REGULAMENTUL (UE) 2019/881 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 17 aprilie 2019

privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică)

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European ([1]),

având în vedere avizul Comitetului Regiunilor ([2]),

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

întrucât:

(1) Rețelele și sistemele informatice și rețelele și serviciile de comunicații îndeplinesc un rol vital pentru societate și au devenit coloana vertebrală a creșterii economice. Tehnologia informației și comunicațiilor (TIC) stă la baza sistemelor complexe care sprijină activitățile de zi cu zi ale societății, asigură funcționarea economiei în sectoare-cheie cum ar fi sănătatea, energia, finanțele și transporturile și, mai ales, susține funcționarea pieței interne.

(2) În prezent, rețelele și sistemele informatice sunt utilizate la scară generală de cetățenii, organizațiile și întreprinderile din întreaga Uniune. Digitalizarea și conectivitatea sunt pe cale să devină caracteristici principale ale unui număr tot mai mare de produse și servicii, preconizându-se că, odată cu apariția internetului obiectelor, un număr extrem de mare de dispozitive digitale conectate vor intra în folosință în Uniune în următorul deceniu. Deși numărul dispozitivelor conectate la internet este în creștere, securitatea și reziliența nu sunt incluse suficient din faza de concepere, ceea ce duce la o securitate cibernetică insuficientă. În acest context, din cauză că certificarea nu este utilizată decât într-o măsură limitată, utilizatorii persoane fizice, organizații sau întreprinderi nu dispun de suficiente informații despre caracteristicile de securitate cibernetică ale produselor TIC, serviciilor TIC și proceselor TIC, ceea ce erodează încrederea în soluțiile digitale. Rețelele și sistemele informatice sunt capabile să susțină toate aspectele vieților noastre și de a determina creșterea economică a Uniunii. Acestea sunt elemente fundamentale pentru realizarea pieței unice digitale.

(3) Creșterea gradului de digitalizare și conectivitate duce la agravarea riscurilor pentru securitatea cibernetică, societatea, în general, devenind astfel mai vulnerabilă la amenințările cibernetice, iar pericolele cu care se confruntă persoanele fizice, mai ales persoanele vulnerabile precum copiii, fiind extrem de mari. Pentru a atenua riscurile menționate, este necesar să fie luate toate măsurile pentru îmbunătățirea securității cibernetice în Uniune, astfel încât rețelele și sistemele informatice, rețelele de comunicații, produsele, serviciile și dispozitivele digitale utilizate de cetățeni, organizații și întreprinderi – de la întreprinderile mici și mijlocii (IMM-uri), astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei ([4]), la operatorii de infrastructuri critice – să fie mai bine protejate împotriva amenințărilor cibernetice.

([1]) JO C 227, 28.6.2018, p. 86.
([2]) JO C 176, 23.5.2018, p. 29.
([3]) Poziția Parlamentului European din 12 martie 2019 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 9 aprilie 2019.
([4]) Recomandarea Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

(4) Punând la dispoziția publicului informații relevante, Agenția Uniunii Europene pentru Securitatea Rețelelor Informatice și a Informațiilor (ENISA), instituită prin Regulamentul (UE) nr. 526/2013 al Parlamentului European și al Consiliului ([5]) contribuie la dezvoltarea sectorului securității cibernetice în Uniune, mai ales în ceea ce privește IMM-urile și întreprinderile nou-înființate. ENISA ar trebui să depună eforturi să coopereze mai îndeaproape cu universitățile și cu institutele de cercetare, pentru a contribui la reducerea dependenței de produse și servicii de securitate cibernetică din afara Uniunii, precum și la consolidarea lanțurilor de aprovizionare din interiorul Uniunii.

(5) În condițiile în care atacurile cibernetice sunt în creștere, o economie și o societate conectate mai vulnerabile la amenințările și atacurile cibernetice necesită protecție mai puternică. Cu toate acestea, deși atacurile cibernetice sunt adesea transfrontaliere, competența și răspunsurile oferite de politicile autorităților de securitate cibernetică și de aplicare a legii sunt predominant naționale. Incidentele de mare amploare ar putea să perturbe furnizarea serviciilor esențiale pe întregul teritoriu al Uniunii. Aceasta necesită răspunsul și gestionarea crizelor la nivelul Uniunii în mod eficace și coordonat, bazându-se pe politicile specifice și pe instrumentele mai generale de solidaritate europeană și asistență reciprocă. În plus, pentru factorii de decizie politică, pentru industrie și pentru utilizatori este important să existe o evaluare periodică a situației în materie de securitate cibernetică și reziliență în Uniune, bazată de la date fiabile la nivelul Uniunii, precum și prognoze sistematice ale evoluțiilor, provocărilor și amenințărilor viitoare, la nivelul Uniunii și la nivel mondial.

(6) Având în vedere intensificarea provocărilor în materie de securitate cibernetică cu care se confruntă Uniunea, este nevoie de un set cuprinzător de măsuri care să se bazeze pe acțiunile anterioare ale Uniunii și să promoveze obiective care se consolidează reciproc. Printre aceste obiective se numără sporirea și mai mult a capacitățile și a gradului de pregătire ale statelor membre și ale întreprinderilor, precum și îmbunătățirea cooperării, a schimbului de informații și coordonării între statele membre și instituțiile, organele, oficiile și agențiile Uniunii. Mai mult decât atât, amenințările cibernetice nu se opresc la frontiere, motiv pentru care este necesară dezvoltarea capacităților la nivelul Uniunii care ar putea completa acțiunea statelor membre, în special în cazul incidentelor și al crizelor cibernetice transfrontaliere de mare amploare, luând în considerare totodată importanța de a se menține și de a se consolida și mai mult capacitățile naționale de a răspunde la amenințările cibernetice, oricare ar fi amploarea acestora.

(7) De asemenea, sunt necesare eforturi suplimentare pentru a spori gradul de sensibilizare a cetățenilor, organizațiilor și întreprinderilor cu privire la aspectele legate de securitatea cibernetică. În plus, având în vedere că incidentele subminează încrederea în furnizorii de servicii digitale și chiar în piața unică digitală, mai ales în rândul consumatorilor, ar trebui consolidată și mai mult încrederea, oferind în mod transparent informații despre nivelul de securitate al produselor TIC, serviciilor TIC și proceselor TIC, subliniind că nici măcar un nivel ridicat de securitate cibernetică nu poate garanta că un produs TIC, un serviciu TIC sau un proces TIC este pe deplin sigur. O creștere a încrederii poate fi facilitată printr-o certificare la nivelul Uniunii care să prevadă cerințe comune în materie de securitate cibernetică și criterii de evaluare aplicabile pe toate piețele naționale și în toate sectoarele.

(8) Securitatea cibernetică nu e o chestiune legată numai de tehnologie, comportamentul uman fiind la fel de important. Din acest motiv, ar trebui promovată intens „igiena cibernetică”, și anume simple măsuri de rutină care, atunci când sunt introduse și aplicate cu regularitate de cetățeni, de organizații și de întreprinderi, reduc la minimum expunerea acestora la riscurile pe care le presupun amenințările cibernetice.

(9) În scopul consolidării structurilor Uniunii de securitate cibernetică, este important să se mențină și să se dezvolte capacitățile statelor membre de a răspunde în mod cuprinzător la amenințările cibernetice, inclusiv la incidentele transfrontaliere.

(10) Întreprinderile și consumatorii individuali ar trebui să dispună de informații exacte despre nivelul de asigurare la care a fost certificată securitatea produselor TIC, serviciilor TIC și proceselor TIC. În același timp, niciun produs TIC sau serviciu TIC nu este pe deplin sigur din punct de vedere cibernetic și este necesar ca normele de bază de igienă cibernetică să fie promovate și să li se acorde prioritate. Având în vedere disponibilitatea tot mai mare a dispozitivelor aferente internetului obiectelor, sectorul privat poate lua în mod voluntar o serie de măsuri pentru a consolida încrederea în produsele TIC, serviciile TIC și procesele TIC.

(11) Produsele și sistemele TIC moderne integrează adeseori una sau mai multe tehnologii și componente terțe, cum ar fi module software, biblioteci sau interfețe de programare a aplicațiilor, sau se bazează pe acestea. Această dependență ar putea cauza riscuri suplimentare pentru securitatea cibernetică, dat fiind că vulnerabilitățile prezente în componentele terțe pot afecta și securitatea produselor TIC, a serviciilor TIC și a proceselor TIC. În numeroase cazuri, identificarea și documentarea unor astfel de dependențe le permite utilizatorilor finali de produse TIC, servicii TIC și procese TIC să își îmbunătățească activitățile de gestionare a riscurilor pentru securitatea cibernetică, îmbunătățind, de exemplu, gestionarea vulnerabilității în materie de securitate cibernetică și procedurile de remediere a acesteia.

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

(12) Organizațiile, producătorii sau furnizorii implicați în conceperea și dezvoltarea produselor TIC, serviciilor TIC și proceselor TIC ar trebui încurajați să introducă măsuri încă din primele etape de concepere și dezvoltare, să protejeze de la bun început, în cel mai înalt grad posibil, securitatea respectivelor produse, servicii și procese, astfel încât producerea unor atacuri cibernetice să fie prezumată, iar impactul acestora să fie anticipat și redus la minimum (denumită în continuare „securitate începând cu momentul conceperii"). Ar trebui să se asigure securitatea pe întregul ciclu de viață al produsului TIC, serviciului TIC și procesului TIC, printr-o evoluție constantă a proceselor de concepere și de dezvoltare, pentru a se reduce riscul de prejudicii cauzate de exploatarea rău intenționată.

(13) Întreprinderile, organizațiile și sectorul public ar trebui să configureze produsele TIC, serviciile TIC sau procesele TIC pe care le concep astfel încât să asigure un nivel mai ridicat de securitate, care să îi permită primul utilizator să primească o configurație intrinsecă cu setările cu cel mai ridicat nivel de securitate posibil (denumită în continuare „securitate implicită") și să reducă astfel sarcina utilizatorilor de a-și configura în mod corespunzător un produs TIC, un serviciu TIC sau un proces TIC. Securitatea implicită nu ar trebui să necesite o configurare extensivă, o înțelegere tehnică specifică sau un comportament neevident din partea utilizatorului, ci ar trebui să funcționeze cu ușurință și în mod fiabil atunci când este implementată. Dacă, de la caz la caz, în urma unei analize a riscurilor și a utilizării se constată că o astfel de configurare implicită nu este fezabilă, ar trebui să li se recomande utilizatorilor să aleagă configurația cu cel mai ridicat nivel de securitate.

(14) Regulamentul (CE) nr. 460/2004 al Parlamentului European și al Consiliului ([6]) a instituit ENISA cu scopul de a contribui la obiectivele de asigurare a unui nivel ridicat și eficace al securității rețelelor și a informațiilor în Uniune și la dezvoltarea unei culturi a securității rețelelor și a informațiilor, în beneficiul cetățenilor, al consumatorilor, al întreprinderilor și al administrațiilor publice. Regulamentul (CE) nr. 1007/2008 al Parlamentului European și al Consiliului ([7]), a prelungit mandatul ENISA până în martie 2012. Regulamentul (UE) nr. 580/2011 al Parlamentului European și al Consiliului ([8]) a prelungit din nou mandatul ENISA până la 13 septembrie 2013. Regulamentul (UE) nr. 526/2013 a prelungit mandatul ENISA până la 19 iunie 2020.

(15) Uniunea a luat deja măsuri importante pentru a asigura securitatea cibernetică și a crește încrederea în tehnologiile digitale. În 2013 a fost adoptată Strategia de securitate cibernetică a Uniunii Europene, menită să orienteze politicile prin care Uniunea răspunde la amenințările cibernetice și riscurile pentru securitatea cibernetică. În cadrul eforturilor depuse pentru a proteja mai bine cetățenii în mediul online, primul act legislativ al Uniunii în domeniul securității cibernetice a fost adoptat în 2016sub forma Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului ([9]). Directiva (UE) 2016/1148 a instituit cerințe privind capacitățile naționale în domeniul securității cibernetice, a creat primele mecanisme de intensificare a cooperării strategice și operaționale între statele membre și a introdus obligații privind măsurile de securitate și notificările incidentelor în sectoare vitale pentru economie și societate, cum ar fi energia, transporturile, furnizarea și distribuirea de apă potabilă, băncile, infrastructurile pieței financiare, asistența medicală, infrastructurile digitale, precum și furnizorii de servicii digitale esențiale (motoarele de căutare, serviciile de *cloud computing* și piețele online).

ENISA a primit un rol esențial de sprijinire a punerii în aplicare a directivei respective. În plus, combaterea eficace a criminalității informatice se numără printre prioritățile importante ale Agendei europene privind securitatea, contribuind la obiectivul general de obținere a unui nivel ridicat de securitate cibernetică. Alte acte juridice, cum ar fi Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([10]), Directivele 2002/58/CE ([11]) și (UE) 2018/1972 ([12]) ale Parlamentului European și ale Consiliului, contribuie, de asemenea, la un nivel înalt de securitate cibernetică în cadrul pieței unice digitale.

