prestatorilor și furnizorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare.

4. Statele membre se asigură că, în cazul în care o entitate constată că serviciile sau sarcinile sale nu sunt în conformitate cu cerințele prevăzute la alineatul (2), aceasta ia, fără întârzieri nejustificate, toate măsurile corective necesare pentru a asigura conformitatea serviciului respectiv.

5. Comisia poate adopta acte de punere în aplicare pentru a stabili specificațiile tehnice și metodologice ale elementelor menționate la alineatul (2). Atunci când pregătește

actele respective, Comisia procedează în conformitate cu procedura de examinare menționată la articolul 37 alineatul (2) și urmează, în cea mai mare măsură posibilă, standardele internaționale și europene, precum și specificațiile tehnice relevante.

6. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 36 în vederea completării elementelor prevăzute la alineatul (2) pentru a ține seama de noi amenințări cibernetice, evoluții tehnologice sau specificități sectoriale.

Articolul 19

Evaluări coordonate la nivelul UE ale riscurilor legate de lanțurile de aprovizionare critice

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

2. Comisia, după consultarea grupului de cooperare și a ENISA, identifică serviciile, sistemele sau produsele TIC critice specifice care pot face obiectul evaluării coordonate a riscurilor menționate la alineatul (1).

Articolul 20

Obligații de raportare

1. Statele membre se asigură că entitățile esențiale și importante notifică, fără întârzieri nejustificate, autorităților competente sau CSIRT, în conformitate cu alineatele (3) și (4), orice incident care are un impact semnificativ asupra prestării serviciilor lor. Dacă este cazul, entitățile respective notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor incidentele care ar putea afecta în mod negativ prestarea serviciului respectiv. Statele membre se asigură că entitățile respective raportează, printre altele, orice informație care să le permită autorităților competente sau CSIRT să stabilească dacă incidentul are un impact transfrontalier.

2. Statele membre se asigură că entitățile esențiale și importante notifică, fără întârzieri nejustificate, autorităților competente sau CSIRT orice amenințare cibernetică semnificativă pe care entitățile respective o identifică și care ar fi putut duce la un incident semnificativ.

   Dacă este cazul, entitățile respective notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor care ar putea fi afectați de o amenințare cibernetică semnificativă măsurile sau măsurile corective pe care destinatarii respectivi le pot lua ca răspuns la amenințarea respectivă. Dacă este cazul, entitățile le notifică, de asemenea, destinatarilor în cauză amenințarea propriu-zisă. Notificarea nu expune entitatea notificatoare unei răspunderi sporite.

3. Un incident este considerat semnificativ dacă:

   (a) incidentul a provocat sau are potențialul de a provoca perturbări operaționale sau pierderi financiare substanțiale pentru entitatea în cauză;

(b) incidentul a afectat sau are potențialul de a afecta alte persoane fizice sau juridice, cauzând pierderi materiale sau morale considerabile.

4. Statele membre se asigură că, în scopul notificării prevăzute la alineatul (1), entitățile în cauză transmit autorităților competente sau CSIRT:

(a) fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care a luat cunoștință de incident, o notificare inițială care, după caz, indică dacă există suspiciuni că incidentul a fost cauzat de acțiuni ilegale sau răuvoitoare;

(b) la cererea unei autorități competente sau a unei CSIRT, un raport intermediar privind actualizarea relevantă a situației;

(c) un raport final, în termen de cel mult o lună de la prezentarea raportului menționat la litera (a), care să includă cel puțin următoarele elemente:

(i) o descriere detaliată a incidentului, a gravității și a impactului acestuia;

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

(iii) măsurile de atenuare aplicate și în curs.

Statele membre se asigură că, în cazuri justificate în mod corespunzător și în acord cu autoritățile competente sau cu CSIRT, entitatea în cauză se poate abate de la termenele prevăzute la literele (a) și (c).

5. Autoritățile naționale competente sau CSIRT furnizează, în termen de 24 de ore de la primirea notificării inițiale menționate la alineatul (4) litera (a), un răspuns entității notificatoare, inclusiv un feedback inițial cu privire la incident și, la cererea entității, orientări privind punerea în aplicare a unor eventuale măsuri de atenuare. În cazul în care CSIRT nu a primit notificarea menționată la alineatul (1), orientările sunt furnizate de autoritatea competentă în colaborare cu CSIRT. CSIRT furnizează sprijin tehnic suplimentar în cazul în care entitatea în cauză solicită acest lucru. În cazul în care se suspectează că incidentul este de natură penală, autoritățile naționale competente sau CSIRT furnizează, de asemenea, orientări privind raportarea incidentului către autoritățile de aplicare a legii.

6. După caz, mai ales dacă incidentul menționat la alineatul (1) implică două sau mai multe state membre, autoritatea competentă sau CSIRT informează celelalte state membre afectate și ENISA cu privire la incident. Astfel, autoritățile competente, echipele CSIRT și punctele unice de contact, în conformitate cu dreptul Uniunii sau cu legislația națională conformă cu dreptul Uniunii, protejează interesele de securitate și comerciale ale entității, precum și confidențialitatea informațiilor furnizate.

7. În cazul în care sensibilizarea publicului este necesară pentru a preveni un incident sau pentru a face față unui incident în curs sau în cazul în care divulgarea incidentului este în alt mod în interesul public, autoritatea competentă sau CSIRT și, după caz, autoritățile sau echipele CSIRT din alte state membre vizate pot, după consultarea entității în cauză, să informeze publicul cu privire la incident sau să solicite entității să facă acest lucru.

8. La cererea autorității competente sau a echipei CSIRT, punctul unic de contact transmite notificările primite în temeiul alineatelor (1) și (2) punctelor unice de contact din celelalte state membre afectate.

9. Punctul unic de contact transmite lunar ENISA un raport de sinteză care include date anonimizate și agregate privind incidentele, amenințările cibernetice semnificative și incidentele evitate la limită notificate în conformitate cu alineatele (1) și (2) și în conformitate cu articolul 27. Pentru a contribui la furnizarea de informații comparabile, ENISA poate emite orientări tehnice cu privire la parametrii informațiilor incluse în raportul de sinteză.

10. Autoritățile competente furnizează autorităților competente desemnate în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] informații cu privire la incidentele și amenințările cibernetice notificate în conformitate cu alineatele (1) și (2) de către entitățile esențiale identificate ca fiind entități critice sau entități echivalente cu entitățile critice, în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice].

11. Comisia poate adopta acte de punere în aplicare pentru a preciza mai în detaliu tipul de informații, formatul și procedura referitoare la o notificare transmisă în temeiul alineatelor (1) și (2). Comisia poate adopta, de asemenea, acte de punere în aplicare pentru a preciza mai în detaliu cazurile în care un incident este considerat semnificativ, astfel cum se menționează la alineatul (3). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 37 alineatul (2).

Articolul 21

Utilizarea sistemelor europene de certificare a securității cibernetice

1. Pentru a demonstra conformitatea cu anumite cerințe de la articolul 18, statele membre le pot solicita entităților esențiale și importante să certifice anumite produse TIC, servicii TIC și procese TIC în cadrul sistemelor europene de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881. Produsele, serviciile și procesele care fac obiectul certificării pot fi elaborate de o entitate esențială sau importantă sau achiziționate de la terți.

2. Comisia este împuternicită să adopte acte delegate pentru a preciza ce categorii de entități esențiale au obligația de a obține un certificat și în cadrul căror sisteme europene specifice de certificare a securității cibernetice în temeiul alineatului (1). Actele delegate se adoptă în conformitate cu articolul 36.

3. Comisia poate solicita ENISA să pregătească o propunere de sistem în temeiul articolului 48 alineatul (2) din Regulamentul (UE) 2019/881 în cazurile în care nu este disponibil niciun sistem european adecvat de certificare a securității cibernetice în sensul alineatului (2).

Articolul 22
Standardizarea

1. Pentru promovarea punerii în aplicare convergente a articolului 18 alineatele (1) și (2), statele membre, fără a impune sau a crea discriminare în favoarea utilizării unui

anumit tip de tehnologie, încurajează utilizarea standardelor și a 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 23

Bazele de date cu numele de domenii și datele de înregistrare

1. Pentru a contribui la securitatea, stabilitatea și reziliența DNS, statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD colectează și mențin date exacte și complete privind înregistrarea numelor de domenii într-o bază de date dedicată, cu diligența necesară, sub rezerva legislației Uniunii în materie de protecție a datelor î cu caracter personal.

2. Statele membre se asigură că bazele de date cu datele de înregistrare a numelor de domenii menționate la alineatul (1) conțin informații relevante pentru identificarea și contactarea titularilor numelor de domenii și a punctelor de contact care administrează numele de domenii în cadrul TLD-urilor.

3. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD dispun de politici și proceduri care să asigure că bazele de date conțin informații exacte și complete. Statele membre se asigură că aceste politici și proceduri sunt puse la dispoziția publicului.

4. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD publică, fără întârzieri nejustificate după înregistrarea unui nume de domeniu, date de înregistrare a domeniului care nu sunt date cu caracter personal.

5. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD oferă acces la datele de înregistrare a numelor de domenii specifice în baza unor cereri legale și justificate în mod corespunzător ale solicitanților de acces legitimi, în conformitate cu legislația Uniunii în materie de protecție a datelor. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD răspund fără întârzieri nejustificate la toate cererile de acces. Statele membre se asigură că politicile și procedurile de divulgare a unor astfel de date sunt puse la dispoziția publicului.

Secțiunea II

Jurisdicție și înregistrare

Articolul 24

Jurisdicție și teritorialitate

1. Se consideră că furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date și furnizorii de rețele de furnizare de conținut menționați la punctul 8 din anexa I, precum și furnizorii digitali menționați la punctul 6 din anexa II se află sub jurisdicția statului membru în care își au sediul principal din Uniune.

2. În sensul prezentei directive, se consideră că entitățile menționate la alineatul (1) își au sediul principal din Uniune în statul membru în care se iau deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică. În cazul în care astfel de decizii nu se iau în niciun sediu din Uniune, se consideră că sediul principal este în statul membru în care entitățile au sediul cu cel mai mare număr de angajați din Uniune.

3. În cazul în care o entitate menționată la alineatul (1) nu este stabilită în Uniune, dar oferă servicii în Uniune, aceasta desemnează un reprezentant în Uniune. Reprezentantul se stabilește în unul dintre statele membre în care se oferă serviciile. O astfel de entitate se consideră sub jurisdicția statului membru în care este stabilit reprezentantul. În absența unui reprezentant desemnat în Uniune în temeiul prezentului articol, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității pentru nerespectarea obligațiilor care îi revin în temeiul prezentei directive.

4. Desemnarea unui reprezentant de către o entitate menționată la alineatul (1) nu aduce atingere acțiunilor în justiție care ar putea fi inițiate împotriva entității înseși.