([6]) Regulamentul (CE) nr. 460/2004 al Parlamentului European și al Consiliului din 10 martie 2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (JO L 77, 13.3.2004, p. 1).

([7]) Regulamentul (CE) nr. 1007/2008 al Parlamentului European și al Consiliului din 24 septembrie 2008 de modificare a Regulamentului (CE) nr. 460/2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor, în ceea ce privește durata de funcționare a acesteia (JO L 293, 31.10.2008, p. 1).

([8]) Regulamentul (UE) nr. 580/2011 al Parlamentului European și al Consiliului din 8 iunie 2011 de modificare a Regulamentului (CE) nr. 460/2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor, în ceea ce privește durata de funcționare a acesteia (JO L 165, 24.6.2011, p. 3).

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

([10]) 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).

([11]) 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).

([12]) 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).

(16) De la adoptarea Strategiei de securitate cibernetică a Uniunii Europene, în 2013, și de la ultima revizuire a mandatului ENISA, contextul general de politici a cunoscut schimbări semnificative, întrucât mediul mondial a devenit mai incert și mai puțin sigur. În acest context și în contextul dezvoltării pozitive a rolului ENISA drept punct de referință în materie de consiliere și de expertiză și drept facilitatoare a cooperării și a consolidării capacităților, precum și în cadrul noii politici de securitate cibernetică a Uniunii, este necesar să se revizuiască mandatul ENISA pentru a stabili rolul ce îi revine în ecosistemul de securitate cibernetică rezultat în urma acestor evoluții și pentru a oferi garanția că ENISA contribuie în mod eficace la răspunsul Uniunii la provocările în materie de securitate cibernetică ce își au originea în transformarea radicală a naturii amenințărilor cibernetice, pentru care, astfel cum se recunoaște în evaluarea ENISA, mandatul actual nu este suficient.

(17) ENISA astfel cum este instituită prin prezentul regulament ar trebui să succeadă ENISA astfel cum a fost instituită prin Regulamentul (UE) nr. 526/2013. ENISA ar trebui să ducă la îndeplinire atribuțiile care îi sunt conferite prin prezentul regulament și prin alte acte juridice ale Uniunii din domeniul securității cibernetice, printre altele prin furnizarea de consiliere și expertiză și prin exercitarea rolului de centru de informare și de cunoștințe al Uniunii. ENISA ar trebui să promoveze schimbul de bune practici între statele membre și părțile interesate din sectorul privat, oferind sugestii în materie de politici Comisiei și statelor membre, acționând ca punct de referință pentru inițiativele de politică sectorială ale Uniunii în ceea ce privește aspectele legate de securitatea cibernetică, încurajând cooperarea operațională între statele membre, precum și între statele membre și instituțiile, organele, oficiile și agențiile Uniunii.

(18) În cadrul Deciziei (CE, Euratom) 2004/97, adoptată de comun acord de reprezentanții statelor membre, reuniți la nivel de șefi de stat sau de guvern ([13]), reprezentanții statelor membre au decis că ENISA își va avea sediul într-un oraș din Grecia care urma să fie stabilit de guvernul elen. Statul membru gazdă al ENISA ar trebui să asigure cele mai bune condiții posibile pentru funcționarea optimă și în mod eficient a ENISA. Pentru îndeplinirea adecvată și eficientă a atribuțiilor sale, pentru recrutarea și menținerea personalului, precum și pentru consolidarea eficienței activităților sale de relaționare este indispensabil ca ENISA să aibă un amplasament adecvat care, printre altele, să ofere conexiuni de transport și facilități adecvate pentru soții sau soțiile și copiii care însoțesc membrii personalului ENISA. Dispozițiile necesare ar trebui stabilite într-un acord încheiat între ENISA și statul membru gazdă, după obținerea aprobării consiliului de administrație al ENISA.

(19) Având în vedere agravarea provocărilor și a riscurilor pentru securitatea cibernetică cu care se confruntă Uniunea, ar trebui crescute resursele financiare și umane alocate ENISA, care să corespundă consolidării rolului și atribuțiilor sale, precum și poziției sale critice în ecosistemul de organizații care apără ecosistemul digital al Uniunii, astfel încât ENISA să își poată îndeplini cu eficacitate atribuțiile care i-au fost conferite prin prezentul regulament.

(20) ENISA ar trebui să dezvolte și să mențină un nivel ridicat de expertiză și să funcționeze ca punct de referință care să stabilească încrederea în piața unică grație independenței sale, calității consilierii acordate și informațiilor diseminate, transparenței procedurilor și a metodelor sale de operare, precum și eforturilor depuse în îndeplinirea atribuțiilor sale. ENISA ar trebui să sprijine activ eforturile depuse la nivel național și ar trebui să contribuie proactiv la eforturile depuse Uniunii, îndeplinindu-și totodată atribuțiile în deplină cooperare cu instituțiile, organele, oficiile și agențiile Uniunii și cu statele membre, evitând orice dublare a activităților și promovând sinergia. În plus, ENISA ar trebui să se bazeze pe informațiile primite de la sectorul privat și alte părți interesate relevante și pe cooperarea cu acestea. Este necesar să se stabilească printr-o serie de atribuții modul în care ENISA își realizează obiectivele, permițându-i în același timp să funcționeze flexibil.

(21) Pentru a putea sprijini în mod corespunzător cooperarea operațională între statele membre, ENISA ar trebui să își consolideze și mai mult capacitățile și aptitudinile tehnice și umane. ENISA ar trebui să își sporească know-how-ul și capacitățile. ENISA și statele membre ar putea, în mod voluntar, să elaboreze programe pentru experții naționali detașați la ENISA, să creeze rezerve de experți și să facă schimburi de personal.

(22) ENISA ar trebui să furnizeze asistență Comisiei sub formă de consiliere, avize și analize cu privire la toate chestiunile de competența Uniunii legate de elaborarea, actualizarea și revizuirea politicilor și legislației din domeniul securității cibernetice, precum și de aspectele sectoriale specifice din acest domeniu, pentru a consolida relevanța politicilor și a legislației Uniunii cu o dimensiune de securitate cibernetică și pentru a permite punerea acestora în aplicare în mod coerent la nivel național. ENISA ar trebui să acționeze ca punct de referință în ceea ce privește consilierea și expertiza pentru inițiativele de politică și legislative sectoriale ale Uniunii în cazul în care intervin chestiuni legate de securitatea cibernetică. ENISA ar trebui să informeze periodic Parlamentul European despre activitățile sale.

([13]) Decizia (CE, Euratom) 2004/97 adoptată de comun acord de reprezentanții statelor membre, reuniți la nivel de șefi de stat sau de guvern din 13 decembrie 2003 privind amplasarea sediilor anumitor oficii și agenții ale Uniunii Europene (JO L 29, 3.2.2004, p. 15).

(23) Nucleul public al internetului deschis, și anume principalele sale protocoale și infrastructură, care constituie un bun public global, oferă funcționalitatea esențială a internetului în ansamblu și susține funcționarea sa normală. ENISA ar trebui să sprijine securitatea nucleului public al internetului deschis și stabilitatea funcționării sale, inclusiv, printre altele, protocoalele-cheie (mai ales DNS, BGP și IPv6), exploatarea sistemului de nume de domenii (cum ar fi operarea tuturor domeniilor de nivel superior) și exploatarea zonei-rădăcină.

(24) Atribuția fundamentală a ENISA este de a promova punerea în aplicare coerentă a cadrului juridic relevant, în special punerea în aplicare eficace a Directivei (UE) 2016/1148 și a altor instrumente juridice relevante care conțin aspecte legate de securitatea cibernetică, fapt esențial pentru sporirea rezilienței cibernetice. Având în vedere evoluția rapidă a naturii amenințărilor cibernetice, este clar că statele membre trebuie să fie sprijinite printr-o abordare mai cuprinzătoare, bazată pe mai multe politici, a consolidării rezilienței cibernetice.

(25) ENISA ar trebui să furnizeze asistență statelor membre și instituțiilor, organelor, oficiilor și agențiilor Uniunii, venind în sprijinul eforturilor lor de a crea și de a consolida capacitățile și pregătirea necesare pentru a preveni, a detecta și a răspunde la amenințările cibernetice și incidentele și în ceea ce privește securitatea rețelelor și a sistemelor informatice. În special, ENISA ar trebui să sprijine dezvoltarea și consolidarea echipelor de intervenție în caz de incidente de securitate informatică (denumite în continuare „echipe CSIRT") naționale și ale Uniunii prevăzute în Directiva (UE) 2016/1148, astfel încât acestea să ajungă la un nivel comun ridicat de maturitate în Uniune. Activitățile desfășurate de ENISA în privința capacităților operaționale ale statelor membre ar trebui să sprijine activ măsurile luate de statele membre pentru a-și respecta obligațiile în temeiul Directivei (UE) 2016/1148 și, prin urmare, să nu li se substituie.

(26) ENISA ar trebui, de asemenea, să acorde asistență la elaborarea și actualizarea strategiilor în materie de securitate a rețelelor și a sistemelor informatice la nivelul Uniunii și, la cerere, la nivelul statelor membre, în special în ceea ce privește securitatea cibernetică, și ar trebui să promoveze diseminarea strategiilor respective și să monitorizeze punerea în aplicare a acestora. Totodată, ENISA ar trebui să contribuie la satisfacerea nevoilor de formare și de materiale de formare, inclusiv nevoile organismelor publice și, dacă este cazul, să asigure în mare măsură formarea formatorilor pe baza cadrului de competențe digitale pentru cetățeni pentru a ajuta statele membre și instituțiile, organele, oficiile și agențiile Uniunii să își dezvolte propriile capacități de formare.

(27) ENISA ar trebui să sprijine statele membre în domeniul sensibilizării și al educării în materie de securitate cibernetică, prin facilitarea unei cooperări mai strânse și a schimbului de bune practici între statele membre. Acest sprijin ar putea să constea în dezvoltarea unei rețele de puncte naționale de contact în domeniul educației și în dezvoltarea unei platforme de formare în materie de securitate cibernetică. Rețeaua de puncte naționale de contact în domeniul educației ar putea funcționa în cadrul rețelei ofițerilor naționali de legătură și ar putea constitui un punct de plecare pentru viitoarea coordonare între statele membre.

(28) ENISA ar trebui să furnizeze asistență grupului de cooperare creat prin Directiva (UE) 2016/1148 în îndeplinirea atribuțiilor sale, în special oferind expertiză, asigurând consiliere și facilitând schimbul de bune practici, printre altele în ceea ce privește identificarea operatorilor de servicii esențiale de către statele membre, precum și în legătură cu dependențele transfrontaliere în ceea ce privește riscurile și incidentele.

(29) Pentru a încuraja cooperarea între sectorul public și cel privat și cooperarea în cadrul acestuia din urmă, mai ales pentru a susține protejarea infrastructurilor critice, ENISA ar trebui să sprijine schimbul de informații în cadrul sectoarelor și între acestea, mai ales în sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, furnizând bune practici și orientări despre instrumentele disponibile, proceduri și îndrumări despre modul de abordare a chestiunilor de reglementare legate de schimbul de informații, de exemplu prin facilitarea înființării unor centre sectoriale de schimb și de analiză de informații.

(30) Pe măsură ce impactul potențial negativ al vulnerabilităților produselor TIC, serviciilor TIC și proceselor TIC este în continuă creștere, descoperirea și remedierea acestor vulnerabilități joacă un rol important în reducerea riscului general pentru securitatea cibernetică. Cooperarea dintre organizații, producători sau furnizori de produse TIC, servicii TIC și procese TIC vulnerabile și membrii comunității de cercetare în domeniul securității cibernetice și autoritățile care descoperă astfel de vulnerabilități s-a dovedit că sporește în mod semnificativ atât ritmul descoperirii de vulnerabilități în produsele TIC, serviciile TIC și procesele TIC, cât și al remedierii acestora. Dezvăluirea coordonată a vulnerabilităților constă într-un proces structurat de cooperare în cadrul căruia vulnerabilitățile sunt raportate proprietarului sistemului informatic, dându-i organizației ocazia de a diagnostica și de a remedia vulnerabilitatea înainte ca informații detaliate referitoare la aceasta să fie divulgate părților terțe sau publicului. Procesul prevede de asemenea coordonarea între partea care descoperă vulnerabilitățile și organizație în ceea ce privește publicarea respectivelor vulnerabilități. Politicile coordonate de divulgare a vulnerabilităților ar putea juca un rol important în eforturile statelor membre de a consolida securitatea cibernetică.

(31) ENISA ar trebui să grupeze și să analizeze rapoartele naționale puse la dispoziție în mod voluntar de echipele CSIRT și de Centrul interinstituțional de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii instituit prin Acordul între Parlamentul European, Consiliul European, Consiliul Uniunii Europene, Comisia Europeană, Curtea de Justiție a Uniunii Europene, Banca Centrală Europeană, Curtea de Conturi Europeană, Serviciul European de Acțiune Externă, Comitetul Economic și Social European, Comitetul European al Regiunilor și Banca Europeană de Investiții privind organizarea și funcționarea unui Centru de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE) ([14]), în scopul de a contribui la stabilirea unor proceduri, limbaje și terminologii comune pentru schimbul de informații. În acest context, ENISA ar trebui de asemenea să atragă participarea sectorului privat, în cadrul Directivei (UE) 2016/1148 care prevede bazele schimbului voluntar de informații tehnice la nivel operațional în interiorul rețelei echipelor de intervenție în caz de incidente de securitate informatică (denumită în continuare „rețeaua CSIRT") creată prin directiva menționată.

(32) ENISA ar trebui să contribuie la răspunsurile la nivelul Uniunii în cazul unor incidente și de crize transfrontaliere de mare amploare legate de securitatea cibernetică. Această atribuție ar trebui îndeplinită în conformitate cu mandatul ENISA în temeiul prezentului regulament, iar statele membre ar trebui să convină asupra unei abordări în contextul Recomandării (UE) 2017/1584 a Comisiei ([15]) și al Concluziilor Consiliului din 26 iunie 2018 privind răspunsul coordonat al UE la incidentele și crizele de securitate cibernetică de mare amploare. Această atribuție ar putea include culegerea de informații relevante și exercitarea rolului de facilitare între rețeaua CSIRT și comunitatea tehnică, precum și cu factorii de decizie responsabili cu gestionarea situațiilor de criză. În plus, ENISA ar trebui să sprijine cooperarea operațională între statele membre în gestionarea din punct de vedere tehnic a incidentelor, la cererea unuia sau a mai multor state membre, facilitând schimbul de soluții tehnice relevante între statele membre și contribuind la comunicarea publică. ENISA ar trebui să sprijine cooperarea operațională testând modalitățile de desfășurare a cooperării prin exerciții periodice de securitate cibernetică.

(33) În sprijinirea cooperării operaționale, ENISA ar trebui să apeleze la expertiza tehnică și operațională de care dispune CERT-UE, prin intermediul unei cooperări structurate. O astfel de cooperare structurată s-ar putea baza pe expertiza de care dispune ENISA. Dacă este cazul, între cele două entități ar trebui încheiate acorduri specifice pentru a se stabili modalitățile practice de punere în aplicare a acestei cooperări și pentru a se evita dublarea activităților.

(34) În efectuarea atribuțiilor sale constând în sprijinirea cooperării operaționale în cadrul rețelei CSIRT, ENISA ar trebui să aibă posibilitatea de a oferi sprijin statelor membre, la cererea lor, de exemplu prin furnizarea de consiliere privind modul de îmbunătățire a capacităților lor de a preveni incidentele, de a le detecta și de a răspunde la acestea, prin facilitarea gestionării din punct de vedere tehnic a incidentelor care au un impact semnificativ sau substanțial sau prin asigurarea faptului că amenințările cibernetice și incidentele sunt analizate. ENISA ar trebui să faciliteze gestionarea din punct de vedere tehnic a incidentelor cu un impact semnificativ sau substanțial, mai ales sprijinind partajarea în mod voluntar a soluțiilor tehnice de către statele membre sau elaborând informații tehnice combinate, de exemplu soluții tehnice partajate în mod voluntar de statele membre. Recomandarea (UE) 2017/1584 invită statele membre să coopereze cu bună credință și să facă schimb de informații între ele și cu ENISA cu privire la incidentele și crizele de mare amploare legate de securitatea cibernetică, fără întârzieri nejustificate. Aceste informații ar trebui să constituie un ajutor suplimentar pentru ENISA în îndeplinirea atribuției sale de sprijinire a cooperării operaționale.

(35) Ca parte a cooperării periodice la nivel tehnic desfășurate pentru a sprijini cunoașterea de către Uniune a situației, ENISA, în strânsă cooperare cu statele membre, ar trebui să pregătească periodic rapoarte aprofundate asupra situației tehnice în materie de securitate cibernetică la nivelul UE referitor la incidente și amenințări cibernetice, pe baza informațiilor disponibile în mod public, a propriei analize și a rapoartelor care i-au fost transmise de echipele CSIRT ale statelor membre sau de punctele unice de contact naționale privind securitatea rețelelor și a sistemelor informatice (denumite în continuare „punctele unice de contact") prevăzute de Directiva (UE) 2016/1148, în ambele cazuri în mod voluntar, de Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol și CERT-UE și, după caz, de Centrul de situații și de analiză a informațiilor al Uniunii Europene (INTCEN UE) din cadrul Serviciului European de Acțiune Externă. Raportul ar trebui să fie pus la dispoziția Consiliului, Comisiei, Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate și ale rețelei CSIRT.

(36) Sprijinul acordat de ENISA, la cererea statelor membre afectate, pentru anchetele tehnice *ex post* privind incidentele care au consecințe semnificative sau substanțiale ar trebui să se axeze pe prevenirea viitoarelor incidente. Statele membre afectate ar trebui să furnizeze informațiile și asistența necesare pentru a-i permite ENISA să sprijine anchetele tehnice într-un mod eficace.

([14]) JO C 12, 13.1.2018, p. 1.

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

(37) Statele membre pot invita întreprinderile afectate de incident să coopereze furnizând ENISA informațiile și asistența necesare, fără a aduce atingere dreptului lor de a proteja informații sensibile din punct de vedere comercial și informații relevante pentru securitatea publică.

(38) Pentru a înțelege mai bine provocările din domeniul securității cibernetice și pentru a oferi consiliere strategică pe termen lung statelor membre și instituțiilor, organelor, oficiilor și agențiilor Uniunii, este necesar ca ENISA să analizeze riscurile pentru securitatea cibernetică actuale și pe cele emergente. În acest scop, ENISA ar trebui ca în cooperare cu statele membre și, după caz, cu organismele de statistică și cu alte entități să culeagă informațiile relevante care sunt puse la dispoziția publicului sau care sunt partajate în mod voluntar, să efectueze analize privind tehnologiile emergente și să furnizeze evaluări tematice privind impactul societal, juridic, economic și în materie de reglementare al inovațiilor tehnologice asupra securității rețelelor și informațiilor, în special asupra securității cibernetice. În plus, ENISA ar trebui să sprijine statele membre și instituțiile, organele, oficiile și agențiile Uniunii în ceea ce privește identificarea riscurilor pentru securitatea cibernetică emergente și prevenirea incidentelor, prin efectuarea unor analize ale amenințărilor cibernetice, vulnerabilităților și incidentelor.

(39) Pentru a spori reziliența Uniunii, ENISA ar trebui să vizeze excelența în domeniul securității cibernetice a infrastructurilor, și în special să sprijine sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, precum și a celor utilizate de furnizorii de servicii digitale enumerați în anexa III la directiva menționată, prin furnizarea de consiliere, emiterea de orientări și schimbul de bune practici. Pentru a asigura un acces mai ușor la informații mai bine structurate privind riscurile pentru securitatea cibernetică și măsurile corective posibile, ENISA ar trebui să creeze și să întrețină „platforma de informare" a Uniunii, un portal de tip ghișeu unic care să permită publicului să obțină informațiile despre securitatea cibernetică ce provin de la instituțiile, organele, oficiile și agențiile Uniunii și cele naționale. Facilitarea accesului la informații mai bine structurate despre riscurile pentru securitatea cibernetică și despre măsurile corective posibile ar putea de asemenea să ajute statele membre să își consolideze capacitățile și să își alinieze practicile, sporindu-și astfel reziliența generală la atacurile cibernetice.

(40) ENISA ar trebui să contribuie la sensibilizarea publicului în privința riscurilor pentru securitatea cibernetică, inclusiv printr-o campanie la nivelul UE de sensibilizare și prin promovarea educării, și să furnizeze, în atenția cetățenilor, organizațiilor și întreprinderilor, orientări privind bunele practici care trebuie adoptate de fiecare utilizator în parte. De asemenea, ENISA ar trebui să contribuie la promovarea bunelor practici și soluții, care să includă igiena cibernetică și alfabetizarea cibernetică, în rândul cetățenilor, organizațiilor și întreprinderilor, prin culegerea și analizarea informațiilor aflate la dispoziția publicului referitoare la incidentele semnificative și prin întocmirea și publicarea de rapoarte și orientări pentru cetățeni, organizații și întreprinderi pentru a îmbunătăți nivelul global de pregătire și de reziliență al acestora. Totodată, ENISA ar trebui să depună eforturi pentru a le oferi consumatorilor informații relevante despre sistemele de certificare aplicabile, furnizându-le, de exemplu, orientări și recomandări. În plus, ENISA ar trebui să organizeze, în concordanță cu Planul de acțiune pentru educația digitală instituit prin Comunicarea Comisiei din 17 ianuarie 2018 și în cooperare cu statele membre și instituțiile, organele, oficiile și agențiile ale Uniunii, activități de informare și campanii publice periodice de educație pentru utilizatorii finali, având ca scop promovarea unor comportamente online mai sigure ale persoanelor și alfabetizarea digitală, precum și sensibilizarea cu privire la eventualele amenințări cibernetice, inclusiv activitățile infracționale online, cum ar fi atacurile de tip *phishing*, rețelele *botnet*, fraudele financiare și bancare, incidentele de fraudă în privința datelor, precum și promovarea consilierii de bază privind autentificarea multifactorială, corectarea erorilor, criptarea, anonimizarea și protecția datelor.

(41) ENISA ar trebui să joace un rol central în accelerarea sensibilizării utilizatorilor finali cu privire la securitatea dispozitivelor și la utilizarea în condiții de securitate a serviciilor, și ar trebui să promoveze securitatea din faza de concepere și protejarea vieții private din faza de concepere la nivelul Uniunii. Pentru a îndeplini acest obiectiv, ENISA ar trebui să utilizeze în mod optim bunele practici și experiențele, mai ales bunele practici și experiențele instituțiilor universitare și ale cercetătorilor din domeniul securității informatice.

(42) Pentru a sprijini întreprinderile din sectorul securității cibernetice, precum și utilizatorii de soluții de securitate cibernetică ENISA ar trebui să înființeze un „observator al pieței" și să asigure întreținerea acestuia, efectuând analize periodice ale principalelor tendințe ale pieței securității cibernetice, atât la nivelul cererii, cât și la nivelul ofertei, și diseminând informații referitoare la aceste tendințe.

(43) ENISA ar trebui să contribuie la eforturile Uniunii de cooperare cu organizațiile internaționale, precum și în cadrele relevante de cooperare internațională din domeniul securității cibernetice. Îndeosebi, ENISA ar trebui să contribuie, după caz, la cooperarea cu organizații precum OCDE, OSCE și NATO. Această cooperare ar putea include exerciții comune de securitate cibernetică și coordonarea comună a răspunsului la incidente. Aceste activități urmează să se desfășoare cu respectarea pe deplin a principiilor de incluziune, reciprocitate și autonomie decizională ale Uniunii, fără a se aduce atingere caracterului specific al politicii de securitate și apărare din oricare stat membru.

(44) Pentru a asigura îndeplinirea în totalitate a obiectivelor sale, ENISA ar trebui să colaboreze cu autoritățile de supraveghere ale Uniunii și cu alte autorități competente din Uniune, cu instituțiile, organele, oficiile și agențiile Uniunii, inclusiv cu CERT-UE, EC3, Agenția Europeană de Apărare (AEA), Agenția pentru Sistemul Global de Navigație prin Satelit European (Agenția GNSS European), Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC), Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă (eu-LISA), Banca Centrală Europeană (BCE), Autoritatea Bancară Europeană (ABE), Comitetul european pentru protecția datelor, Agenția pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei (ACER), Agenția Uniunii Europene pentru Siguranța Aviației (AESA) și orice altă agenție a Uniunii implicată în securitatea cibernetică. ENISA ar trebui, de asemenea, să colaboreze cu autoritățile care îndeplinesc atribuții de protecție a datelor pentru a face schimb de know-how și de bune practici și ar trebui să ofere consiliere privind aspectele legate de securitatea cibernetică ce ar putea avea un impact asupra activității acestora. Reprezentanții autorităților naționale și ale Uniunii responsabile de aplicarea legii și de protecția datelor ar trebui să fie eligibili pentru a fi reprezentați în Grupul consultativ al ENISA. În activitatea sa de colaborare cu autoritățile responsabile de aplicarea legii, cu privire la aspectele de securitate a rețelelor și a informațiilor care ar putea avea un impact asupra activității acestora, ENISA ar trebui să respecte canalele de informații și rețelele existente.

(45) S-ar putea institui parteneriate cu instituțiile universitare care au inițiative de cercetare în domeniile relevante și ar trebui să existe canale adecvate pentru contribuțiile din partea organizațiilor consumatorilor și altor organizații, care ar trebui luate în considerare.

(46) ENISA, în rolul său de secretariat al rețelei CSIRT, ar trebui să sprijine echipele CSIRT ale statelor membre și CERT-UE în ceea ce privește cooperarea operațională legată de atribuțiile relevante ale rețelei CSIRT, astfel cum se menționează în Directiva (UE) 2016/1148. De asemenea, ENISA ar trebui să promoveze și să sprijine cooperarea dintre echipele CSIRT relevante în caz de incidente, atacuri sau întreruperi la nivelul rețelelor sau al infrastructurilor gestionate sau protejate de echipele CSIRT și care implică sau pot implica cel puțin două echipe CSIRT, ținând seama în mod corespunzător de procedurile standard de operare ale rețelei CSIRT.