Articolul 25

Registrul entităților esențiale și importante

1. ENISA creează și ține un registru al entităților esențiale și importante menționate la articolul 24 alineatul (1). Entitățile transmit ENISA următoarele informații până la [cel târziu 12 luni de la intrarea în vigoare a directivei]:

   (a) denumirea entității;

   (b) adresa sediului său principal și a celorlalte sedii legale ale sale din Uniune sau, dacă nu este stabilită în Uniune, adresa reprezentantului său desemnat în temeiul articolului 24 alineatul (3);

   (c) datele de contact actualizate, inclusiv adresele de e-mail și numerele de telefon ale entităților.

2. Entitățile menționate la alineatul (1) notifică ENISA fără întârziere și, în orice caz, în termen de trei luni de la data la care a intrat în vigoare modificarea, cu privire la orice modificare a datelor pe care le-au transmis în temeiul alineatului (1).

3. La primirea informațiilor prevăzute la alineatul (1), ENISA le transmite punctelor unice de contact, în funcție de locația indicată a sediului principal al fiecărei entități

sau, în cazul în care nu este stabilită în Uniune, a reprezentantului desemnat al acesteia. În cazul în care o entitate menționată la alineatul (1) are, pe lângă sediul său principal din Uniune, alte sedii în alte state membre, ENISA informează, de asemenea, punctele unice de contact ale statelor membre respective.

4. În cazul în care o entitate nu își înregistrează activitatea sau nu furnizează informațiile relevante în termenul prevăzut la alineatul (1), orice stat membru în care entitatea prestează servicii este competent să asigure respectarea de către entitatea respectivă a obligațiilor prevăzute în prezenta directivă.

CAPITOLUL V

Schimbul de informații

Articolul 26

Acorduri privind schimbul de informații în materie de securitate cibernetică

1. Fără a aduce atingere Regulamentului (UE) 2016/679, statele membre se asigură că entitățile esențiale și importante pot face schimb reciproc de informații relevante în materie de securitate cibernetică, inclusiv de informații referitoare la amenințări cibernetice, vulnerabilități, indicatori de compromis, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, în cazul în care un astfel de schimb de informații:

   (a) vizează prevenirea și detectarea incidentelor, răspunsul la incidente sau atenuarea acestora;

   (b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea răspândirii amenințărilor cibernetice, sprijinirea gamei de capacități defensive, remedierea și divulgarea vulnerabilităților, tehnicile de detectare a amenințărilor, strategiile de atenuare sau etapele proceselor de răspuns și de recuperare.

2. Statele membre se asigură că schimbul de informații are loc în cadrul unor comunități de încredere ale entităților esențiale și importante. Un astfel de schimb este pus în aplicare prin acorduri privind schimbul de informații, ținând seama de caracterul potențial sensibil al informațiilor partajate și în conformitate cu normele din dreptul Uniunii menționate la alineatul (1).

3. Statele membre stabilesc norme care să specifice procedura, elementele operaționale (inclusiv utilizarea platformelor TIC dedicate), conținutul și condițiile acordurilor privind schimbul de informații menționate la alineatul (2). Aceste norme stabilesc, de asemenea, detaliile implicării autorităților publice în astfel de acorduri, precum și elementele operaționale, inclusiv utilizarea platformelor informatice dedicate. Statele membre oferă sprijin pentru aplicarea unor astfel de acorduri în conformitate cu politicile lor menționate la articolul 5 alineatul (2) litera (g).

4. Entitățile esențiale și importante informează autoritățile competente cu privire la participarea lor la acordurile privind schimbul de informații menționate la alineatul (2), odată cu încheierea unor astfel de acorduri sau, după caz, cu retragerea din astfel de acorduri, după ce retragerea intră în vigoare.

5. În conformitate cu dreptul Uniunii, ENISA sprijină instituirea acordurilor privind schimbul de informații în materie de securitate cibernetică menționate la alineatul (2) oferind bune practici și orientări.

Articolul 27

Notificarea voluntară a informațiilor relevante

Statele membre se asigură că, fără a aduce atingere articolului 3, entitățile care nu intră în domeniul de aplicare al prezentei directive pot transmite notificări, în mod voluntar, cu privire la incidente semnificative, amenințări cibernetice sau incidente evitate la limită. Atunci când tratează notificările, statele membre acționează în conformitate cu procedura prevăzută la articolul 20. Statele membre pot trata notificările obligatorii cu prioritate față de notificările voluntare. Notificarea voluntară nu impune entității raportoare nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis notificarea.

CAPITOLUL VI

Supravegherea și asigurarea respectării legislației

Articolul 28

Aspecte generale privind supravegherea și asigurarea respectării legislației

1. Statele membre se asigură că autoritățile competente monitorizează în mod eficace și iau măsurile necesare pentru a asigura respectarea prezentei directive, în special a obligațiilor prevăzute la articolele 18 și 20.
2. Autoritățile competente lucrează în strânsă cooperare cu autoritățile de protecție a datelor în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal.

Articolul 29

Supravegherea și asigurarea respectării legislației pentru entitățile esențiale

1. Statele membre se asigură că măsurile de supraveghere sau de asigurare a respectării legislației impuse entităților esențiale în ceea ce privește obligațiile prevăzute în prezenta directivă sunt eficace, proporționale și disuasive, ținând seama de circumstanțele fiecărui caz în parte.
2. Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile esențiale, au competența de a supune entitățile respective:
   (a) unor inspecții la fața locului și unei supravegheri *ex situ*, inclusiv unor verificări aleatorii;
   (b) unor audituri periodice;
   (c) unor audituri de securitate specifice bazate pe evaluări ale riscurilor sau pe informații disponibile legate de riscuri;

(d) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor;

(e) unor cereri de informații necesare pentru a evalua măsurile de securitate cibernetică adoptate de entitate, inclusiv politicile de securitate cibernetică documentate, precum și respectarea obligației de notificare a ENISA în temeiul articolului 25 alineatele (1) și (2);

(f) unor cereri de acces la date, la documente sau la toate informațiile necesare pentru îndeplinirea sarcinilor lor de supraveghere;

(g) unor cereri de dovezi privind punerea în aplicare a politicilor în materie de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și elementele de probă care stau la baza acestora.

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

4. Statele membre se asigură că, atunci când își exercită sarcinile de asigurare a respectării legislației în ceea ce privește entitățile esențiale, autoritățile competente au competența:

(a) de a emite avertismente cu privire la nerespectarea de către entități a obligațiilor prevăzute în prezenta directivă;

(b) de a emite instrucțiuni obligatorii sau un ordin prin care le solicită acestor entități să remedieze deficiențele identificate sau încălcările obligațiilor prevăzute în prezenta directivă;

(c) de a dispune ca entitățile respective să înceteze comportamentul care nu respectă obligațiile prevăzute în prezenta directivă și să se abțină de la repetarea comportamentului respectiv;

(d) de a dispune ca entitățile respective să asigure conformitatea măsurilor lor de gestionare a riscurilor și/sau a obligațiilor lor de raportare cu obligațiile prevăzute la articolele 18 și 20 într-un anumit mod și într-o anumită perioadă;

(e) de a dispune ca entitățile respective să informeze persoana (persoanele) fizică (fizice) sau juridică (juridice) căreia (cărora) îi (le) furnizează servicii sau activități care sunt potențial afectate de o amenințare cibernetică semnificativă cu privire la toate măsurile de protecție sau de remediere pe care le-ar putea lua persoana (persoanele) fizică (fizice) sau juridică (juridice) în cauză ca răspuns la amenințarea respectivă;

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

(g) de a desemna un ofițer de monitorizare cu sarcini bine definite pe o perioadă determinată de timp pentru a supraveghea respectarea obligațiilor care le revin în temeiul articolelor 18 și 20;

(h) de a dispune ca entitățile respective să facă publice într-un mod specific aspectele legate de nerespectarea obligațiilor prevăzute în prezenta directivă;

(i) de a face o declarație publică în care identifică persoana (persoanele) juridică (juridice) și fizică (fizice) responsabilă (responsabile) pentru încălcarea unei obligații prevăzute în prezenta directivă și natura încălcării respective;

(j) de a impune sau a solicita impunerea de către organismele sau instanțele relevante, în conformitate cu legislația națională, a unei amenzi administrative în temeiul articolului 31, în plus față de măsurile menționate la literele (a)-(i) de la prezentul alineat sau în locul acestora, în funcție de circumstanțele fiecărui caz în parte.

5. În cazul în care măsurile de asigurare a respectării legislației adoptate în temeiul alineatului (4) literele (a)-(d) și (f) se dovedesc ineficiente, statele membre se asigură că autoritățile competente au competența de a stabili un termen în care entității esențiale i se solicită să ia măsurile necesare pentru remedierea deficiențelor sau să respecte cerințele autorităților respective. În cazul în care acțiunea solicitată nu este întreprinsă în termenul stabilit, statele membre se asigură că autoritățile competente au competența:

(a) să suspende sau să solicite unui organism de certificare sau de autorizare suspendarea unei certificări sau a unei autorizații privind o parte sau toate serviciile sau activitățile furnizate de o entitate esențială;

(b) să impună sau să solicite impunerea de către organismele sau instanțele relevante, în conformitate cu legislația națională, a unei interdicții temporare de a exercita funcții de conducere în cadrul entității respective împotriva oricărei persoane care exercită responsabilități de conducere la nivel de director executiv sau de reprezentant legal în entitatea esențială respectivă, precum și împotriva oricărei alte persoane fizice declarate responsabilă de încălcare.

Aceste sancțiuni se aplică numai până în momentul în care entitatea ia măsurile necesare în vederea remedierii deficiențelor sau a respectării cerințelor impuse de autoritatea competentă în temeiul cărora au fost aplicate aceste sancțiuni.

6. Statele membre se asigură că orice persoană fizică responsabilă de o entitate esențială sau care acționează în calitate de reprezentant al acestei entități pe baza competenței de a o reprezenta, a autorității de a lua decizii în numele acesteia sau a autorității de a exercita controlul asupra acesteia are competența de a se asigura că aceasta respectă obligațiile prevăzute în prezenta directivă. Statele membre se asigură că aceste persoane fizice pot fi trase la răspundere pentru încălcarea obligațiilor care le revin de a asigura respectarea obligațiilor prevăzute în prezenta directivă.

7. Atunci când iau măsuri de asigurare a respectării legislației sau aplică sancțiuni în temeiul alineatelor (4) și (5), autoritățile competente respectă dreptul la apărare, iau în considerare circumstanțele fiecărui caz în parte și țin seama în mod corespunzător cel puțin de:

(a) gravitatea încălcării și importanța dispozițiilor încălcate. Printre încălcările care ar trebui considerate grave se numără: încălcări repetate, neîndeplinirea obligației de notificare sau de remediere a incidentelor cu un efect perturbator semnificativ, neremedierea deficiențelor în urma instrucțiunilor obligatorii din partea autorităților competente, obstrucționarea auditurilor sau a activităților de monitorizare dispuse de autoritatea competentă în urma constatării unei încălcări, furnizarea de informații false sau vădit denaturate în ceea ce privește cerințele de gestionare a riscurilor sau obligațiile de raportare prevăzute la articolele 18 și 20.