(47) Pentru ca Uniunea să fie mai bine pregătită să răspundă la incidente, ENISA ar trebui să organizeze în mod periodic exerciții de securitate cibernetică la nivelul Uniunii și să ajute statele membre și instituțiile, organele, oficiile și agențiile Uniunii, la cererea acestora, să organizeze astfel de exerciții. O dată la doi ani ar trebui să se organizeze un exercițiu cuprinzător pe scară largă care să includă elemente tehnice, operaționale sau strategice. În plus, ENISA ar trebui să poată organiza periodic exerciții mai puțin cuprinzătoare, având același obiectiv de a spori nivelul de pregătire a Uniunii pentru răspunde incidentelor.

(48) ENISA ar trebui să își dezvolte și să își mențină în continuare expertiza în materie de certificare a securității cibernetice, pentru a sprijini politicile Uniunii din acest domeniu. ENISA ar trebui să se bazeze pe bunele practici existente și să promoveze adoptarea certificării de securitate cibernetică în Uniune. În acest scop, ea ar trebui, printre altele, să contribuie la instituirea și întreținerea unui cadru de certificare a securității cibernetice la nivelul Uniunii (denumit în continuare „cadru european de certificare a securității cibernetice”), pentru a crește transparența asigurării securității cibernetice a produselor TIC, a serviciilor TIC și a proceselor TIC, consolidând astfel încrederea în piața internă digitală și în competitivitatea sa.

(49) Politicile de securitate cibernetică eficiente ar trebui să se bazeze pe metode de evaluare a riscurilor bine puse la punct, atât în sectorul public, cât și în sectorul privat. Metodele de evaluare a riscurilor sunt utilizate la diferite niveluri, fără a exista o practică comună în ceea ce privește aplicarea lor eficientă. Promovarea și dezvoltarea bunelor practici pentru evaluarea riscurilor și pentru soluții interoperabile de gestionare a riscurilor în cadrul organizațiilor din sectorul public și privat vor spori nivelul de securitate cibernetică din Uniune. În acest scop, ENISA ar trebui să sprijine cooperarea dintre părțile interesate la nivelul Uniunii, facilitând eforturile acestora referitoare la elaborarea și adoptarea de standarde europene și internaționale în ceea ce privește gestionarea riscurilor și securitatea măsurabilă a produselor, sistemelor, rețelelor și serviciilor electronice, care, împreună cu software-ul, formează rețelele și sistemele informatice.

(50) ENISA ar trebui să încurajeze statele membre, producătorii sau furnizorii de produse TIC, de servicii TIC sau de procese TIC să își ridice standardele generale de securitate, astfel încât toți utilizatorii de internet să poată lua măsurile necesare pentru a-și asigura securitatea cibernetică personală și ar trebui să motiveze în acest sens. În special, producătorii și furnizorii de produse TIC, de servicii TIC și de procese TIC ar trebui să furnizeze toate actualizările necesare și să recheme, ar trebui să retragă sau să recicleze produsele TIC, serviciile TIC sau procesele TIC care nu îndeplinesc standardele de securitate cibernetică, iar importatorii și distribuitorii ar trebui să se asigure că produsele TIC, serviciile TIC și procesele TIC pe care le introduc pe piața Uniunii sunt conforme cerințelor aplicabile și nu prezintă niciun risc pentru consumatorii din Uniune.

(51) În cooperare cu autoritățile competente, ENISA ar trebui să poată difuza informații privind nivelul de securitate cibernetică al produselor TIC, al serviciilor TIC și al proceselor TIC oferite pe piața internă și ar trebui să poată emite avertismente care să vizeze producătorii sau furnizorii de produse TIC, de servicii TIC și de procese TIC și care să îi oblige să îmbunătățească securitatea produselor TIC, a serviciilor TIC și a proceselor TIC ale acestora, inclusiv securitatea cibernetică.

(52) ENISA ar trebui să ia în considerare pe deplin activitățile în curs de cercetare, dezvoltare și evaluare tehnologică, în special cele desfășurate în cadrul diferitelor inițiative de cercetare ale Uniunii, pentru a consilia instituțiile, organele, oficiile și agențiile Uniunii și, după caz, statele membre, la solicitarea acestora, cu privire la necesitățile și la prioritățile de cercetare din domeniul securității cibernetice. Pentru a identifica necesitățile și prioritățile în materie de cercetare, ENISA ar trebui de asemenea să consulte grupurile de utilizatori relevante. Mai precis, s-ar putea stabili o cooperare cu Consiliul European pentru Cercetare și cu Institutul European pentru Inovare și Tehnologie și cu Institutul pentru Studii de Securitate al Uniunii Europene.

(53) ENISA ar trebui să consulte periodic organizațiile de standardizare, mai ales organizațiile europene de standardizare, atunci când pregătește sistemele europene de certificare a securității cibernetice.

(54) Amenințările pentru securitatea cibernetică au o dimensiune mondială. Este necesară consolidarea cooperării internaționale pentru îmbunătățirea standardelor de securitate cibernetică, inclusiv prin definirea de norme de comportament și adoptarea de coduri de conduită comune, prin utilizarea de standarde internaționale, prin schimburi de informații și prin promovarea unei colaborări internaționale mai rapide ca răspuns la problemele de securitate a rețelelor și a informațiilor, precum și a unei abordări comune la nivel mondial a acestor probleme. În acest scop, ENISA ar trebui să sprijine continuarea implicării și cooperării Uniunii cu țări terțe și cu organizații internaționale, furnizând, după caz, expertiza și analiza necesară instituțiilor, organelor, oficiilor și agențiilor relevante ale Uniunii.

(55) ENISA ar trebui să fie în măsură să răspundă solicitărilor ad-hoc de consiliere și asistență care îi sunt adresate de statele membre și de instituțiile, organele, oficiile și agențiile Uniunii, legate de aspecte care țin de mandatul ENISA.

(56) Este rezonabil și se recomandă să se aplice anumite principii privind guvernanța ENISA pentru a respecta declarația comună și abordarea comună convenite în iulie 2012 de Grupul de lucru interinstituțional privind agențiile descentralizate ale UE, al căror scop este de a raționaliza activitățile agențiilor descentralizate și de a le îmbunătăți performanțele. Recomandările cuprinse în declarația comună și în abordarea comună ar trebui să se reflecte, după caz, în programele de activitate, evaluările și practicile administrative și de raportare ale ENISA.

(57) Consiliul de administrație, alcătuit din reprezentanți ai statelor membre și ai Comisiei, ar trebui să stabilească direcția generală a activităților ENISA și să se asigure că aceasta își îndeplinește atribuțiile în conformitate cu prezentul regulament. Consiliului de administrație ar trebui să i se încredințeze competențele necesare pentru întocmirea bugetului, verificarea execuției acestuia, adoptarea normelor financiare adecvate, stabilirea unor proceduri de lucru transparente pentru luarea deciziilor de către ENISA, adoptarea documentului unic de programare al ENISA, adoptarea propriului regulament de procedură, numirea directorului executiv, luarea deciziei cu privire la prelungirea sau încetarea mandatului directorului executiv.

(58) Pentru buna funcționare în condiții de eficacitate a ENISA, Comisia și statele membre ar trebui să se asigure că persoanele care urmează să fie numite în consiliul de administrație au nivelul adecvat de competență și de experiență profesională. Comisia și statele membre ar trebui, de asemenea, să depună eforturi pentru a limita rotația reprezentanților lor în consiliul de administrație, cu scopul de a asigura continuitatea activității acestuia.

(59) Pentru buna funcționare a ENISA este necesar ca numirea directorului executiv să fie făcută pe baza meritelor și aptitudinilor sale administrative și manageriale atestate, precum și a competenței și experienței relevante în domeniul securității cibernetice. Directorul executiv ar trebui să își ducă la îndeplinire atribuțiile în deplină independență. Directorul executiv ar trebui să elaboreze o propunere privind programul anual de activitate al ENISA, după consultări prealabile cu Comisia, și să ia toate măsurile necesare pentru a asigura punerea în aplicare corespunzătoare a programului de activitate respectiv. Directorul executiv ar trebui să întocmească un raport anual cuprinzând și punerea în aplicare a programului anual de activitate al ENISA, care să fie prezentat consiliului de administrație, să elaboreze un proiect de situație a estimărilor de venituri și cheltuieli ale ENISA și să execute bugetul. În plus, directorul executiv ar trebui să aibă opțiunea de a înființa grupuri de lucru ad-hoc pentru a aborda aspecte specifice, în special de natură științifică, tehnică, juridică sau socioeconomică. Se consideră drept necesară instituirea unui grup de lucru ad-hoc, mai ales în legătură cu pregătirea unei anumite propuneri de sistem european

de certificare a securității cibernetice (denumită în continuare „propuneri de sistem"). Directorul executiv ar trebui să se asigure că selecționarea membrilor grupurilor de lucru ad-hoc se realizează în conformitate cu cele mai înalte standarde de competență, urmărindu-se să se asigure o reprezentare echilibrată din perspectiva genului și corespunzătoare, în funcție de problemele specifice – între administrațiile publice ale statelor membre, instituțiile, organele, oficiile și agențiile Uniunii și sectorul privat, inclusiv industria, utilizatorii și experții universitari în domeniul securității rețelelor și a informațiilor.

(60) Comitetul executiv ar trebui să contribuie la funcționarea eficace a consiliului de administrație. În cadrul lucrărilor sale pregătitoare legate de deciziile consiliului de administrație, comitetul executiv ar trebui să examineze în detaliu informațiile relevante, să analizeze opțiunile disponibile și să ofere consiliere și soluții pentru pregătirea deciziilor relevante ale consiliului de administrație.

(61) ENISA ar trebui să aibă drept organism consultativ un grup consultativ al ENISA, pentru a asigura un dialog regulat cu sectorul privat, cu organizațiile de consumatori și cu alte părți interesate relevante. Grupul consultativ al ENISA, instituit de consiliul de administrație la propunerea directorului executiv, ar trebui să se concentreze pe probleme relevante pentru părțile interesate și să le aducă în atenția ENISA. Grupul consultativ al ENISA ar trebui să fie consultat în special în legătură cu proiectul de program anual de activitate al ENISA. Componența Grupului consultativ al ENISA și atribuțiile încredințate acestuia ar trebui să asigure faptul că părțile interesate sunt reprezentate într-o măsură suficientă în ceea ce privește activitatea ENISA.

(62) Ar trebui instituit Grupul părților interesate pentru certificarea securității cibernetice pentru a ajuta ENISA și Comisia să faciliteze consultarea părților interesate relevante. Grupul părților interesate pentru certificarea securității cibernetice ar trebui compus din membri care să reprezinte într-o proporție echilibrată industria, în ceea ce privește atât cererea, cât și oferta de produse TIC și servicii TIC, și care să includă îndeosebi IMM-uri, furnizorii de servicii digitale, organismele europene și internaționale de standardizare, organismele de acreditare naționale, autoritățile de supraveghere a protecției datelor și organismele de evaluare a conformității în temeiul Regulamentului (CE) nr. 765/2008 al Parlamentului European și al Consiliului ([16]), și mediul universitar și organizațiile consumatorilor.

(63) ENISA ar trebui să dispună de norme de prevenire și gestionare a conflictelor de interese. De asemenea, ENISA ar trebui să aplice dispozițiile relevante ale Uniunii privind accesul public la documente, prevăzute în Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului ([17]). Prelucrarea datelor cu caracter personal de către ENISA ar trebui să intre sub incidența Regulamentului (UE) 2018/1725 al Parlamentului European și al Consiliului ([18]). ENISA ar trebui să se conformeze dispozițiilor aplicabile instituțiilor, organelor, oficiilor și agențiilor Uniunii, precum și dispozițiilor legislațiilor naționale privind gestionarea informațiilor, în special a informațiilor sensibile neclasificate și a informațiilor clasificate ale Uniunii Europene (IUEC).

(64) Pentru a garanta autonomia și independența deplină a ENISA și a-i permite să îndeplinească atribuții suplimentare, inclusiv atribuții urgente neprevăzute, ar trebui să i se aloce ENISA un buget suficient și autonom, ale cărui venituri să provină în principal din contribuția Uniunii și din contribuții ale țărilor terțe care iau parte la activitățile ENISA. Un buget corespunzător este capital pentru asigurarea faptului că ENISA dispune de capacități suficiente pentru a-și îndeplini toate atribuțiile sporite și a-și realiza obiectivele. Majoritatea angajaților ENISA ar trebui să fie implicați direct în punerea în aplicare operațională a mandatului ENISA. Statul membru gazdă și oricare alt stat membru ar trebui să poată contribui în mod voluntar la bugetul ENISA. Procedura bugetară a Uniunii ar trebui să rămână aplicabilă în ceea ce privește toate subvențiile plătibile din bugetul general al Uniunii. De asemenea, Curtea de Conturi ar trebui să auditeze conturile ENISA pentru a asigura transparența și responsabilitatea.

(65) Certificarea securității cibernetice este importantă pentru sporirea securității produselor TIC, serviciilor TIC și proceselor TIC și a încrederii în acestea. Piața unică digitală și, mai ales, economia bazată pe date și internetul obiectelor pot prospera numai dacă publicul larg are încredere în faptul că astfel de produse, servicii și procese oferă un anumit nivel de asigurare a securității cibernetice. Autovehiculele conectate și automatizate, dispozitivele medicale electronice, sistemele industriale automatizate de control și rețelele inteligente sunt numai câteva exemple de sectoare în care certificarea este deja utilizată la scară largă sau poate fi utilizată în viitorul apropiat. Certificarea securității cibernetice este esențială și în sectoarele reglementate prin Directiva (UE) 2016/1148.

([16]) Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30).

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

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

(66) În comunicarea sa din 2016 intitulată „Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator”, Comisia a subliniat că sunt necesare produse și soluții de securitate cibernetică caracterizate prin calitate superioară, accesibilitatea prețului și interoperabilitate. Oferta de produse TIC, servicii TIC și procese TIC din cadrul pieței unice rămâne foarte fragmentată din punct de vedere geografic. Această fragmentare se explică prin faptul că sectorul securității cibernetice din Europa s-a dezvoltat de-a lungul timpului în principal pe baza cererii guvernamentale naționale. În plus, lipsa de soluții interoperabile (standarde tehnice), de practici și de mecanisme de certificare la nivelul Uniunii este una dintre lacunele care afectează piața unică în domeniul securității cibernetice. Acest lucru îngreunează competitivitatea întreprinderilor europene la nivel național, la nivelul Uniunii și la nivel mondial. De asemenea acest lucru reduce posibilitățile de alegere a tehnologiilor de securitate cibernetică viabile și utilizabile la care au acces persoanele fizice și întreprinderile. În mod similar, în Comunicarea din 2017 privind evaluarea la jumătatea perioadei a punerii în aplicare a strategiei privind piața unică digitală – O piață unică digitală conectată pentru toți, Comisia a evidențiat necesitatea ca produsele și sistemele conectate să fie sigure și a apreciat că prin crearea unui cadru european de securitate pentru TIC, care să stabilească norme privind modul de organizare a certificării de securitate a TIC în Uniune, internetul s-ar putea bucura în continuare de încredere și, totodată, actuala fragmentare a pieței interne ar putea fi contracarată.

(67) În prezent, certificarea securității cibernetice a produselor TIC, serviciilor TIC și proceselor TIC nu este utilizată decât într-o măsură limitată. Atunci când există, certificarea se aplică în principal la nivelul statelor membre sau în cadrul sistemelor instituite de sector. În acest context, un certificat eliberat de o autoritate națională de certificare a securității cibernetice nu este, în principiu, recunoscut de celelalte state membre. Prin urmare, este posibil ca întreprinderile să fie nevoite să își certifice produsele TIC, serviciile TIC și procesele TIC în fiecare dintre statele membre în care își desfășoară activitatea, de exemplu pentru a putea participa la procedurile de achiziții publice naționale, sporindu-și astfel cheltuielile. În plus, deși apar noi sisteme, nu pare să existe o abordare coerentă și holistică a aspectelor orizontale ale securității cibernetice, de exemplu în domeniul internetului obiectelor. Sistemele existente prezintă importante deficiențe și diferențe în ceea ce privește produsele vizate, nivelurile de asigurare, criteriile de fond și utilizarea efectivă, ceea ce împiedică funcționarea unor mecanisme de recunoaștere reciprocă în Uniune.

(68) S-au depus eforturi pentru ca certificatele să beneficieze de o recunoaștere reciprocă în cadrul Uniunii, dar acestea nu au fost decât parțial încununate de succes. Cel mai important exemplu în acest sens îl constituie Acordul de recunoaștere reciprocă (ARR) al Grupului înalților funcționari pentru securitatea sistemelor informatice (SOG-IS). Deși reprezintă cel mai important model de cooperare și de recunoaștere reciprocă din domeniul certificării de securitate, SOG-IS nu cuprinde decât unele state membre. Din această cauză, ARR al SOG-IS a avut o eficacitate limitată din perspectiva pieței interne.

(69) Prin urmare, este necesar să se adopte o abordare comună și să se instituie un cadru european de certificare a securității cibernetice prin care să se stabilească principalele cerințe orizontale pentru sistemele europene de certificare a securității cibernetice ce urmează să fie create și să se permită recunoașterea și utilizarea în toate statele membre a certificatelor europene de securitate cibernetică și a declarațiilor de conformitate UE pentru produse TIC, servicii TIC sau procese TIC. Procedând astfel, este esențial să se plece de la sistemele naționale și internaționale existente, precum și de la sistemele de recunoaștere reciprocă, mai ales SOG-IS, și să se înlesnească tranziția de la sistemele existente în cadrul acestora către sisteme din noul cadru european de certificare a securității cibernetice. Cadrul european de certificare a securității cibernetice ar trebui să aibă un dublu scop. În primul rând, ar trebui să contribuie la creșterea încrederii în produsele TIC, serviciile TIC și procesele TIC care au fost certificate în temeiul sistemelor europene de certificare de securitate cibernetică. În al doilea rând, ar trebui să evite multiplicarea de sisteme naționale de certificare a securității cibernetice ce se contrazic sau se suprapun și să permită astfel reducerea costurilor pentru întreprinderile care își desfășoară activitatea pe piața unică digitală. Sistemele europene de certificare a securității cibernetice ar trebui să fie nediscriminatorii și să se bazeze pe standarde europene sau internaționale, cu excepția cazului în care aceste standarde sunt ineficace sau inadecvate pentru îndeplinirea obiectivelor legitime ale Uniunii în această privință.

(70) Cadrul european de certificare a securității cibernetice ar trebui instituit în mod uniform în toate statele membre pentru a împiedica practica de căutare a certificării celei mai avantajoase, generată de nivelurile diferite de strictețe în state membre diferite.

(71) Sistemele europene de certificare a securității cibernetice ar trebui să se bazeze pe ceea ce există deja la nivel național și internațional și, dacă este necesar, pe specificațiile tehnice din foruri și consorții, culegând roadele actualelor puncte forte și evaluând și remediind punctele slabe.

(72) Este nevoie de soluții flexibile în materie de securitate cibernetică pentru ca industria să fie cu un pas înaintea amenințărilor cibernetice; prin urmare, toate sistemele de certificare ar trebui să fie concepute astfel încât să evite riscul de a fi rapid depășite.

(73) Comisia ar trebui să fie împuternicită să adopte sisteme europene de certificare a securității cibernetice în ceea ce privește grupuri specifice de produse TIC, servicii TIC și procese TIC. Aceste sisteme ar trebui să fie puse în aplicare și supervizate de către autoritățile naționale de certificare a securității cibernetice, iar certificatele eliberate în temeiul acestor sisteme ar trebui să fie valabile și recunoscute în întreaga Uniune. Sistemele de certificare gestionate de industrie sau de alte organizații private nu ar trebui să fie incluse în domeniul de aplicare al prezentului regulament. Cu toate acestea, organismele care gestionează sisteme de acest tip ar trebui să poată propune Comisiei să le ia în considerare ca bază pentru aprobarea lor ca sistem european de certificare a securității cibernetice.

(74) Dispozițiile prezentului regulament ar trebui să se aplice fără a aduce atingere dreptului Uniunii care prevede norme specifice privind certificarea produselor TIC, a serviciilor TIC și a proceselor TIC. În special, Regulamentul (UE) 2016/679 cuprinde dispoziții privind instituirea de mecanisme de certificare și introducerea de sigilii și mărci de protecție a datelor pentru a demonstra conformitatea cu regulamentul respectiv a operațiunilor de prelucrare efectuate de operatori și de persoanele împuternicite de aceștia. Aceste mecanisme de certificare și sigilii și mărci de protecție a datelor ar trebui să le permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor al produselor TIC, al serviciilor TIC și al proceselor TIC în cauză. Prezentul regulament nu aduce atingere certificării operațiunilor de prelucrare a datelor în temeiul Regulamentului (UE) 2016/679, inclusiv în cazul în care aceste operațiuni sunt integrate în produse TIC, servicii TIC și procese TIC.

(75) Sistemele europene de certificare a securității cibernetice ar trebui să aibă drept scop asigurarea conformității cu cerințele specificate a produselor TIC, serviciilor TIC și proceselor TIC certificate în temeiul unui astfel de sistem, pentru a proteja disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor stocate ori transmise sau prelucrate ori funcțiile sau serviciile oferite prin aceste produse, servicii și procese, sau accesibile prin intermediul lor pe durata întregului lor ciclu de viață. În prezentul regulament nu pot fi detaliate cerințele de securitate cibernetică referitoare la toate produsele TIC, serviciile TIC și procesele TIC. Produsele TIC, serviciile TIC și procesele TIC și necesitățile în materie de securitate cibernetică referitoare la acestea sunt atât de variate încât este foarte dificil să se elaboreze cerințe generale de securitate cibernetică care să fie valabile în toate circumstanțele. Prin urmare, este necesar să se adopte o noțiune largă și generală a securității cibernetice în scopul certificării, care ar trebui completată printr-o serie de obiective de securitate cibernetică specifice care să fie luate în considerare atunci când se concep sisteme europene de certificare a securității cibernetice. Modalitățile prin care aceste obiective vor fi atinse de produse TIC, servicii TIC și procese TIC specifice ar trebui detaliate și mai precis, într-o etapă ulterioară, la nivelul fiecărui sistem de certificare adoptat de Comisie, de exemplu prin trimitere la standarde sau la specificații tehnice dacă nu sunt disponibile standarde corespunzătoare.

(76) Specificațiile tehnice de utilizat în sistemele europene de certificare a securității cibernetice ar trebui să respecte cerințele prevăzute în anexa II la Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului ([19]). Cu toate acestea, unele abateri de la aceste cerințe ar putea fi considerate necesare în cazuri justificate corespunzător, când respectivele specificații tehnice sunt destinate utilizării într-un sistem european de certificare a securității cibernetice care face trimitere la nivelul de asigurare „ridicat”. Motivele care stau la baza acestor abateri ar trebui puse la dispoziția publicului.

(77) O evaluare a conformității este o procedură prin care se evaluează dacă au fost îndeplinite cerințele specifice referitoare la un produs TIC, serviciu TIC sau proces TIC. Această procedură este efectuată de o parte terță independentă, alta decât producătorul sau furnizorul produselor TIC, serviciilor TIC sau proceselor TIC care sunt evaluate. Un certificat european de securitate cibernetică ar trebui să fie eliberat în urma unei evaluări pozitive a unui produs TIC, serviciu TIC sau proces TIC. Un certificat european de securitate cibernetică ar trebui să fie considerat drept o confirmare a faptului că evaluarea s-a derulat în mod adecvat. În funcție de nivelul de asigurare, sistemul european de certificare a securității cibernetice ar trebui să indice dacă certificatul european de securitate cibernetică este eliberat de un organism privat sau de unul public. Evaluarea și certificarea de conformitate nu pot garanta în sine că produsele, serviciile TIC sau procesele TIC certificate îndeplinesc condițiile de securitate cibernetică. Acestea sunt, mai degrabă, proceduri și metodologii tehnice menite să ateste că produsele TIC, serviciile TIC și procesele TIC au fost testate și că îndeplinesc anumite cerințe de securitate cibernetică prevăzute în alte dispoziții, de exemplu în cadrul standardelor tehnice.

(78) Alegerea, de către utilizatorii certificatelor europene de securitate cibernetică, a certificării adecvate și a cerințelor de securitate aferente ar trebui să se bazeze pe o evaluare a riscurilor asociate cu utilizarea produselor TIC, serviciilor TIC sau proceselor TIC. Astfel, nivelul de asigurare ar trebui să fie corespunzător nivelului riscului asociat cu utilizarea preconizată a unui produs TIC, serviciu TIC sau proces TIC.

([19]) 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).

(79) Un sistem european de certificare a securității cibernetice ar putea să prevadă efectuarea unei evaluări de conformitate pe răspunderea exclusivă a producătorului sau a furnizorului de produse TIC, servicii TIC și procese TIC (denumită în continuare „autoevaluare a conformității"). În astfel de cazuri, este suficient ca producătorul sau furnizorul de produse TIC, servicii TIC și procese TIC să efectueze el însuși toate verificările pentru a asigura conformitatea produselor TIC, a serviciilor TIC sau a proceselor TIC cu sistemul european de certificare a securității cibernetice. Autoevaluarea conformității ar trebui considerată adecvată pentru produse TIC, servicii TIC și procese TIC având o complexitate redusă și care prezintă un risc scăzut pentru public, cum ar fi mecanisme de concepție și producție simple. În plus, autoevaluarea conformității ar trebui să fie permisă pentru produsele TIC, serviciile TIC și procesele TIC numai dacă acestea corespund unui nivel de asigurare „de bază".

(80) Un sistem european de certificare a securității cibernetice ar putea permite atât autoevaluarea conformității, cât și certificarea produselor TIC, a serviciilor TIC sau a proceselor TIC. În acest caz, sistemul ar trebui să prevadă modalități clare și ușor de înțeles, astfel încât consumatorii și alți utilizatori să diferențieze produsele TIC, serviciile TIC și procesele TIC pentru care producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC este răspunzător pentru evaluare, de produsele TIC, serviciile TIC și procesele TIC care sunt certificate de o parte terță.