(b) durata încălcării, inclusiv caracterul repetitiv al încălcărilor;

(c) daunele reale cauzate sau pierderile suferite ori daunele sau pierderile potențiale care ar fi putut fi cauzate, în măsura în care acestea pot fi

determinate. La evaluarea acestui aspect, se ține seama, printre altele, de pierderile financiare sau economice reale sau potențiale, de efectele asupra altor servicii și de numărul de utilizatori afectați sau potențial afectați;

(d) caracterul încălcării (intenționat sau din neglijență);

(e) măsurile luate de entitate pentru a preveni sau a atenua daunele și/sau pierderile;

(f) aderarea la coduri de conduită aprobate sau la mecanisme de certificare aprobate;

(g) nivelul de cooperare al persoanei (persoanelor) fizice sau juridice considerate responsabile cu autoritățile competente.

8. Autoritățile competente prezintă o motivare detaliată a deciziilor lor de asigurare a respectării legislației. Înainte de a lua astfel de decizii, autoritățile competente notifică entităților în cauză constatările lor preliminare și acordă entităților respective un termen rezonabil pentru prezentarea observațiilor.

9. Statele membre se asigură că autoritățile lor competente informează autoritățile competente relevante din statul membru în cauză desemnate în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] atunci când își exercită competențele de supraveghere și de asigurare a respectării legislației menite să asigure conformitatea unei entități esențiale identificate ca fiind critică sau ca fiind o entitate echivalentă cu o entitate critică, în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] cu obligațiile care decurg din prezenta directivă. La cererea autorităților competente în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice], autoritățile competente își pot exercita competențele de supraveghere și de asigurare a respectării legislației cu privire la o entitate esențială identificată ca fiind critică sau ca fiind o entitate echivalentă cu o entitate critică.

Articolul 30

Supravegherea și asigurarea respectării legislației pentru entitățile importante

1. Atunci când li se furnizează dovezi sau indicii că o entitate importantă nu respectă obligațiile prevăzute în prezenta directivă, în special la articolele 18 și 20, statele membre se asigură că autoritățile competente iau măsuri, dacă este necesar, prin intermediul unor măsuri de supraveghere *ex post*.

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

(a) unor inspecții la fața locului și unei supravegheri *ex situ ex post*;

(b) unor audituri de securitate specifice bazate pe evaluări ale riscurilor sau pe informații disponibile legate de riscuri;

(c) unor scanări de securitate bazate pe criterii obiective, echitabile și transparente de evaluare a riscurilor;

(d) unor cereri de informații necesare pentru a evalua *ex post* măsurile de securitate cibernetică, inclusiv politicile de securitate cibernetică documentate, precum și

respectarea obligației de notificare a ENISA în temeiul articolului 25 alineatele (1) și (2);

(e) unor cereri de acces la date, la documente și/sau la informații necesare pentru îndeplinirea sarcinilor de supraveghere;

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

4. Statele membre se asigură că, atunci când își exercită sarcinile de asigurare a respectării legislației în ceea ce privește entitățile importante, autoritățile competente au competența:

(a) de a emite avertismente cu privire la nerespectarea de către entități a obligațiilor prevăzute în prezenta directivă;

(b) de a emite instrucțiuni obligatorii sau un ordin prin care le solicită acestor entități să remedieze deficiențele identificate sau încălcarea obligațiilor prevăzute în prezenta directivă;

(c) de a dispune ca entitățile respective să înceteze comportamentul care nu respectă obligațiile prevăzute în prezenta directivă și să se abțină de la repetarea comportamentului respectiv;

(d) de a dispune ca entitățile respective să asigure conformitatea măsurilor lor de gestionare a riscurilor sau a obligațiilor lor de raportare cu obligațiile prevăzute la articolele 18 și 20 într-un anumit mod și într-o anumită perioadă;

(e) de a dispune ca entitățile respective să informeze persoana (persoanele) fizică (fizice) sau juridică (juridice) căreia (cărora) îi (le) furnizează servicii sau activități care sunt potențial afectate de o amenințare cibernetică semnificativă cu privire la toate măsurile de protecție sau de remediere pe care le-ar putea lua persoana (persoanele) fizică (fizice) sau juridică (juridice) în cauză ca răspuns la amenințarea respectivă;

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

(g) de a dispune ca entitățile respective să facă publice într-un mod specificat aspectele legate de nerespectarea obligațiilor lor prevăzute în prezenta directivă;

(h) de a face o declarație publică în care identifică persoana (persoanele) juridică (juridice) și fizică (fizice) responsabilă (responsabile) pentru încălcarea unei obligații prevăzute în prezenta directivă și natura încălcării respective;

(i) de a impune sau a solicita impunerea de către organismele sau instanțele relevante, în conformitate cu legislația națională, a unei amenzi administrative în temeiul articolului 31, în plus față de măsurile menționate la literele (a)-(h) de la prezentul alineat sau în locul acestora, în funcție de circumstanțele fiecărui caz în parte.

5. Articolul 29 alineatele (6)-(8) se aplică, de asemenea, măsurilor de supraveghere și de asigurare a respectării legislației prevăzute în prezentul articol pentru entitățile importante enumerate în anexa II.

Articolul 31

Condiții generale pentru impunerea de amenzi administrative entităților esențiale și importante

1. Statele membre se asigură că impunerea de amenzi administrative entităților esențiale și importante în temeiul prezentului articol pentru încălcări ale obligațiilor prevăzute în prezenta directivă este, în fiecare caz în parte, eficace, proporțională și disuasivă.

2. În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate la articolul 29 alineatul (4) literele (a)-(i), la articolul 29 alineatul (5) și la articolul 30 alineatul (4) literele (a)-(h).

3. Atunci când se ia decizia de a impune o amendă administrativă și se decide cuantumul acesteia în fiecare caz în parte, se acordă atenția cuvenită, cel puțin, elementelor prevăzute la articolul 29 alineatul (7).

4. Statele membre se asigură că încălcările obligațiilor prevăzute la articolul 18 sau la articolul 20 fac obiectul, în conformitate cu alineatele (2) și (3) din prezentul articol, unor amenzi administrative maxime de cel puțin 10 000 000 EUR sau de 2 % din cifra de afaceri mondială totală anuală a întreprinderii căreia îi aparține entitatea esențială sau importantă în exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare.

5. Statele membre pot prevedea competența de a impune penalități cu titlu cominatoriu pentru a obliga o entitate esențială sau importantă să înceteze o încălcare în conformitate cu o decizie prealabilă a autorității competente.

6. Fără a aduce atingere competențelor autorităților competente menționate la articolele 29 și 30, fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative entităților administrației publice menționate la articolul 4 punctul (23), sub rezerva obligațiilor prevăzute în prezenta directivă.

Articolul 32

Încălcări care implică o încălcare a securității datelor cu caracter personal

1. În cazul în care autoritățile competente au indicii că încălcarea de către o entitate esențială sau importantă a obligațiilor prevăzute la articolele 18 și 20 atrage după sine o încălcare a securității datelor cu caracter personal, astfel cum este definită la articolul 4 alineatul (12) din Regulamentul (UE) nr. 2016/679, care este notificată în temeiul articolului 33 din regulamentul respectiv, acestea informează într-un termen rezonabil autoritățile de supraveghere competente în temeiul articolelor 55 și 56 din regulamentul respectiv.

2. În cazul în care autoritățile de supraveghere competente în conformitate cu articolele 55 și 56 din Regulamentul (UE) 2016/679 decid să își exercite competențele în temeiul articolului 58 litera (i) din regulamentul respectiv și să impună o amendă administrativă, autoritățile competente nu impun o amendă administrativă pentru aceeași încălcare în temeiul articolului 31 din prezenta directivă. Cu toate acestea, autoritățile competente pot aplica acțiuni de asigurare a

respectării legislației sau pot exercita competențele de sancționare prevăzute la articolul 29 alineatul (4) literele (a)-(i), la articolul 29 alineatul (5) și la articolul 30 alineatul (4) literele (a)-(h) din prezenta directivă.

3. În cazul în care autoritatea de supraveghere competentă în temeiul Regulamentului (UE) 2016/679 este stabilită într-un alt stat membru decât autoritatea competentă, aceasta din urmă poate informa autoritatea de supraveghere stabilită în același stat membru.

Articolul 33

Sancțiuni

1. 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.

2. În termen de [doi] ani de la intrarea în vigoare a prezentei directive, statele membre notifică Comisiei normele și măsurile respective, precum și, fără întârzieri nejustificate, orice modificare ulterioară a acestora.

Articolul 34

Asistență reciprocă

1. Dacă o entitate esențială sau importantă furnizează servicii în mai multe state membre sau are sediul principal ori 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 un alt sediu ori reprezentantul și autoritățile competente ale acelor alte state membre cooperează și își oferă asistență reciprocă, după caz. Această cooperare implică cel puțin următoarele:

   (a) autoritățile competente care aplică măsuri de supraveghere sau de asigurare a respectării legislației într-un stat membru informează și consultă, prin intermediul punctului unic de contact, autoritățile competente din celelalte state membre în cauză cu privire la măsurile de supraveghere și de asigurare a respectării legislației luate și la acțiunile subsecvente acestora, în conformitate cu articolele 29 și 30;

   (b) o autoritate competentă poate solicita unei alte autorități competente să ia măsurile de supraveghere sau de asigurare a respectării legislației menționate la articolele 29 și 30;

   (c) la primirea unei cereri justificate din partea altei autorități competente, o autoritate competentă acordă asistență celeilalte autorități competente, astfel încât acțiunile de supraveghere sau de asigurare a respectării legislației menționate la articolele 29 și 30 să poată fi puse în aplicare într-un mod eficace, eficient și consecvent. O astfel de asistență reciprocă poate acoperi cererile de informații și măsurile de supraveghere, inclusiv cererile de efectuare a unor inspecții la fața locului, a unei supravegheri *ex situ* sau a unor audituri

de securitate specifice. O autoritate competentă căreia i se adresează o cerere de asistență nu poate refuza cererea respectivă, cu excepția cazului în care, în urma unui schimb cu celelalte autorități în cauză, cu ENISA și cu Comisia, se stabilește că fie autoritatea nu are competența de a furniza asistența solicitată, fie asistența solicitată nu este proporțională cu sarcinile de supraveghere ale autorității competente desfășurate în conformitate cu articolul 29 sau cu articolul 30.

2. Dacă este cazul și de comun acord, autoritățile competente din diferite state membre pot desfășura acțiunile comune de supraveghere menționate la articolele 29 și 30.

CAPITOLUL VII

Dispoziții tranzitorii și finale

Articolul 35

Revizuirea

Comisia revizuiește periodic funcționarea prezentei directive și prezintă un raport Parlamentului European și Consiliului. Raportul evaluează în special relevanța sectoarelor, a subsectoarelor, a dimensiunii și a tipului de entități menționate în anexele I și II pentru funcționarea economiei și a societății în ceea ce privește securitatea cibernetică. În acest scop și în vederea intensificării cooperării strategice și operaționale, Comisia ține cont de rapoartele grupului de cooperare și ale rețelei CSIRT privind experiența obținută la nivel strategic și operațional. Primul raport se transmite până la… [54 de luni de la data intrării în vigoare a prezentei directive].