(81) Producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC care efectuează o autoevaluare a conformității ar trebui să poată să întocmească și să semneze declarația de conformitate UE în cadrul procedurii de evaluare a conformității. Declarația de conformitate UE este un document care specifică faptul că un anumit produs TIC, serviciul TIC sau proces TIC este conform cu cerințele sistemului european de certificare a securității cibernetice. Prin eliberarea și semnarea declarației de conformitate UE, producătorul sau furnizorul își asumă răspunderea pentru conformitatea produsului TIC, a serviciului TIC sau a procesului TIC cu cerințele legale ale sistemului european de certificare a securității cibernetice. O copie a declarației de conformitate UE ar trebui transmisă autorității naționale de certificare a securității cibernetice și ENISA.

(82) Producătorii sau furnizorii de produse TIC, servicii TIC sau procese TIC ar trebui să pună la dispoziția autorității naționale competente de certificare a securității cibernetice, pe durata stabilită în sistemul european de certificare a securității cibernetice relevant, declarația de conformitate UE, documentația tehnică și toate celelalte informații relevante legate de conformitatea produselor TIC, serviciilor TIC sau proceselor TIC cu un sistem european de certificare a securității cibernetice. Documentația tehnică ar trebui să specifice cerințele aplicabile și să acopere, în măsura relevantă pentru evaluare, conceperea, producerea și exploatarea produsului TIC, a serviciului TIC sau a procesului TIC în măsura relevantă pentru autoevaluarea conformității. Documentația tehnică ar trebui să fie alcătuită astfel încât să permită evaluarea faptului că un produs TIC sau un serviciu TIC respectă cerințele relevante aplicabile în cadrul sistemului respectiv.

(83) Guvernanța cadrului european de certificare de securitate cibernetică ține seama de implicarea statelor membre și de implicarea corespunzătoare a părților interesate și stabilește rolul Comisiei în timpul planificării și al propunerii, solicitării, pregătirii, adoptării și revizuirii sistemelor europene de certificare a securității cibernetice.

(84) Comisia ar trebui să elaboreze, cu sprijinul Grupului european pentru certificarea securității cibernetice (ECCG) și al Grupului părților interesate pentru certificarea securității cibernetice și după o consultare deschisă și largă, un program de activitate etapizat la nivelul Uniunii pentru sistemele europene de certificare a securității cibernetice și să îl publice sub forma unui instrument fără caracter obligatoriu. Programul de activitate etapizat la nivelul Uniunii ar trebui să fie un document strategic care să permită mai ales industriei, autorităților naționale și organismelor de standardizare să pregătească în avans viitoare sisteme europene de certificare a securității cibernetice. Programul de activitate etapizat la nivelul Uniunii ar trebui să includă o prezentare multianuală a solicitărilor de propuneri de sisteme pe care Comisia intenționează să le transmită ENISA în baza unor considerente specifice, în vederea pregătirii. Comisia ar trebui să țină seama de programul de activitate etapizat la nivelul Uniunii atunci când își pregătește planul etapizat pentru standardizarea TIC și solicitările de standardizare adresate organizațiilor de standardizare europene. Ținând seama de rapiditatea cu care se introduc noile tehnologii și cu care acestea sunt, de apariția unor riscuri pentru securitatea cibernetică anterior necunoscute sau de evoluția legislației și a pieței, Comisia sau ECCG ar trebui să aibă dreptul să solicite ENISA să pregătească propuneri de sisteme care nu fuseseră incluse în programul de activitate etapizat la nivelul Uniunii. În astfel de situații, Comisia și ECCG ar trebui să evalueze și necesitatea unei asemenea solicitări, luând în considerare obiectivele generale ale prezentului regulament și necesitatea de a asigura continuitatea în ceea ce privește planificarea și utilizarea resurselor ENISA.

La primirea unei astfel de solicitări, ENISA ar trebui să pregătească fără întârzieri nejustificate propuneri de sisteme pentru, produse TIC, servicii TIC și procese TIC specifice. Comisia ar trebui să evalueze impactul pozitiv și negativ al solicitării sale asupra pieței specifice în cauză, mai ales impactul acestora asupra IMM-urilor, inovării, obstacolelor la intrare pe piața respectivă și costurilor pentru utilizatorii finali. Pe baza propunerii de sistem pregătite de ENISA, Comisia ar trebui să fie apoi împuternicită să adopte sistemul european de certificare a securității cibernetice prin intermediul unor acte de punere în aplicare. Ținând seama de scopul general și de obiectivele de securitate prevăzute în prezentul regulament, sistemele europene de certificare a securității cibernetice adoptate de Comisie ar trebui să specifice un set minim de elemente referitoare la obiectul, sfera de aplicare și funcționarea fiecărui sistem. Elementele respective ar trebui să includă, printre altele, sfera de aplicare și obiectul certificării de securitate cibernetică, inclusiv categoriile de produse TIC, servicii TIC și procese TIC care fac obiectul acesteia, specificații detaliate cu privire la cerințele de securitate cibernetică, de exemplu prin trimitere la standarde sau la specificații tehnice, criteriile specifice de evaluare și metodele de evaluare, precum și nivelul de asigurare vizat („de bază”, „substanțial” sau „ridicat”) și nivelurile de evaluare, după caz. ENISA ar trebui să poată să refuze o solicitare din partea ECCG. O astfel de decizie ar trebui adoptată de consiliul de administrație și motivată în mod corespunzător.

(85) ENISA ar trebui să întrețină un site web care să ofere informații despre sistemele europene de certificare a securității cibernetice și să le asigure publicitatea, conținând, printre altele, cererile de pregătire a unei propuneri de sistem, precum și observațiile primite în cadrul procesului de consultare derulat de ENISA în etapa de pregătire. Site-ul ar trebui să ofere informații și despre certificatele europene de securitate cibernetică și declarațiile de conformitate UE eliberate în temeiul prezentului regulament, inclusiv informații despre retragerea și expirarea acestor certificate europene de securitate cibernetică și declarații de conformitate UE. Site-ul ar trebui să indice și sistemele naționale de certificare a securității cibernetice care au fost înlocuite de un sistem european de certificare a securității cibernetice.

(86) Nivelul de asigurare al unui sistem european de certificare este temeiul încrederii că un produs TIC, serviciu TIC sau proces TIC îndeplinește cerințele de securitate ale unui sistem european de certificare a securității cibernetice specific. Pentru a asigura coerența cadrului european de certificare a securității cibernetice, un sistem european de certificare a securității cibernetice ar trebui să poată să specifice niveluri de asigurare pentru certificatele europene de securitate cibernetică și pentru declarațiile de conformitate UE eliberate în cadrul respectivului sistem. Fiecare certificat european de securitate cibernetică s-ar putea referi la unul din nivelurile de asigurare: „de bază”, „substanțial” sau „ridicat”, pe când declarația de conformitate UE nu s-ar putea referi decât la nivelul de asigurare „de bază”. Nivelurile de asigurare ar indica rigoarea și profunzimea corespunzătoare evaluării produsului TIC, serviciului TIC sau procesului TIC și s-ar caracteriza prin trimitere la specificațiile tehnice și la standardele și procedurile conexe, incluzând controale tehnice, al căror scop este atenuarea sau prevenirea incidentelor. Fiecare nivel de asigurare ar trebui să fie coerent în cadrul diferitelor domenii sectoriale în care se aplică certificarea.

(87) Un sistem european de certificare a securității cibernetice ar putea specifica mai multe niveluri de evaluare în funcție de rigoarea și de profunzimea metodologiei de evaluare utilizate. Nivelurile de evaluare ar trebui să corespundă unuia din nivelurile de asigurare și să fie asociată unei combinații adecvate de componente ale asigurării. Pentru toate nivelurile de asigurare, produsul TIC, serviciul TIC sau procesul TIC ar trebui să conțină o serie de funcții securizate, astfel cum sunt precizate de sistem, care pot include: o configurație securizată a produsului livrat, un cod semnat, o actualizare securizată, atenuarea consecințelor defectelor de exploatare (*exploit mitigation*) și protecția completă a memoriilor în stivă sau heap. Aceste funcții ar trebui să fie dezvoltate și întreținute prin utilizarea unor abordări axate pe dezvoltare și prin instrumente conexe pentru a asigura că sunt încorporate în mod fiabil mecanisme software și hardware eficace.

(88) Pentru nivelul de asigurare „de bază”, evaluarea ar trebui să se bazeze cel puțin pe următoarele componente ale asigurării: evaluarea ar trebui să includă cel puțin o analiză a documentației tehnice a produsului TIC, serviciului TIC sau procesului TIC de către organismul de evaluare a conformității. În cazul în care certificarea include procese TIC, procesul utilizat pentru conceperea, dezvoltarea și întreținerea unui produs TIC sau serviciu TIC ar trebui de asemenea să facă obiectul analizei tehnice. În cazul în care un sistem european de certificare a securității cibernetice prevede o autoevaluare a conformității, ar trebui să fie suficient ca producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC să fi efectuat o autoevaluare a conformității produselor TIC, serviciilor TIC sau proceselor TIC cu sistemul de certificare.

(89) Pentru nivelul de asigurare „substanțial”, în plus față de cerințele pentru nivelul de asigurare „de bază”, evaluarea ar trebui să se bazeze cel puțin pe verificarea conformității funcțiilor de securitate ale produsului TIC, serviciului TIC sau procesului TIC cu documentația sa tehnică.

(90) Pentru nivelul de asigurare „ridicat”, în plus față de elementele necesare pentru nivelul de asigurare „substanțial”, evaluarea ar trebui să se bazeze cel puțin pe un test de eficacitate care să evalueze rezistența funcțiilor de securitate ale produsului TIC, serviciului TIC sau procesului TIC împotriva atacurilor cibernetice lansate de persoane care au competențe și resurse semnificative.

(91) Recurgerea la certificarea europeană de securitate cibernetică și la declarația de conformitate UE ar trebui să rămână voluntară, cu excepția cazului în care există dispoziții contrare în dreptul Uniunii sau în dreptul statelor membre adoptat în conformitate cu dreptul Uniunii. În lipsa unui drept armonizat al Uniunii, statele membre pot adopta reglementări tehnice la nivel național, care să prevadă certificarea obligatorie în cadrul unui sistem european de certificare a securității cibernetice în conformitate cu Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului ([20]). Statele membre ar putea recurge la certificarea europeană de securitate cibernetică și în contextul achizițiilor publice și al Directivei 2014/24/UE a Parlamentului European și a Consiliului ([21]).

(92) În unele domenii ar putea fi necesar, în viitor, ca anumite cerințe specifice în materie de securitate cibernetică și certificarea acestora să fie obligatorii pentru anumite produse TIC, servicii TIC sau procese TIC în scopul îmbunătățirii nivelului de securitate cibernetică în Uniune. Comisia ar trebui să monitorizeze cu regularitate impactul sistemelor europene de certificare a securității cibernetice adoptate asupra disponibilității produselor TIC, și serviciilor TIC și proceselor TIC securizate pe piața internă și să evalueze periodic nivelul de utilizare a sistemelor de certificare de către producători și de către furnizorii de produse TIC, servicii TIC sau procese TIC din Uniune. Ar trebui să se evalueze eficiența sistemelor europene de certificare a securității cibernetice și să se analizeze dacă anumite sisteme ar trebui să devină obligatorii, din perspectiva legislației Uniunii legate de securitatea cibernetică, și mai ales a Directivei (UE) 2016/1148, luând în considerare securitatea rețelelor și a sistemelor informatice utilizate de operatorii de servicii esențiale.

(93) Certificatele europene de securitate cibernetică și declarațiile de conformitate UE ar trebui să îi ajute pe utilizatorii finali să facă alegeri în cunoștință de cauză. Prin urmare, produsele TIC, serviciile TIC și procesele TIC care au fost certificate sau pentru care a fost emisă o declarație de conformitate ar trebui însoțite de informații structurate care sunt adaptate nivelului tehnic estimat al utilizatorului final preconizat. Toate aceste informații ar trebui să fie puse la dispoziție online, și, după caz, în formă fizică. Concret, utilizatorul final ar trebui să aibă acces la informații referitoare la numărul de referință al sistemului de certificare, nivelul de asigurare, descrierea riscurilor pentru securitatea cibernetică asociate produsului TIC, serviciului TIC sau procesului TIC, și autoritatea sau organismul emitent, sau ar trebui să aibă posibilitatea de a obține la o copie a certificatului european de securitate cibernetică. În plus, utilizatorul final ar trebui să fie informat despre politica de asistență în materie de securitate cibernetică a producătorului sau a furnizorului de produse TIC, servicii TIC și procese TIC, și anume cât timp se poate aștepta utilizatorul final să primească actualizări sau corecții în materie de securitate cibernetică. După caz, ar trebui furnizate orientări privind acțiunile sau setările pe care utilizatorul final le poate aplica pentru a-și menține sau a-și crește nivelul de securitate cibernetică al produsului TIC sau al serviciului TIC și date de contact ale unui punct de contact unic pentru a raporta atacurile cibernetice și pentru a primi asistență în eventualitatea acestora (pe lângă raportarea automată). Informațiile respective ar trebui să fie actualizate periodic și să fie disponibile pe un site care să furnizeze informații despre sistemele europene de certificare a securității cibernetice.

(94) Pentru realizarea obiectivelor prezentului regulament și pentru a se evita fragmentarea pieței interne, sistemele sau procedurile naționale de certificare a securității cibernetice pentru produsele TIC, serviciile TIC sau procesele TIC care fac obiectul unui sistem european de certificare a securității cibernetice ar trebui să înceteze să mai producă efecte de la o dată stabilită de Comisie prin intermediul actelor de punere în aplicare. În plus, statele membre ar trebui să nu introducă noi sisteme naționale de certificare a securității cibernetice pentru produse TIC, servicii TIC sau procese TIC care fac deja obiectul unui sistem european de certificare a securității cibernetice existent. Cu toate acestea, statele membre nu ar trebui împiedicate să adopte sau să mențină sisteme naționale de certificare a securității cibernetice în scopuri de securitate națională. Statele membre ar trebui să informeze Comisia și ECCG cu privire la orice intenție de a elabora noi sisteme naționale de certificare a securității cibernetice. Comisia și ECCG ar trebui să evalueze impactul noului sistem național de certificare a securității cibernetice asupra bunei funcționări a pieței interne, inclusiv din perspectiva interesului strategic de a solicita în schimb un sistem european de certificare a securității cibernetice.

(95) Sistemele europene de certificare a securității cibernetice urmăresc armonizarea practicilor în privința securității cibernetice în Uniune. Este nevoie ca acestea să contribuie la creșterea nivelului de securitate cibernetică în Uniune. De asemenea, în modul de concepere a sistemelor europene de certificare a securității cibernetice ar trebui să se ia în calcul și să se permită dezvoltarea în continuare de inovații în domeniul securității cibernetice.

([20]) 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).

([21]) Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE (JO L 94, 28.3.2014, p. 65).

(96) Sistemele europene de certificare a securității cibernetice ar trebui să țină seama de actualele metode de dezvoltare hardware și software și mai ales de impactul frecventelor actualizări software sau firmware aduse certificatelor europene de securitate cibernetică individuale. Sistemele europene de certificare a securității cibernetice ar trebui să precizeze condițiile în care o actualizare poate necesita ca un produs TIC, un serviciu TIC sau un proces TIC să fie certificat din nou sau ca sfera de aplicare a unui anumit certificat european de securitate cibernetică să fie restrânsă, ținând seama de orice efecte negative posibile ale actualizării asupra conformității cu cerințele de securitate ale certificatului respectiv.

(97) Odată ce se adoptă un sistem european de certificare a securității cibernetice, producătorii sau furnizorii de produse TIC, servicii TIC sau procese TIC ar trebui să aibă posibilitatea de a depune o cerere de certificare a produselor lor TIC sau a serviciilor lor TIC pe lângă un organism de evaluare a conformității ales de ei, aflat oriunde în Uniune. Organismele de evaluare a conformității ar trebui să fie acreditate de un organism național de acreditare dacă respectă anumite cerințe specifice, stabilite în prezentul regulament. Acreditarea ar trebui să fie acordată pentru o perioadă maximă de cinci ani și să poată fi reînnoită în aceleași condiții dacă organismul de evaluare a conformității îndeplinește cerințele în continuare. Organismele naționale de acreditare ar trebui să restricționeze, să suspende sau să revoce acreditarea unui organism de evaluare a conformității în cazul în care condițiile de acreditare nu sunt sau nu mai sunt îndeplinite sau în cazul în care măsurile luate de un organism de evaluare a conformității încalcă prezentul regulament.

(98) Trimiterile din legislația națională la standarde naționale care au încetat să mai producă efecte ca urmare a intrării în vigoare a unui sistem european de certificare a securității cibernetice poate constitui o sursă de confuzie. Prin urmare, statele membre ar trebui să reflecte adoptarea unui sistem european de certificare a securității cibernetice în legislația lor națională.

(99) Pentru a se ajunge la standarde echivalente pe întreg teritoriul Uniunii, pentru a se facilita recunoașterea reciprocă și a se promova acceptarea generală a certificatelor europene de securitate cibernetică și a declarațiilor de conformitate UE, este necesar să se instituie un sistem de evaluare *inter pares* în rândul autorităților naționale de certificare a securității cibernetice. Evaluarea *inter pares* ar trebui să aibă drept obiect procedurile de supraveghere a conformității produselor TIC, serviciilor TIC și proceselor TIC cu certificatele europene de securitate cibernetică, de monitorizare a obligațiilor producătorilor sau ale furnizorilor de produse TIC, servicii TIC sau procese TIC care efectuează autoevaluarea conformității, de monitorizare a organismelor de evaluare a conformității, precum și adecvarea expertizei personalului organismelor care eliberează certificate pentru nivelul de asigurare „ridicat”. Prin intermediul unui act de punere în aplicare, Comisia ar trebui să elaboreze cel puțin un plan cincinal pentru evaluarea *inter pares*, precum și să stabilească criteriile și metodologia pentru funcționarea sistemului de evaluare *inter pares*.

(100) Fără a aduce atingere sistemului general de evaluare *inter pares* care urmează să fie pus în practică de toate autoritățile naționale de certificare a securității cibernetice, anumite sisteme europene de certificare a securității cibernetice pot include un mecanism de evaluare *inter pares* pentru organismele care eliberează certificate europene de securitate cibernetică pentru produse TIC, servicii TIC sau procese TIC la nivelul de asigurare „ridicat” în temeiul respectivelor sisteme. ECCG ar trebui să sprijine punerea în practică a acestor mecanisme de evaluare *inter pares*. Evaluările *inter pares* ar trebui să evalueze îndeosebi dacă organismele în cauză își îndeplinesc atribuțiile în mod armonizat și pot include mecanisme de recurs. Rezultatele evaluărilor *inter pares* ar trebui puse la dispoziția publicului. Organismele în cauză pot adopta măsurile corespunzătoare pentru a-și adapta în consecință practicile și expertiza.

(101) Statele membre ar trebui să desemneze una sau mai multe autorități naționale de certificare a securității cibernetice care să supravegheze conformitatea cu obligațiile ce decurg din prezentul regulament. O autoritate națională de certificare a securității cibernetice poate fi o autoritate deja existentă sau o nouă autoritate. Un stat membru ar trebui să aibă în același timp posibilitatea de a desemna, în urma acordului cu alt stat membru, una sau mai multe autorități naționale de certificare de securitate cibernetică pe teritoriul celuilalt stat membru.

(102) Autoritățile naționale de certificare de securitate cibernetică ar trebui în special să monitorizeze obligațiile producătorilor sau ale furnizorilor de produse TIC, de servicii TIC sau de procese TIC stabiliți pe teritoriul lor respectiv în ceea ce privește declarația de conformitate UE și să asigure respectarea acestor obligații, ar trebui să ofere asistență organismelor naționale de acreditare la monitorizarea și supravegherea activităților derulate de organismele de evaluare a conformității, oferindu-le expertiză și informații relevante, ar trebui să autorizeze organismele de evaluare a conformității să își îndeplinească atribuțiile atunci când aceste organisme îndeplinesc cerințele suplimentare prevăzute într-un sistem european de certificare a securității cibernetice și ar trebui să monitorizeze evoluțiile relevante în domeniul certificării de securitate cibernetică. Autoritățile naționale de certificare a securității cibernetice ar trebui să trateze plângerile depuse de persoane fizice sau juridice în legătură cu certificatele europene de securitate cibernetică eliberate de respectivele autorități sau în legătură cu certificatele europene

de securitate cibernetică eliberate de organismele de evaluare a conformității, atunci când astfel de certificate indică nivelul de asigurare „ridicat", ar trebui să investigheze, în măsura în care este oportun, obiectul plângerii și să informeze reclamantul cu privire la progresele și rezultatul investigației, într-un termen rezonabil. În plus, autoritățile naționale de certificare a securității cibernetice ar trebui să coopereze cu alte autorități naționale de certificare a securității cibernetice sau cu alte autorități publice, inclusiv schimbând informații despre o posibilă neconformitate a produselor TIC, a serviciilor TIC și a proceselor TIC cu cerințele prezentului regulament sau ale anumitor sisteme europene de certificare a securității cibernetice. Comisia ar trebui să faciliteze schimbul de informații punând la dispoziție un sistem electronic general de gestionare a informațiilor, de exemplu sistemul de informare și de comunicare pentru supravegherea pieței (ICSMS) și sistemul de alertă rapidă pentru produse nealimentare periculoase (RAPEX) folosite deja de autoritățile de supraveghere a pieței în temeiul Regulamentului (CE) nr. 765/2008.

(103) Pentru a asigura aplicarea coerentă a cadrului european de certificare a securității cibernetice, ar trebui să se instituie un ECCG, compus din reprezentanți ai autorităților naționale de certificare a securității cibernetice sau ai altor autorități naționale competente. Principalele atribuții ale ECCG ar trebui să constea în furnizarea de consiliere și asistență Comisiei în activitatea sa pentru a asigura coerența în punerea în aplicare și asigurarea respectării cadrului european de certificare a securității cibernetice, în acordarea de asistență ENISA și în cooperarea îndeaproape cu aceasta la elaborarea propunerilor de sisteme europene de certificare a securității cibernetice; în cazuri justificate corespunzător să solicite ENISA să pregătească o propunere de sistem; să adopte avize adresate ENISA cu privire la propunerile de sisteme și să adopte avize adresate Comisiei cu privire la întreținerea și revizuirea sistemelor europene de certificare a securității cibernetice existente. ECCG ar trebui să faciliteze schimbul de bune practici și de expertiză între diferitele autorități naționale de certificare a securității cibernetice care sunt responsabile cu autorizarea organismelor de evaluare a conformității și cu eliberarea certificatelor europene de securitate cibernetică.

(104) În vederea sporirii gradului de sensibilizare și pentru a facilita acceptarea viitoarelor sisteme europene de certificare a securității cibernetice, Comisia poate emite orientări generale sau sectoriale în materie de securitate cibernetică, de exemplu cu privire la bunele practici sau la comportamentul responsabil în materie de securitate cibernetică, subliniind efectul pozitiv al utilizării de produse TIC, servicii TIC și procese TIC certificate.

(105) Pentru a facilita și mai mult comerțul și având în vedere că lanțurile de aprovizionare TIC sunt mondiale, Uniunea poate încheia, în conformitate cu articolul 218 din Tratatul privind funcționarea Uniunii Europene (TFUE), acorduri de recunoaștere reciprocă referitoare la certificatele europene de securitate cibernetică. Ținând seama de avizele primite din partea ENISA și a Grupului european pentru certificarea securității cibernetice, Comisia poate recomanda inițierea negocierilor relevante. Fiecare sistem european de certificare a securității cibernetice ar trebui să prevadă condiții specifice pentru astfel de acorduri de recunoaștere reciprocă cu țări terțe.

(106) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, ar trebui conferite competențe de executare Comisiei. Competențele respective ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului ([22]).

(107) Procedura de examinare ar trebui utilizată pentru adoptarea actelor de punere în aplicare privind sistemele europene de certificare a securității cibernetice pentru produse TIC, servicii TIC și procese TIC, pentru adoptarea actelor de punere în aplicare privind modalitățile de desfășurare a anchetelor întreprinse de ENISA, pentru adoptarea actelor de punere în aplicare privind un plan pentru evaluarea *inter pares* a autorităților naționale de certificare a securității cibernetice, precum și pentru adoptarea actelor de punere în aplicare privind circumstanțele, formatele și procedurile de notificare către Comisie a organismelor acreditate de evaluare a conformității de către autoritățile naționale de certificare a securității cibernetice.

(108) Funcționarea ENISA ar trebui să facă obiectul unei evaluări periodice și independente. Evaluarea ar trebui să țină seama de îndeplinirea de către ENISA a obiectivelor sale, de practicile sale de lucru și de relevanța atribuțiilor sale, mai ales a atribuțiilor legate de cooperarea operațională la nivelul Uniunii. Evaluarea respectivă ar trebui să analizeze impactul, eficacitatea și eficiența cadrului european de certificare a securității cibernetice. În cazul unei revizuiri, Comisia ar trebui să evalueze modul în care se poate consolida rolul ENISA de punct de referință pentru consiliere și expertiză și ar trebui să evalueze rolul potențial al ENISA de a sprijini evaluarea produselor TIC, a serviciilor TIC și a proceselor TIC ale țărilor terțe care nu respectă normele Uniunii, în cazul în care astfel de produse, servicii și procese intră în Uniune.

([22]) 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).

(109) Întrucât obiectivele prezentului regulament nu pot fi realizate în mod satisfăcător de către statele membre, dar, având în vedere amploarea și efectele sale, pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană (TUE). În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea acestor obiective.