Articolul 36

Exercitarea delegării

1. Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

2. Competența de a adopta acte delegate menționată la articolul 18 alineatul (6) și la articolul 21 alineatul (2) se conferă Comisiei pentru o perioadă de cinci ani de la […]

3. Delegarea de competențe menționată la articolul 18 alineatul (6) și la articolul 21 alineatul (2) poate fi revocată în orice moment de Parlamentul European sau de Consiliu. Decizia de revocare pune capăt delegării competenței menționate în decizia respectivă. Aceasta produce efecte începând cu ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene* sau la o dată ulterioară specificată în decizie. Aceasta nu aduce atingere valabilității actelor delegate aflate deja în vigoare.

4. Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

5. De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

6. Un act delegat adoptat în temeiul articolului 18 alineatul (6) și al articolului 21 alineatul (2) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 37

Procedura comitetului

1. Comisia este asistată de un comitet. Comitetul respectiv este un comitet în sensul Regulamentului (UE) nr. 182/2011.
2. În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.
3. În cazul în care avizul comitetului urmează să fie obținut prin procedură scrisă, respectiva procedură se încheie fără rezultat atunci când, în termenul stabilit pentru emiterea avizului, președintele comitetului decide în acest sens sau un membru al comitetului solicită acest lucru.

Articolul 38

Transpunerea

1. Statele membre adoptă și publică, în termen de … [18 luni de la data intrării în vigoare a prezentei directive], actele cu putere de lege și actele administrative necesare pentru a se conforma prezentei directive. Statele membre informează de îndată Comisia cu privire la aceasta. Statele membre aplică măsurile respective începând cu … [ziua următoare datei menționate la primul paragraf].
2. Atunci când statele membre adoptă dispozițiile respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a unei astfel de trimiteri.

Articolul 39

Modificarea Regulamentului (UE) nr. 910/2014

Articolul 19 din Regulamentul (UE) nr. 910/2014 se elimină.

Articolul 40

Modificarea Directivei (UE) 2018/1972

Articolele 40 și 41 din Directiva (UE) 2018/1972 se elimină.

Articolul 41

Abrogare

Directiva (UE) 2016/1148 se abrogă cu efect de la... [data termenului de transpunere a directivei].

Trimiterile la Directiva (UE) 2016/1148 se interpretează ca trimiteri la prezenta directivă și se citesc în conformitate cu tabelul de corespondență din anexa III.

Articolul 42

Intrarea în vigoare

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

Articolul 43

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*

FIȘĂ FINANCIARĂ LEGISLATIVĂ

Cuprins

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

Propunere de directivă privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148

1.2. Domeniul (domeniile) de politică vizat(e) (*clusterul de programe*)

Rețele de comunicații, conținut și tehnologie

1.3. Obiectul propunerii/inițiativei:

☐ **o nouă acțiune**

☐ **o acțiune nouă întreprinsă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[40]

☒ **prelungirea unei acțiuni existente**

☐ **o fuziune sau o redirecționare a uneia sau mai multor acțiuni către o altă/o nouă acțiune**

1.4. Motivele propunerii/inițiativei

1.4.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei

Obiectivul revizuirii este de a spori nivelul de reziliență cibernetică a unui set cuprinzător de întreprinderi care își desfășoară activitatea în Uniunea Europeană în toate sectoarele relevante, de a reduce inconsecvențele în ceea ce privește reziliența pe piața internă în sectoarele care fac deja obiectul directivei și de a îmbunătăți nivelul de conștientizare comună a situației și capacitatea colectivă de a se pregăti și de a răspunde.

1.4.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu mai buna coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii” este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

Reziliența în materie de securitate cibernetică în întreaga Uniune nu poate fi eficace dacă este abordată într-un mod disparat prin fragmentări naționale sau regionale. Directiva NIS a ajuns să abordeze această deficiență prin stabilirea unui cadru pentru securitatea rețelelor și a sistemelor informatice la nivel național și la nivelul Uniunii. Cu toate acestea, prima revizuire periodică a Directivei NIS a evidențiat o serie de deficiențe inerente, care au condus în cele din urmă la diferențe considerabile între statele membre în ceea ce privește capacitățile, planificarea și nivelul de protecție, care afectează, în același timp, condițiile de concurență echitabile pentru întreprinderile similare de pe piața internă.

Intervenția UE, care depășește măsurile actuale prevăzute în Directiva NIS, este justificată în principal de: (i) caracterul transfrontalier al problemei; (ii) potențialul acțiunii UE de îmbunătățire și de facilitare a unor politici naționale eficace;

[40] Astfel cum se menționează la articolul 58 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

(iii) contribuția acțiunilor politice concertate și colaborative NIS la protejarea eficace a protecției datelor și a vieții private.

Prin urmare, obiectivele declarate pot fi realizate mai bine prin acțiuni la nivelul UE decât prin acțiuni individuale ale statelor membre.

1.4.3. Învățăminte desprinse din experiențele anterioare similare

Directiva NIS este primul instrument orizontal al pieței interne care vizează îmbunătățirea rezilienței rețelelor și a sistemelor din Uniune la riscurile de securitate cibernetică. Aceasta a contribuit deja în mare măsură la creșterea nivelului comun de securitate cibernetică în rândul statelor membre. Cu toate acestea, revizuirea funcționării și a punerii în aplicare a directivei a evidențiat o serie de deficiențe care, pe lângă digitalizarea în creștere și necesitatea unui răspuns mai actualizat, trebuie abordate într-un act juridic revizuit.

1.4.4. Compatibilitatea și posibila sinergie cu alte instrumente corespunzătoare

Noua propunere este pe deplin consecventă și coerentă cu alte inițiative conexe, cum ar fi Propunerea de regulament privind reziliența operațională digitală a sectorului financiar („DORA”) și Propunerea de directivă privind reziliența operatorilor critici de servicii esențiale. Prezenta propunere este, de asemenea, în concordanță cu Codul european al comunicațiilor electronice, cu Regulamentul general privind protecția datelor și cu Regulamentul e-IDAS.

Propunerea este o parte esențială a Strategiei UE privind o uniune a securității.

1.5. Durata și impactul financiar

☐ **durată limitată**

– ☐ de la [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ impactul financiar din AAAA până în AAAA pentru creditele de angajament și din AAAA până în AAAA pentru creditele de plată

☒ **durată nelimitată**

– Punere în aplicare cu o perioadă de creștere în intensitate din 2022 până în 2025,

– urmată de o perioadă de funcționare la capacitate maximă.

1.6. Modul (modurile) de gestionare preconizat(e)[41]

Gestiune directă asigurată de către Comisie

– ☒ prin intermediul departamentelor sale, inclusiv al personalului din delegațiile Uniunii;

– ☐ prin intermediul agențiilor executive

☐ **Gestiune partajată** cu statele membre

☐ **Gestiune indirectă**, cu delegarea sarcinilor de execuție bugetară:

– ☐ țărilor terțe sau organismelor pe care le-au desemnat acestea;

– ☐ organizațiilor internaționale și agențiilor acestora (a se preciza);

– ☐ BEI și Fondului European de Investiții;

– X☐ organismelor menționate la articolele 70 și 71 din Regulamentul financiar;

– ☐ organismelor de drept public;

– ☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să prezinte garanții financiare adecvate;

– ☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și care prezintă garanții financiare adecvate;

– ☐ persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, și care sunt identificate în actul de bază relevant.

– *Dacă se indică mai multe moduri de gestiune, a se furniza detalii suplimentare în secțiunea „Observații”.*

Observații

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, căreia i s-a acordat un nou mandat permanent prin Regulamentul privind securitatea cibernetică, ar urma să sprijine statele membre și Comisia în punerea în aplicare a Directivei NIS revizuite.

Ca urmare a revizuirii Directivei NIS, începând cu 2022/2023, ENISA va avea domenii de acțiune suplimentare. Deși aceste domenii de acțiune ar fi acoperite de atribuțiile generale ale ENISA conform mandatului său, ele vor genera un volum de muncă suplimentar pentru

[41] Explicații detaliate privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

agenție. Mai precis, pe lângă domeniile sale de acțiune actuale, în temeiul propunerii Comisiei de revizuire a Directivei NIS, ENISA va trebui, de asemenea, să includă în mod specific în programul său de lucru, printre altele, următoarele acțiuni: (i) elaborarea și menținerea unui registru european al vulnerabilităților [articolul 6 alineatul (2) din propunere], (ii) asigurarea secretariatului Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (CyCLONe) (articolul 14 din propunere) și publicarea unui raport anual privind situația în materie de securitate cibernetică în UE (articolul 15 din propunere), (iii) sprijinirea organizării de evaluări *inter pares* între statele membre (articolul 16 din propunere), (iv) colectarea de date agregate privind incidentele de la statele membre și emiterea unor orientări tehnice [articolul 20 alineatul (9) din propunere], (v) crearea și menținerea unui registru pentru entitățile care furnizează servicii transfrontaliere (articolul 25 din propunere).

Prin urmare, se va face o cerere de 5 ENI suplimentare începând cu 2022, cu bugetul corespunzător de aproximativ 0,61 milioane EUR pe an, pentru a acoperi aceste noi posturi (a se vedea Fișa financiară separată pentru agenții).

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile aferente monitorizării și raportării.

Comisia va revizui periodic funcționarea directivei și va prezenta un raport Parlamentului European și Consiliului, prima dată la trei ani de la intrarea în vigoare. De asemenea, Comisia va evalua transpunerea corectă a directivei de către statele membre.

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea modului (modurilor) de gestiune, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

Unitatea din cadrul DG CNECT responsabilă cu domeniul de politică va gestiona punerea în aplicare a directivei.

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

Risc foarte scăzut, întrucât ecosistemul Directivei NIS este deja instituit.

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

Nu sunt relevante. Numai utilizarea bugetului administrativ („pachetul global”).

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate, de exemplu din strategia antifraudă.

Nu sunt relevante. Numai utilizarea bugetului administrativ („pachetul global”).

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli propusă (propuse)

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul de cheltuieli	Contribuție			
	Numărul [Rubrica…7……...……]	Dif./Nedif. [42]	din partea țărilor AELS[43]	din partea țărilor candidate[44]	din partea țărilor terțe	în sensul articolului [21 alineatul (2) litera (b)] din Regulamentul financiar
	20 02 06 cheltuieli de gestiune 20 02 06	Nedif.	NU	NU	NU	NU

[42] Dif. = credite diferențiate/Nedif. = credite nediferențiate.

[43] AELS: Asociația Europeană a Liberului Schimb.

[44] Țările candidate și, după caz, candidații potențiali din Balcanii de Vest.

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	**<…>**	[Rubrica……...……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***După 2027***	**TOTAL**
Credite operaționale (repartizate în funcție de liniile bugetare menționate la punctul 3.1)	Angajamente	(1)									
	Plăți	(2)									
Credite cu caracter administrativ finanțate din pachetul financiar al programului[45]	Angajamente = Plăți	(3)									
TOTAL credite pentru pachetul financiar al programului	Angajamente	=1+3									
	Plăți	=2+3									

Rubrica din cadrul financiar multianual	7	„Cheltuieli administrative” Reuniuni: reuniunile plenare ale Grupului de cooperare NIS au loc, de obicei, de 4 ori pe an. Comisia acoperă costurile legate de cheltuielile de catering și de călătorie ale reprezentanților celor 27 de state membre (câte un reprezentant pentru fiecare stat membru). Costurile unei reuniuni ar putea ajunge până la 15 000 EUR. Delegații: delegațiile se referă la monitorizarea punerii în aplicare a Directivei NIS. Exemplu: într-un an (mai 2019-iulie 2020), trebuia să organizăm așa-numitele „vizite la nivel de țară în domeniul NIS” și să vizităm toate cele 27 de state membre pentru a

[45] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

		discuta punerea în aplicare a Directivei NIS în întreaga UE.

Această secțiune ar trebui completată utilizând „datele bugetare cu caracter administrativ” care trebuie introduse mai întâi în anexa la fişa financiară legislativă, încărcată în DECIDE pentru consultarea interservicii.

milioane EUR (cu trei zecimale)

		2021	2022	2023	2024	2025	2026	2027	*După 2027*	TOTAL
Resurse umane		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Alte cheltuieli administrative		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
TOTAL credite de la RUBRICA 7 din cadrul financiar multianual	(Total angajamente = Total plăți)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

milioane EUR (cu trei zecimale)

		2021	2022	2023	2024	2025	2026	2027	*După 2027*	TOTAL
TOTAL credite de la RUBRICILE din cadrul financiar multianual	Angajamente									
	Plăți									

3.2.2. Sinteza impactului estimat asupra creditelor administrative

– ☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

– ☐X Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

Anii	2021	2022	2023	2024	2025	2026	2027	TOTAL
RUBRICA 7 din cadrul financiar multianual								
Resurse umane	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Alte cheltuieli administrative	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Subtotal RUBRICA 7 din cadrul financiar multianual	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**

În afara RUBRICII 7[46] of the multiannual financial framework								
Resurse umane								
Alte cheltuieli cu caracter administrativ								
Subtotal în afara RUBRICII 7 din cadrul financiar multianual								

TOTAL	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

Necesarul de credite pentru resursele umane și pentru alte cheltuieli cu caracter administrativ va fi acoperit de creditele direcției generale (DG) respective care sunt deja alocate pentru gestionarea acțiunii și/sau au fost redistribuite intern în cadrul DG-ului respectiv, completate, după caz, cu resurse suplimentare care ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

[46] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

3.2.2.1. Necesarul de resurse umane estimat

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

– X☐ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimări în echivalent normă întreagă

Anii		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• **Posturi din schema de personal (funcționari și agenți temporari)**								
La sediu și în reprezentanțele Comisiei		6	6	6	6	6	6	6
În delegații								
Cercetare								
• Personal extern (în echivalent normă întreagă: ENI) – AC, AL, END, INT și JPD [47] Rubrica 7								
Finanțare de la RUBRICA 7 din cadrul financiar multianual	- la sediu	3	3	3	3	3	3	3
	- în delegații							
Finanțare din pachetul financiar al programului [48]	- la sediu							
	- în delegații							
Cercetare								
Altele (precizați)								
TOTAL		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând cont de constrângerile bugetare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și personal temporar	• Pregătirea actelor delegate în conformitate cu articolul 18 alineatul (6), articolul 21 alineatul (2) și articolul 36 • Pregătirea actelor de punere în aplicare în conformitate cu articolul 12 alineatul (8), articolul 18 alineatul (5) și articolul 20 alineatul (11) • Asigurarea unui secretariat pentru Grupul de cooperare NIS • Organizarea reuniunilor plenare ale Grupului de cooperare NIS și a reuniunilor direcțiilor de lucru; • Coordonarea activității statelor membre cu privire la diverse documente (orientări, seturi de instrumente etc.) • Legătura cu alte servicii ale Comisiei, cu ENISA și cu autoritățile naționale în vederea punerii în aplicare a Directivei NIS • Analiza metodelor naționale și a celor mai bune practici legate de punerea în aplicare a Directivei NIS
Personal extern	Sprijin pentru toate atribuțiile de mai sus, după caz

[47] AC = agent contractual; AL = agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = tânăr profesionist în delegații.

[48] Subplafonul pentru personal extern acoperit din creditele operaționale (fostele linii „BA”).

3.2.3. Contribuțiile terților

Propunerea/inițiativa:

– X☐ nu prevede cofinanțare din partea terților

– ☐ prevede cofinanțare din partea terților, estimată mai jos:

Credite în milioane EUR (cu trei zecimale)

Anii	2021	2022	2023	2024	2025	2026	2027	TOTAL
A se preciza organismul care asigură cofinanțarea								
TOTAL credite cofinanțate								

3.3. Impactul estimat asupra veniturilor

– ☐X Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☐ Propunerea/inițiativa are următorul impact financiar:

☐ asupra resurselor proprii

☐ asupra altor venituri

vă rugăm să precizați dacă veniturile sunt alocate unor linii de cheltuieli ☐

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Impactul propunerii/inițiativei[49]						
	2021	2022	2023	2024	2025	2026	2027
Articolul …..							

Pentru veniturile alocate, a se preciza linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate).

Alte observații (de exemplu, metoda/formula utilizată pentru calcularea impactului asupra veniturilor sau orice alte informații).

[49] În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sumele brute după deducerea unei cote de 20 % pentru costurile de colectare.

ANEXĂ
la FIȘA FINANCIARĂ LEGISLATIVĂ

Titlul propunerii/inițiativei:

Propunere de directivă de revizuire a Directivei (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

……
……

1. NUMĂRUL și COSTURILE aferente RESURSELOR UMANE CONSIDERATE NECESARE

2. COSTURI aferente ALTOR CHELTUIELI ADMINISTRATIVE

3. METODE de CALCUL UTILIZATE pentru ESTIMAREA COSTURILOR

3.1 Resurse umane

3.2 Alte cheltuieli administrative

*Prezenta anexă, **care trebuie completată de fiecare DG/serviciu care participă la propunere/inițiativă**, trebuie să însoțească fișa financiară legislativă la momentul lansării consultării interservicii.*

Tabelele de date sunt utilizate ca sursă pentru tabelele conținute în fișa financiară legislativă. Acestea sunt destinate exclusiv uzului intern în cadrul Comisiei.

1. Costurile aferente resurselor umane considerate necesare

☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

X☐ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

RUBRICA 7 din cadrul financiar multianual		**2021**		**2022**		**2023**		**2024**		**2025**		**2026**		**2027**		**TOTAL**	
		ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite
• Posturi din schema de personal (funcționari și agenți temporari)																	
La sediu și în reprezentanțele Comisiei	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
în delegațiile Uniunii	AD																
	AST																
• Personal extern [50] 0,24																	
Pachet global	AC	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	END																
	INT																
în delegațiile Uniunii	AC																
	AL																
	END																

[50] AC = agent contractual; AL = agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = tânăr profesionist în delegații.

	INT																
	JPD																
Alte linii bugetare (*a se preciza*)																	
Subtotal – RUBRICA 7 din cadrul financiar multianual		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând cont de constrângerile bugetare.

În afara RUBRICII 7 din cadrul financiar multianual		2021		2022		2023		2024		2025		2025		2025		TOTAL	
		ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite	ENI	Credite
• Posturi din schema de personal (funcționari și agenți temporari)																	
Cercetare	AD																
	AST																
• Personal extern [51]																	
Personal extern acoperit din credite operaționale (fostele linii „BA”).	- la sediu AC																
	- la sediu END																
	- la sediu INT																
	- în delegațiile Uniunii AC																
	- în delegațiile Uniunii AL																
	- în delegațiile Uniunii END																
	- în delegațiile Uniunii INT																
	- în delegațiile Uniunii JPD																
Cercetare	AC																
	END																
	INT																
Alte linii bugetare (*a se*																	

[51] AC = agent contractual; AL = agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = tânăr profesionist în delegații.

preciza)																	
Subtotal – În afara RUBRICII 7 din cadrul financiar multianual																	

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând cont de constrângerile bugetare.

Impactul estimat asupra resurselor umane ale ENISA

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, căreia i s-a acordat un nou mandat permanent prin Regulamentul privind securitatea cibernetică, ar urma să sprijine statele membre și Comisia în punerea în aplicare a Directivei NIS revizuite. Ca urmare a revizuirii Directivei NIS, începând cu 2022/2023, ENISA va avea domenii de acțiune suplimentare. Deși aceste domenii de acțiune ar fi acoperite de atribuțiile generale ale ENISA conform mandatului său, ele vor genera un volum de muncă suplimentar pentru agenție. Mai precis, pe lângă domeniile sale de acțiune actuale, în temeiul propunerii Comisiei de revizuire a Directivei NIS, ENISA va trebui, de asemenea, să includă în mod specific în programul său de lucru, printre altele, următoarele acțiuni: (i) elaborarea și menținerea unui registru european al vulnerabilităților [articolul 6 alineatul (2) din propunere], (ii) asigurarea secretariatului Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (CyCLONe) (articolul 14 din propunere) și publicarea unui raport anual privind situația în materie de securitate cibernetică în UE (articolul 15 din propunere), (iii) sprijinirea organizării de evaluări *inter pares* între statele membre (articolul 16 din propunere), (iv) colectarea de date agregate privind incidentele de la statele membre și emiterea unor orientări tehnice [articolul 20 alineatul (9) din propunere], (v) crearea și menținerea unui registru pentru entitățile care furnizează servicii transfrontaliere (articolul 25 din propunere). Prin urmare, se va face o cerere de 5 ENI suplimentare începând cu 2022, cu bugetul corespunzător de aproximativ 0,61 milioane EUR pe an, pentru a acoperi aceste noi posturi (a se vedea Fișa financiară separată pentru agenții).

Prin urmare, se va face o cerere de 5 ENI suplimentare începând cu 2022, cu bugetul corespunzător pentru a acoperi aceste noi posturi.

☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

☐X Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

	Anul **N** [52] **2022**	Anul **N+1** **2023**	Anul **N+2** **2024**	Anul **N+3** **2025**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)	**TOTAL**

[52] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

Agenți temporari (grade AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Agenți temporari (grade AST)								
Agenți contractuali	0,160	0,160	0,160	0,160	0,160	0,160		
Experți naționali detașați								**0,96**

TOTAL	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Cerințe privind personalul (ENI):

	Anul **N** [53] **2022**	Anul **N+1** **2023**	Anul **N+2** **2024**	Anul **N+3** **2025**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)	**TOTAL**
Agenți temporari (grade AD)	3	3	3	3	3	3		**18**
Agenți temporari (grade AST)								
Agenți contractuali	2	2	2	2	2	2		**12**

[53] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

Experți naționali detașați								

TOTAL	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Costuri aferente altor cheltuieli administrative

☐ Propunerea/inițiativa nu implică utilizarea de credite administrative.

X☐ Propunerea/inițiativa implică utilizarea de credite administrative, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

RUBRICA 7 din cadrul financiar multianual	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
La sediu:								
Cheltuieli pentru delegații și reprezentare	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Cheltuieli aferente conferințelor și reuniunilor	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Comitete[54]								
Studii și consultări								
Sisteme de informare și de gestiune								

[54] Se indică tipul de comitet și grupul de care aparține.

Echipamente și servicii TIC[55]								
Alte linii bugetare (*a se preciza, dacă este cazul*)								
În delegațiile Uniunii								
Cheltuieli pentru delegații, conferințe și reprezentare								
Perfecționare profesională								
Cheltuieli de achiziționare și de închiriere și cheltuieli aferente								
Echipamente, mobilier, materiale și servicii								
Subtotal RUBRICA 7 din cadrul financiar multianual	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[55] TIC: Tehnologiile informației și comunicațiilor: trebuie consultată DIGIT.

milioane EUR (cu trei zecimale)

În afara RUBRICII 7 din cadrul financiar multianual	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Total**
Cheltuieli cu asistența tehnică și administrativă (cu excepția personalului extern) din creditele operaționale (fostele linii „BA”)								
- la sediu								
- în delegațiile Uniunii								
Alte cheltuieli de gestiune pentru cercetare								
Alte linii bugetare (*a se preciza, dacă este cazul*)								
Subtotal – În afara RUBRICII 7 din cadrul financiar multianual								

TOTAL **RUBRICA 7 și în afara RUBRICII 7** din cadrul financiar multianual	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Necesarul de credite administrative va fi asigurat din creditele alocate deja pentru gestionarea acțiunii și/sau realocate intern, completate, după caz, prin resurse suplimentare ce ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii de alocare anuală și în lumina constrângerilor bugetare existente.

3. Metodele de calcul utilizate pentru estimarea costurilor

3.1 Resurse umane

Această parte stabilește metoda de calcul utilizată pentru estimarea resurselor umane considerate necesare [ipoteze referitoare la volumul de muncă, inclusiv locuri de muncă concrete (profiluri profesionale specifice sistemului Sysper2), categoriile de personal și costurile medii aferente]

RUBRICA 7 din cadrul financiar multianual
NB: Costurile medii pentru fiecare categorie de personal de la sediul central sunt disponibile pe site-ul BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Funcționari și personal temporar 6 Funcționari ENI (cost mediu 0,150) = 0,9 pe an - Pregătirea actelor delegate în conformitate cu articolul 18 alineatul (6), articolul 21 alineatul (2) și articolul 36 - Pregătirea actelor de punere în aplicare în conformitate cu articolul 12 alineatul (8), articolul 18 alineatul (5) și articolul 20 alineatul (11) - Asigurarea unui secretariat pentru Grupul de cooperare NIS - Organizarea reuniunilor plenare ale Grupului de cooperare NIS și a reuniunilor direcțiilor de lucru; - Coordonarea activității statelor membre cu privire la diverse documente (orientări, seturi de instrumente etc.) - Legătura cu alte servicii ale Comisiei, cu ENISA și cu autoritățile naționale în vederea punerii în aplicare a Directivei NIS - Analiza metodelor naționale și a celor mai bune practici legate de punerea în aplicare a Directivei NIS
• Personal extern 3 AC (cost mediu 0,08) = 0,24 pe an - Sprijin pentru toate atribuțiile de mai sus, după caz

În afara RUBRICII 7 din cadrul financiar multianual
• Numai posturile finanțate din bugetul de cercetare
• Personal extern

3.2 Alte cheltuieli administrative

A se detalia metoda de calcul utilizată pentru fiecare linie bugetară,

și în special ipotezele pe care se bazează (de exemplu, numărul de reuniuni pe an, costurile medii etc.)

RUBRICA 7 din cadrul financiar multianual
Reuniuni: reuniunile plenare ale Grupului de cooperare NIS au loc, de obicei, de 4 ori pe an. Comisia acoperă costurile legate de cheltuielile de catering și de călătorie ale reprezentanților celor 27 de state membre (câte un reprezentant pentru fiecare stat membru). Costurile unei reuniuni ar putea ajunge până la 15 000 EUR, ceea ce înseamnă 60 000 EUR pe an. Delegații: delegațiile se referă la monitorizarea punerii în aplicare a Directivei NIS. Exemplu: într-un an (mai 2019-iulie 2020), trebuia să organizăm așa-numitele „vizite la nivel de țară în domeniul NIS” și să vizităm toate cele 27 de state membre pentru a discuta punerea în aplicare a Directivei NIS în întreaga UE.

În afara RUBRICII 7 din cadrul financiar multianual

ANEXA 7

la
DECIZIA COMISIEI

referitoare la normele interne privind execuția bugetului general al Uniunii Europene (secțiunea Comisia Europeană) în atenția departamentelor Comisiei

FIȘA FINANCIARĂ LEGISLATIVĂ „AGENȚII”

Prezenta fișă financiară legislativă acoperă cererea de creștere a personalului ENISA cu 5 ENI din 2022 pentru a efectua activități suplimentare legate de punerea în aplicare a Directivei NIS. Aceste activități sunt deja acoperite de mandatul ENISA.

Cuprins

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

Propunere de directivă privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148

1.2. Domeniul (domeniile) de politică vizat(e)

Rețele de comunicații, conținut și tehnologie

1.3. Obiectul propunerii/inițiativei

☐ **o nouă acțiune**

☐ **o acțiune nouă întreprinsă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[56]

☒ **prelungirea unei acțiuni existente**

☐ **o fuziune a uneia sau mai multor acțiuni către o altă/o nouă acțiune**

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

Obiectivul revizuirii este de a spori nivelul de reziliență cibernetică a unui set cuprinzător de întreprinderi care își desfășoară activitatea în Uniunea Europeană în toate sectoarele relevante, de a reduce inconsecvențele în ceea ce privește reziliența pe piața internă în sectoarele care fac deja obiectul directivei și de a îmbunătăți nivelul de conștientizare comună a situației și capacitatea colectivă de a se pregăti și de a răspunde.

1.4.2. Obiectiv(e) specific(e)

Pentru a aborda problema nivelului scăzut de reziliență cibernetică a întreprinderilor care își desfășoară activitatea în Uniunea Europeană, obiectivul specific este de a se asigura că entitățile din toate sectoarele care depind de rețele și de sisteme informatice și care furnizează servicii esențiale economiei și societății în ansamblu sunt obligate să ia măsuri de securitate cibernetică și să raporteze incidentele în vederea creșterii nivelului general de reziliență cibernetică în întreaga piață internă.

Pentru a soluționa problema inconsecvenței rezilienței între statele membre și între sectoare, obiectivul specific este de a se asigura că toate entitățile care își desfășoară activitatea în sectoare vizate de cadrul juridic NIS și care sunt similare ca dimensiune și au un rol comparabil fac obiectul aceluiași regim de reglementare (fie în interiorul, fie în afara domeniului de aplicare), indiferent de jurisdicția în care intră sub incidența UE.

Pentru a se asigura că toate entitățile care își desfășoară activitatea în sectoarele vizate de cadrul juridic privind NIS trebuie să respecte aceleași obligații bazate pe conceptul de gestionare a riscurilor în ceea ce privește măsurile de securitate și trebuie să raporteze toate incidentele pe baza unui set uniform de criterii, obiectivele specifice sunt de a se asigura că autoritățile competente pun în aplicare mai eficient normele stabilite de instrumentul juridic prin măsuri aliniate de supraveghere și de asigurare a respectării legislației și de a asigura un

[56] Astfel cum se menționează la articolul 58 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

nivel comparabil al resurselor alocate autorităților competente în statele membre, care le-ar permite să îndeplinească sarcinile principale prevăzute de cadrul NIS.

Pentru a aborda problema conștientizării comune a situației și a lipsei unui răspuns comun în caz de criză, obiectivul specific este de a asigura schimbul de informații esențiale între statele membre prin introducerea unor obligații clare pentru autoritățile competente de a face schimb de informații și de a coopera în ceea ce privește amenințările și incidentele cibernetice și prin dezvoltarea unei capacități operaționale comune de răspuns la crize la nivelul Uniunii.

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care ar trebui să le aibă propunerea/inițiativa asupra beneficiarilor vizați/grupurilor vizate.

Se preconizează că propunerea va aduce beneficii semnificative: estimările indică faptul că acest lucru ar putea duce la o reducere cu 11,3 miliarde EUR a costurilor aferente incidentelor de securitate cibernetică. Domeniul de aplicare sectorial ar fi extins în mod considerabil în cadrul NIS, dar, pe lângă beneficiile de mai sus, sarcina care poate fi creată de cerințele în materie de NIS, în special din perspectiva supravegherii, ar fi, de asemenea, echilibrată atât pentru noile entități care urmează să fie acoperite, cât și pentru autoritățile competente. Acest lucru se datorează faptului că noul cadru NIS ar stabili o abordare pe două niveluri, cu accent pe entitățile mari și esențiale și o diferențiere a regimului de supraveghere care permite doar supravegherea *ex post* pentru un număr mare de entități, în special pentru cele considerate „importante”, dar nu „esențiale”.

În general, propunerea ar conduce la compromisuri și sinergii eficiente, cu cel mai bun potențial dintre toate opțiunile de politică analizate pentru a asigura un nivel sporit și consecvent de reziliență cibernetică a entităților-cheie din întreaga Uniune, ceea ce ar duce, în cele din urmă, la economii de costuri atât pentru întreprinderi, cât și pentru societate.

Propunerea ar conduce, de asemenea, la anumite costuri de asigurare a conformității și de asigurare a respectării legislației pentru autoritățile relevante ale statelor membre (s-a estimat o creștere globală de aproximativ 20-30 % a resurselor). Cu toate acestea, noul cadru ar aduce, de asemenea, beneficii substanțiale printr-o mai bună imagine de ansamblu a principalelor întreprinderi și prin interacțiunea cu acestea, printr-o cooperare operațională transfrontalieră consolidată, precum și prin asistență reciprocă și mecanisme de evaluare *inter pares*. Acest lucru ar duce la o creștere globală a capacităților în materie de securitate cibernetică în statele membre.

Pentru societățile care s-ar încadra în domeniul de aplicare al cadrului NIS, se estimează că acestea ar avea nevoie de o creștere de maximum 22 % a cheltuielilor lor actuale în materie de securitate TIC pentru primii ani de la introducerea noului cadru NIS (aceasta ar fi de 12 % pentru societățile care intră deja sub incidența actualei Directive NIS). Totuși, această creștere medie a cheltuielilor în materie de securitate TIC ar conduce la un beneficiu proporțional al unor astfel de investiții, în special datorită unei reduceri considerabile a costurilor aferente incidentelor de securitate cibernetică (estimate la 118 miliarde EUR pe o perioadă de zece ani).

Întreprinderile mici și microîntreprinderile ar fi excluse din domeniul de aplicare al cadrului NIS. Pentru întreprinderile mijlocii, se poate preconiza o creștere a nivelului cheltuielilor în materie de securitate TIC în primii ani de la introducerea noului cadru NIS. În același timp, creșterea nivelului cerințelor de securitate pentru aceste entități ar stimula, de asemenea, capacitățile lor în materie de securitate cibernetică și ar contribui la îmbunătățirea gestionării riscurilor TIC.

Ar exista un impact asupra bugetelor și administrațiilor naționale: pe termen scurt și mediu, se preconizează o creștere estimată a resurselor de aproximativ 20-30 %.

Nu se preconizează niciun alt impact negativ semnificativ. Conform estimărilor, propunerea va conduce la capabilități de securitate cibernetică mai solide și, prin urmare, va avea un impact de atenuare mai substanțial asupra numărului de incidente și a gravității acestora, inclusiv asupra încălcărilor securității datelor. De asemenea, este probabil ca propunerea să

aibă un impact pozitiv asupra asigurării unor condiții de concurență echitabile între statele membre pentru toate entitățile care intră în domeniul de aplicare al NIS și să reducă asimetriile informaționale în materie de securitate cibernetică.

1.4.4. Indicatori de performanță

A se preciza indicatorii care permit monitorizarea progreselor și a realizărilor obținute.

Evaluarea indicatorilor va fi efectuată de Comisie, cu sprijinul ENISA și al Grupului de cooperare, începând cu trei ani de la intrarea în vigoare a noului act legislativ NIS. Unii dintre indicatorii de monitorizare pe baza cărora urmează să fie evaluat succesul revizuirii NIS sunt următorii:

- Gestionarea îmbunătățită a incidentelor: Prin adoptarea de măsuri în materie de securitate cibernetică, întreprinderile își îmbunătățesc nu numai capacitatea de a evita în totalitate anumite incidente, ci și capacitatea lor de reacție în caz de incidente. Prin urmare, măsurile de succes sunt i) reducerea timpului mediu necesar pentru detectarea unui incident, ii) timpul necesar în medie organizațiilor pentru a se redresa în urma unui incident și iii) costul mediu al daunelor cauzate de un incident.

- Creșterea gradului de conștientizare a conducerii superioare a întreprinderilor cu privire la riscurile de securitate cibernetică: Solicitând întreprinderilor să ia măsuri, Directiva NIS revizuită ar contribui la creșterea gradului de conștientizare a conducerii superioare cu privire la riscurile legate de securitatea cibernetică. Acest lucru poate fi măsurat prin studierea măsurii în care întreprinderile care intră în domeniul de aplicare al NIS acordă prioritate securității cibernetice în politicile și procesele interne ale întreprinderilor, după cum reiese din documentația internă, din programele de formare relevante și din activitățile de sensibilizare pentru angajați și acordând prioritate investițiilor TIC legate de securitate. Conducerea tuturor entităților esențiale și importante ar trebui, de asemenea, să cunoască normele prevăzute în Directiva NIS.

- Egalizarea cheltuielilor sectoriale: Cheltuielile pentru securitatea TIC variază considerabil de la un sector la altul în UE. Prin impunerea obligației ca întreprinderile din mai multe sectoare să ia măsuri, abaterile de la cheltuielile sectoriale medii în materie de securitate TIC ca procent din totalul cheltuielilor TIC ar trebui să scadă de la un sector la altul și de la un stat membru la altul.

- Consolidarea autorităților competente și intensificarea cooperării: Directiva NIS revizuită ar putea conferi sarcini suplimentare autorităților competente. Acest lucru ar avea un impact măsurabil asupra resurselor financiare și umane dedicate agențiilor de securitate cibernetică la nivel național și ar trebui, de asemenea, să aibă un impact pozitiv asupra capacității autorităților competente de a coopera în mod proactiv și, prin urmare, ar spori numărul de cazuri în care autoritățile competente colaborează între ele în scopul gestionării incidentelor transfrontaliere sau al desfășurării de activități comune de supraveghere.

- Intensificarea schimbului de informații: De asemenea, revizuirea NIS ar îmbunătăți schimbul de informații între întreprinderi și cu autoritățile competente. Unul dintre obiectivele revizuirii ar putea fi creșterea numărului de entități care participă la diferitele forme de schimb de informații.

1.5. Motivele propunerii/inițiativei

1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei

Propunerea are ca obiectiv mărirea nivelului de reziliență cibernetică a unui set cuprinzător de întreprinderi care își desfășoară activitatea în Uniunea Europeană în toate sectoarele relevante, reducerea inconsecvențelor în ceea ce privește reziliența pe piața internă în sectoarele care fac deja obiectul directivei și îmbunătățirea nivelului de conștientizare comună a situației și capacitatea colectivă de a se pregăti și de a răspunde. Aceasta se va baza pe ceea ce s-a realizat în ultimii 4 ani prin punerea în aplicare a Directivei (UE) 2016/1148.

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu mai buna coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii” este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

Reziliența în materie de securitate cibernetică în întreaga Uniune nu poate fi eficace dacă este abordată într-un mod disparat prin fragmentări naționale sau regionale. Directiva NIS a ajuns să abordeze această deficiență prin stabilirea unui cadru pentru securitatea rețelelor și a sistemelor informatice la nivel național și la nivelul Uniunii. Cu toate acestea, prima revizuire periodică a Directivei NIS a evidențiat o serie de deficiențe inerente, care au condus în cele din urmă la diferențe considerabile între statele membre în ceea ce privește capacitățile, planificarea și nivelul de protecție, care afectează, în același timp, condițiile de concurență echitabile pentru întreprinderile similare de pe piața internă.

Intervenția UE, care depășește măsurile actuale prevăzute în Directiva NIS, este justificată în principal de: (i) caracterul transfrontalier al problemei; (ii) potențialul acțiunii UE de îmbunătățire și de facilitare a unor politici naționale eficace; (iii) contribuția acțiunilor politice concertate și colaborative NIS la protejarea eficace a protecției datelor și a vieții private.

Prin urmare, obiectivele declarate pot fi realizate mai bine prin acțiuni la nivelul UE decât prin acțiuni individuale ale statelor membre.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

Directiva NIS este primul instrument orizontal al pieței interne care vizează îmbunătățirea rezilienței rețelelor și a sistemelor din Uniune la riscurile de securitate cibernetică. De la intrarea sa în vigoare în 2016, directiva a contribuit deja în mare măsură la creșterea nivelului comun de securitate cibernetică în rândul statelor membre. Cu toate acestea, revizuirea funcționării și a punerii în aplicare a directivei a evidențiat o serie de deficiențe care, pe lângă digitalizarea în creștere și necesitatea unui răspuns mai actualizat, trebuie abordate într-un act juridic revizuit.

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

Noua propunere este pe deplin consecventă și coerentă cu alte inițiative conexe, cum ar fi Propunerea de regulament privind reziliența operațională digitală a sectorului financiar („DORA”) și Propunerea de directivă privind reziliența operatorilor critici de servicii esențiale. Prezenta propunere este, de asemenea, în concordanță cu Codul european al

comunicațiilor electronice, cu Regulamentul general privind protecția datelor și cu Regulamentul e-IDAS.

Propunerea este o parte esențială a Strategiei UE privind o uniune a securității.

1.5.5. Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de realocare a creditelor

Gestionarea acestor atribuții de către ENISA necesită profiluri specifice și un volum de muncă suplimentar care nu poate fi absorbit fără o creștere a resurselor umane.

1.6. Durata și impactul financiar ale propunerii/inițiativei

☐ **durată limitată**

– ☐ Propunere/inițiativă în vigoare de la [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ Impact financiar din AAAA până în AAAA

☒ **durată nelimitată**

– Punere în aplicare cu o perioadă de creștere în intensitate din 2022 până în 2025,

– urmată de o perioadă de funcționare la capacitate maximă.

1.7. Modul (modurile) de gestionare preconizat(e)[57]

☒ **Gestiune directă** asigurată de către Comisie

prin intermediul

– ☐ agențiilor executive

☐ **Gestiune partajată** cu statele membre

☐X **Gestiune indirectă**, cu delegarea sarcinilor de execuție bugetară:

☐ organizațiilor internaționale și agențiilor acestora (a se preciza);

☐ BEI și Fondului European de Investiții;

☒ organismelor menționate la articolele 70 și 71;

☐ organismelor de drept public;

☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să prezinte garanții financiare adecvate;

☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și care prezintă garanții financiare adecvate;

☐ persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, și care sunt identificate în actul de bază relevant.

Observații

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, căreia i s-a acordat un nou mandat permanent prin Regulamentul privind securitatea cibernetică, ar urma să sprijine statele membre și Comisia în punerea în aplicare a Directivei NIS revizuite.

Ca urmare a revizuirii Directivei NIS, începând cu 2022/2023, ENISA va avea domenii de acțiune suplimentare. Deși aceste domenii de acțiune ar fi acoperite de atribuțiile generale ale ENISA conform mandatului său, ele vor genera un volum de muncă suplimentar pentru agenție. Mai precis, pe lângă domeniile sale de acțiune actuale, în temeiul propunerii Comisiei de revizuire a Directivei NIS, ENISA va trebui, de asemenea, să includă în mod specific în programul său de lucru, printre altele, următoarele acțiuni: (i) elaborarea și menținerea unui registru european al vulnerabilităților [articolul 6 alineatul (2) din propunere], (ii) asigurarea secretariatului Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (CyCLONe) (articolul 14 din propunere) și publicarea unui raport anual privind

[57] Explicații detaliate privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

situația în materie de securitate cibernetică în UE (articolul 15 din propunere), (iii) sprijinirea organizării de evaluări *inter pares* între statele membre (articolul 16 din propunere), (iv) colectarea de date agregate privind incidentele de la statele membre și emiterea unor orientări tehnice [articolul 20 alineatul (9) din propunere], (v) crearea și menținerea unui registru pentru entitățile care furnizează servicii transfrontaliere (articolul 25 din propunere).

Prin urmare, se va face o cerere de 5 ENI suplimentare începând cu 2022, cu bugetul corespunzător de aproximativ 0,61 milioane EUR pe an, pentru a acoperi aceste noi posturi.

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile aferente monitorizării și raportării.

Comisia va revizui periodic funcționarea directivei și va prezenta un raport Parlamentului European și Consiliului, prima dată la trei ani de la intrarea în vigoare.

De asemenea, Comisia va evalua transpunerea corectă a directivei de către statele membre.

Monitorizarea și raportarea propunerii vor respecta principiile definite în mandatul permanent al ENISA în temeiul Regulamentului (UE) 2019/881 (Regulamentul privind securitatea cibernetică).

Sursele de date utilizate pentru monitorizarea planificată ar proveni în principal de la ENISA, Grupul de cooperare, rețeaua CSIRT și autoritățile statelor membre. Pe lângă datele colectate din rapoartele (inclusiv rapoartele anuale de activitate) ENISA, ale Grupului de cooperare și ale rețelei CSIRT, ar putea fi utilizate instrumente specifice de colectare a datelor atunci când este necesar (de exemplu, sondaje adresate autorităților naționale, Eurobarometru și rapoarte din campania Luna securității cibernetice și exerciții paneuropene).

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea modului (modurilor) de gestiune, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

Unitatea din cadrul DG CNECT responsabilă cu domeniul de politică va gestiona punerea în aplicare a directivei.

În ceea ce privește gestionarea ENISA, articolul 15 din Regulamentul privind securitatea cibernetică prevede o listă detaliată a funcțiilor de control ale consiliului de administrație al ENISA.

În temeiul articolului 31 din Regulamentul privind securitatea cibernetică, directorul executiv al ENISA este responsabil cu execuția bugetului ENISA, iar auditorul intern al Comisiei exercită asupra ENISA aceleași prerogative ca și asupra departamentelor Comisiei. Consiliul de administrație al ENISA emite un aviz cu privire la conturile finale ale ENISA.

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

Risc foarte scăzut, întrucât ecosistemul Directivei NIS este deja instituit și acoperă deja ENISA, care are un mandat permanent în urma intrării în vigoare a Regulamentului din 2019 privind securitatea cibernetică.

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

Majorarea bugetară solicitată aplică titlul 1 și este destinată finanțării salariilor. Acest lucru înseamnă un risc foarte scăzut de eroare la nivelul plăților.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate, de exemplu din strategia antifraudă.

Ar urma să se aplice măsurile de prevenire și de protecție ale ENISA, și anume:

— personalul agenției verifică plățile pentru orice fel de servicii sau de studii solicitate, înainte de efectuarea plății, luând în considerare toate obligațiile contractuale, principiile economice și bunele practici financiare sau de gestionare; toate acordurile și contractele încheiate între agenție și beneficiarii plăților vor cuprinde dispoziții antifraudă (control, cerințe privind raportarea etc.);

— pentru a combate fraudele, corupția și alte activități ilegale, dispozițiile Regulamentului (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului din 25 mai 1999 privind investigațiile efectuate de Oficiul European Antifraudă (OLAF) se aplică fără restricții;

— în temeiul articolului 33 din Regulamentul privind securitatea cibernetică, ENISA a aderat, până la 28 decembrie 2019, la Acordul interinstituțional din 25 mai 1999 dintre Parlamentul European, Consiliul Uniunii Europene și Comisia Comunităților Europene privind investigațiile interne desfășurate de Oficiul European de Luptă Antifraudă (OLAF). ENISA emite, fără întârziere, dispozițiile corespunzătoare aplicabile tuturor angajaților agenției.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

- Linii bugetare existente

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul de cheltuieli	Contribuție			
	Numărul	Dif./Nedif. [58]	din partea țărilor AELS[59]	din partea țărilor candidate[60]	din partea țărilor terțe	în sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
2	02 10 04	./Nedif.	DA	NU	NU	/NU

- Noile linii bugetare solicitate

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din	Linia bugetară	Tipul de	Contribuție

[58] Dif. = credite diferențiate/Nedif. = credite nediferențiate.
[59] AELS: Asociația Europeană a Liberului Schimb.
[60] Țările candidate și, după caz, candidații potențiali din Balcanii de Vest.

cadrul financiar multianual		cheltuieli				
	Numărul	Dif./Nedif.	din partea țărilor AELS	din partea țărilor candidate	din partea țărilor terțe	în sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
	[XX.YY.YY.YY]		DA/NU	DA/NU	DA/NU	DA/NU

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	Numărul	[Rubrica... 2 Piața unică, inovare și sectorul digital.....]

[Organism]: <…ENISA….>			Anul **N**[61] **2022**	Anul **N+1** **2023**	Anul **N+2** **2024**	Anul **N+3** **2025**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6) **2026**	**2027**		**TOTAL**
Titlul 1:	Angajamente	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Plăți	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Titlul 2:	Angajamente	(1a)								
	Plăți	(2 a)								
Titlul 3:	Angajamente	(3a)								
	Plăți	(3b)								
TOTAL credite pentru [organismul] <ENISA…….>	Angajamente	=1+1a +3a	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Plăți	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

Rubrica din cadrul financiar multianual	**5**	„Cheltuieli administrative”

milioane EUR (cu trei zecimale)

		Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			**TOTAL**
DG: <…….>									
• Resurse umane									
• Alte cheltuieli administrative									
TOTAL DG <…….>	Credite								

TOTAL credite de la RUBRICA 5 din cadrul financiar multianual	(Total angajamente = Total plăți)								

milioane EUR (cu trei zecimale)

		Anul **N**[62] **2022**	Anul **N+1** **2023**	Anul **N+2** **2024**	Anul **N+3** **2025**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6) **2026**	**2027**		**TOTAL**
TOTAL credite de la RUBRICILE 1-5 din cadrul financiar multianual	Angajamente	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Plăți	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

3.2.2. Impactul estimat asupra creditelor [organismului]

– ☐x Propunerea/inițiativa nu implică utilizarea de credite operaționale

– ☐ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

Credite de angajament în milioane EUR (cu trei zecimale)

A se indica obiectivele și realizările			Anul **N**		Anul **N+1**		Anul **N+2**		Anul **N+3**		A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)						**TOTAL**	
	REALIZĂRI																	
⇩	Tip[63]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Total nr.	Total costuri
OBIECTIVUL SPECIFIC NR. 1[64]…																		
- Realizare																		
- Realizare																		
- Realizare																		
Subtotal pentru obiectivul specific nr. 1																		
OBIECTIVUL SPECIFIC NR. 2…																		
- Realizare																		
Subtotal pentru obiectivul specific nr. 2																		
TOTAL COSTURI																		

63 Realizările se referă la produsele și serviciile care trebuie furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de drumuri construiți etc.).

64 Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

3.2.3. Impactul estimat asupra resurselor umane ale ENISA

3.2.3.1. Sinteză

Ca urmare a revizuirii Directivei NIS, începând cu 2022/2023, ENISA va avea atribuții suplimentare. Deși aceste atribuții ar fi acoperite de mandatul ENISA, ele vor genera un volum de muncă suplimentar pentru agenție. Mai precis, pe lângă atribuțiile sale actuale, în temeiul propunerii Comisiei de revizuire a Directivei NIS, ENISA va fi însărcinată, printre altele, (i) cu elaborarea și menținerea unui registru european al vulnerabilităților [articolul 6 alineatul (2)], (ii) cu asigurarea secretariatului Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (CyCLONe) (articolul 14) și cu publicarea unui raport anual privind situația în materie de securitate cibernetică în UE (articolul 15), (iii) cu sprijinirea organizării de evaluări *inter pares* între statele membre (articolul 16), (iv) cu colectarea de date agregate privind incidentele de la statele membre și cu emiterea unor orientări tehnice [articolul 20 alineatul (9)], (v) cu crearea și menținerea unui registru pentru entitățile care furnizează servicii transfrontaliere (articolul 25).

Prin urmare, se va face o cerere de 5 ENI suplimentare începând cu 2022, cu bugetul corespunzător pentru a acoperi aceste noi posturi.

– ☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

– ☐X Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

	Anul **N** [65] **2022**	Anul **N+1** **2023**	Anul **N+2** **2024**	Anul **N+3** **2025**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6) **2026** **2027**			**TOTAL**
Agenți temporari (grade AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Agenți temporari (grade AST)								
Agenți contractuali	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Experți naționali detașați								
TOTAL	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

65 Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

Cerințe privind personalul (ENI):

	Anul **N** [66] **2022**	Anul **N+1** **2023**	Anul **N+2** **2024**	Anul **N+3** **2025**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6) **2026** **2027**			**TOTAL**
Agenți temporari (grade AD)	3	3	3	3	3	3		**18**
Agenți temporari (grade AST)								
Agenți contractuali	2	2	2	2	2	2		**12**
Experți naționali detașați								
TOTAL	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Necesarul de resurse umane estimat pentru DG-ul sub tutela căruia se află agenția

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

– ☐ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimarea se exprimă în numere întregi (sau cel mult cu o zecimală)

	Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)		
• **Posturi din schema de personal (funcționari și agenți temporari)**							
XX 01 01 01 (la sediu și în reprezentanțele Comisiei)							
XX 01 01 02 (în delegații)							
XX 01 05 01 (cercetare indirectă)							
10 01 05 01 (cercetare directă)							

66 Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

• Personal extern (în echivalent normă întreagă: ENI)[67]							
XX 01 02 01 (AC, END, INT din „pachetul global")							
XX 01 02 02 (AC, AL, END, INT și JPD în delegații)							
XX 01 04 ***yy***[68]	- la sediu[69]						
	- în delegații						
XX 01 05 02 (AC, END, INT - cercetare indirectă)							
10 01 05 02 (AC, INT, END - cercetare directă)							
Alte linii bugetare (a se preciza)							
TOTAL							

XX este domeniul de politică sau titlul din buget în cauză.

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând cont de constrângerile bugetare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și personal temporar	
Personal extern	

Descrierea metodei de calcul al costului pentru unitățile ENI ar trebui inclusă în anexa V secțiunea 3.

67 AC = agent contractual; AL = agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = tânăr profesionist în delegații.

68 Subplafonul pentru personal extern acoperit din creditele operaționale (fostele linii „BA").

69 În principal pentru fondurile structurale, Fondul european agricol pentru dezvoltare rurală (FEADR) și Fondul european pentru pescuit (FEP).

3.2.4. Compatibilitatea cu actualul cadru financiar multianual

– ☐X Propunerea/inițiativa este compatibilă cu cadrul financiar multianual existent.

– ☐ Propunerea/inițiativa necesită o reprogramare a rubricii corespunzătoare din cadrul financiar multianual.

A se explica reprogramarea necesară, precizându-se liniile bugetare vizate și sumele aferente. Propunerea este compatibilă cu CFM pentru perioada 2021-2027. Compensarea bugetului solicitat pentru a acoperi creșterea resurselor umane în cadrul ENISA se va realiza prin reducerea cu același cuantum a bugetului alocat programului Europa digitală la aceeași rubrică.

– ☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau la revizuirea cadrului financiar multianual[70].

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare vizate, precum și sumele aferente.

3.2.5. Contribuțiile terților

– Propunerea/inițiativa nu prevede cofinanțare din partea terților.

– Propunerea/inițiativa prevede cofinanțarea estimată mai jos:

milioane EUR (cu trei zecimale)

	Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			Total
A se preciza organismul care asigură cofinanțarea								
TOTAL credite cofinanțate								

[70] A se vedea articolele 11 și 17 din Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului de stabilire a cadrului financiar multianual pentru perioada 2014-2020.

3.3. Impactul estimat asupra veniturilor

– ☐ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☐ Propunerea/inițiativa are următorul impact financiar:

☐ asupra resurselor proprii

☐ asupra altor venituri

☐ vă rugăm să precizați dacă veniturile sunt alocate unor linii de cheltuieli

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul financiar în curs	Impactul propunerii/inițiativei[71]						
		Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)		
Articolul …..								

Pentru veniturile diverse „alocate”, a se preciza linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate).

A se preciza metoda de calcul al impactului asupra veniturilor.

[71] În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sumele brute după deducerea unei cote de 20 % pentru costurile de colectare.