(110) Regulamentul (UE) nr. 526/2013 ar trebui abrogat,

ADOPTĂ PREZENTUL REGULAMENT:

TITLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect și domeniu de aplicare

(1) În vederea asigurării bunei funcționări a pieței interne, urmărind în același timp atingerea, în Uniune, a unui nivel ridicat de securitate cibernetică, de reziliență cibernetică și de încredere, prezentul regulament stabilește:

(a) obiectivele, atribuțiile și aspectele organizaționale legate de ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică); și

(b) un cadru pentru instituirea de sisteme europene de certificare a securității cibernetice cu scopul de a asigura un nivel adecvat de securitate cibernetică a produselor TIC, serviciilor TIC și proceselor TIC în Uniune, precum și cu scopul de a evita fragmentarea pieței interne în ceea ce privește sistemele de certificare a securității cibernetice din Uniune.

Cadrul menționat la primul paragraf litera (b) se aplică fără a aduce atingere dispozițiilor specifice cuprinse în alte acte juridice ale Uniunii privind certificarea voluntară sau obligatorie.

(2) Prezentul regulament nu aduce atingere competențelor statelor membre în ceea ce privește activitățile aferente securității publice, apărării, securității naționale și nici activităților statului din domeniul dreptului penal.

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „securitate cibernetică” înseamnă activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice;

2. „rețea și sistem informatic” înseamnă rețea și sistem informatic astfel cum sunt definite la articolul 4 punctul 1 din Directiva (UE) 2016/1148;

3. „strategie națională privind securitatea rețelelor și a sistemelor informatice” înseamnă o strategie națională privind securitatea rețelelor și a sistemelor informatice astfel cum este definită la articolul 4 punctul 3 din Directiva (UE) 2016/1148;

4. „operator de servicii esențiale” înseamnă un operator de servicii esențiale astfel cum este definit la articolul 4 punctul 4 din Directiva (UE) 2016/1148;

5. „furnizor de servicii digitale” înseamnă un furnizor de servicii digitale astfel cum este definit la articolul 4 punctul 6 din Directiva (UE) 2016/1148;

6. „incident” înseamnă un incident astfel cum este definit la articolul 4 punctul 7 din Directiva (UE) 2016/1148;

7. „administrarea incidentului” înseamnă o administrare a incidentului astfel cum este definită la articolul 4 punctul 8 din Directiva (UE) 2016/1148;

8. „amenințare cibernetică” înseamnă orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora;

9. „sistem european de certificare a securității cibernetice” înseamnă un set cuprinzător de norme, cerințe tehnice, standarde și proceduri, instituite la nivelul Uniunii, care se aplică certificării sau evaluării conformității anumitor produse TIC, servicii TIC și procese TIC;

10. „sistem național de certificare a securității cibernetice” înseamnă un set cuprinzător de norme, cerințe tehnice, standarde și proceduri elaborate și adoptate de o autoritate națională publică, care se aplică certificării sau evaluării conformității produselor TIC, serviciilor TIC și proceselor TIC care intră în domeniul de aplicare al sistemului în cauză;

11. „certificat european de securitate cibernetică” înseamnă un document emis de un organism relevant prin care se atestă că un anumit produs TIC, serviciu TIC sau proces TIC a fost evaluat în scopul verificării conformității cu cerințele de securitate specifice prevăzute în cadrul unui sistem european de certificare a securității cibernetice;

12. „produs TIC” înseamnă un element sau un grup de elemente al unei rețele sau al unui sistem informatic;

13. „serviciu TIC” înseamnă un serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice;

14. „proces TIC” înseamnă un set de activități desfășurate pentru a concepe, a dezvolta, a furniza sau a întreține un produs TIC sau un serviciu TIC;

15. „acreditare” înseamnă acreditare astfel cum este definită la articolul 2 punctul 10 din Regulamentul (CE) nr. 765/2008;

16. „organism național de acreditare” înseamnă un organism național de acreditare astfel cum este definit la articolul 2 punctul 11 din Regulamentul (CE) nr. 765/2008;

17. „evaluare a conformității” înseamnă o evaluare a conformității astfel cum este definită la articolul 2 punctul 12 din Regulamentul (CE) nr. 765/2008;

18. „organism de evaluare a conformității” înseamnă un organism de evaluare a conformității astfel cum este definit la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008;

19. „standard” înseamnă un standard astfel cum este definit la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012;

20. „specificație tehnică” înseamnă un document care stabilește cerințele tehnice pe care trebuie să le îndeplinească un produs TIC, un serviciu TIC sau un proces TIC, ori procedurile de evaluare a conformității referitoare la acestea;

21. „nivel de asigurare” înseamnă temeiul încrederii că un produs TIC, un serviciu TIC sau un proces TIC întrunește cerințele de securitate ale unui sistem european de certificare a securității cibernetice specific și indică nivelul la care a fost evaluat un produs TIC, un serviciu TIC sau un proces TIC, dar care nu măsoară ca atare securitatea produsului TIC, a serviciului TIC sau a procesului TIC în cauză;

22. „autoevaluare a conformității” înseamnă o acțiune desfășurată de un producător sau de un furnizor de produse TIC, de servicii TIC sau de procese TIC, care evaluează dacă respectivele produse TIC, servicii TIC sau procese TIC îndeplinesc cerințele unui sistem european de certificare a securității cibernetice specific.

TITLUL II

ENISA (AGENȚIA UNIUNII EUROPENE PENTRU SECURITATE CIBERNETICĂ)

CAPITOLUL I

Mandat și obiective

Articolul 3

Mandat

(1) ENISA îndeplinește atribuțiile care îi sunt încredințate în temeiul prezentului regulament în scopul de a asigura un nivel comun ridicat de securitate cibernetică în întreaga Uniune, inclusiv sprijinind în mod activ statele membre și instituțiile, organele, oficiile și agențiile Uniunii pentru a-și îmbunătăți securitatea cibernetică. ENISA servește drept punct de referință în ceea ce privește consilierea și expertiza în materie de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii, precum și pentru alte părți interesate relevante din Uniune.

ENISA contribuie la reducerea fragmentării pe piața internă prin îndeplinirea atribuțiilor care îi sunt încredințate în temeiul prezentului regulament.

(2) ENISA îndeplinește atribuțiile care îi sunt încredințate prin acte juridice ale Uniunii care stabilesc măsuri de apropiere a actelor cu putere de lege și a actelor administrative ale statelor membre care au legătură cu securitatea cibernetică.

(3) În îndeplinirea atribuțiilor sale, ENISA acționează în mod independent, evitând să dubleze activitățile statelor membre și ținând seama de expertiza pe care o au deja statele membre.

(4) ENISA își dezvoltă propriile resurse, inclusiv capacitățile și competențele tehnice și umane, necesare pentru a îndeplini atribuțiile care îi sunt încredințate în temeiul prezentului regulament.

Articolul 4

Obiective

(1) ENISA este un centru de expertiză în materie de securitate cibernetică, datorită independenței sale, calității științifice și tehnice a consilierii și asistenței acordate și a informațiilor furnizate, transparenței procedurilor de operare și metodelor de funcționare, precum și a diligenței cu care își îndeplinește atribuțiile.

(2) ENISA oferă asistență instituțiilor, organelor, oficiilor și agențiilor Uniunii, precum și statelor membre, la elaborarea și punerea în aplicare a politicilor Uniunii legate de securitatea cibernetică, inclusiv a politicilor sectoriale privind securitatea cibernetică.

(3) ENISA sprijină consolidarea capacităților și procesul de pregătire în întreaga Uniune, furnizând asistență instituțiilor, organelor, oficiilor și agențiilor Uniunii, precum și statelor membre și părților interesate din sectorul public și privat pentru a spori protecția rețelelor și a sistemelor informatice ale acestora, pentru a dezvolta și a îmbunătăți reziliența cibernetică și capacitățile de răspuns și pentru a dezvolta aptitudini și competențe în domeniul securității cibernetice.

(4) ENISA promovează cooperarea, inclusiv schimbul de informații și coordonarea la nivelul Uniunii între statele membre, instituțiile, organele, oficiile și agențiile Uniunii și părțile interesate relevante din sectorul public și privat cu privire la chestiuni legate de securitatea cibernetică.

(5) ENISA contribuie la sporirea capacităților de securitate cibernetică la nivelul Uniunii pentru a sprijini acțiunile statelor membre în materie de prevenire a amenințărilor cibernetice și de răspuns la acestea, în special în cazul incidentelor transfrontaliere.

(6) ENISA promovează recurgerea la certificarea europeană a securității cibernetice, cu scopul de a evita fragmentarea pieței interne. ENISA contribuie la instituirea și menținerea unui cadru de certificare europeană a securității cibernetice în conformitate cu titlul III din prezentul regulament, pentru a crește transparența securității cibernetice a produselor TIC, a serviciilor TIC și a proceselor TIC, consolidând astfel încrederea în piața internă digitală și în competitivitatea acesteia.

(7) ENISA promovează un nivel ridicat de sensibilizare în privința securității cibernetice, inclusiv a igienei cibernetice și alfabetizării cibernetice a cetățenilor, organizațiilor și întreprinderilor.

CAPITOLUL II

Atribuții

Articolul 5

Elaborarea și punerea în aplicare a politicii și a dreptului Uniunii

ENISA contribuie la elaborarea și punerea în aplicare a politicii și a dreptului Uniunii:

1. acordând asistență și consiliere cu privire la elaborarea și revizuirea politicii și a dreptului Uniunii în domeniul securității cibernetice, precum și cu privire la inițiative politice și legislative sectoriale în cazul în care sunt implicate aspecte legate de securitatea cibernetică, în special prin furnizarea de avize independente și analize și prin desfășurarea de lucrări pregătitoare;

2. acordând asistență statelor membre pentru punerea în aplicare cu coerență a politicii și dreptului Uniunii privind securitatea cibernetică, mai ales în ceea ce privește Directiva (UE) 2016/1148, inclusiv prin intermediul emiterii avizelor, orientărilor, consilierii și bunelor practici referitoare la teme precum gestionarea riscurilor, raportarea incidentelor și schimbul de informații, precum și facilitând schimbul de bune practici între autoritățile competente în această privință;

3. acordând asistență statelor membre și instituțiilor, organelor, oficiilor și agențiilor Uniunii la elaborarea și promovarea unor politici în materie de securitate cibernetică legate de susținerea disponibilității sau a integrității generale a nucleului public al internetului deschis;

4. contribuind la activitatea grupului de cooperare instituit în temeiul articolului 11 din Directiva (UE) 2016/1148, prin furnizarea de expertiză și de asistență;

5. sprijinind:

   (a) elaborarea și punerea în aplicare a politicii Uniunii în domeniul identității electronice și al serviciilor de încredere, în special furnizând consiliere și orientări tehnice, precum și prin facilitarea schimbului de bune practici între autoritățile competente;

   (b) promovarea unui nivel sporit de securitate a comunicațiilor electronice, inclusiv prin furnizarea de consiliere și de expertiză, precum și prin facilitarea schimbului de bune practici între autoritățile competente;

   (c) statele membre în punerea în aplicare a aspectelor specifice legate de securitatea cibernetică cuprinse în politica și dreptul Uniunii referitoare la protecția datelor și a vieții private, inclusiv prin consilierea Comitetului european pentru protecția datelor, la cerea acestuia.

6. sprijinind revizuirea periodică a activităților legate de politica Uniunii prin elaborarea unui raport anual privind stadiul punerii în aplicare a cadrului juridic aplicabil în ceea ce privește:

   (a) informările privind notificările incidentelor transmise de statele membre prin punctele unice de contact grupului de cooperare în temeiul articolului 10 alineatul (3) din Directiva (UE) 2016/1148;

   (b) rezumatul notificărilor privind încălcarea securității sau pierderea integrității primite de la prestatorii de servicii de încredere, transmise ENISA de organismele de supraveghere în temeiul articolului 19 alineatul (3) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([23]);

   (c) notificările privind incidentele de securitate transmise de furnizorii de rețele publice de comunicații electronice sau servicii de comunicații electronice destinate publicului, transmise ENISA de autoritățile competente în temeiul articolului 40 din Directiva (UE) 2018/1972.

([23]) 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).

Articolul 6

Consolidarea capacităților

(1) ENISA acordă asistență:

(a) statelor membre, în eforturile lor de a îmbunătăți prevenirea, detectarea și analizarea amenințărilor cibernetice și a incidentelor și capacitatea de răspuns la acestea, prin furnizarea cunoștințelor și a expertizei necesare;

(b) statelor membre și instituțiilor, organelor, oficiilor și agențiilor Uniunii la elaborarea și punerea în aplicare a politicilor pentru divulgarea vulnerabilităților în mod voluntar;

(c) instituțiilor, organelor, oficiilor și agențiilor Uniunii, în eforturile lor de a îmbunătăți prevenirea, detectarea și analiza amenințărilor cibernetice și a incidentelor și de a îmbunătăți capacitățile de răspuns la astfel de amenințări cibernetice și incidente, mai ales printr-un sprijin adecvat acordat CERT-UE;

(d) statelor membre în ceea ce privește dezvoltarea echipelor CSIRT naționale, la solicitarea acestora, în temeiul articolului 9 alineatul (5) din Directiva (UE) 2016/1148;

(e) statelor membre în ceea ce privește elaborarea strategiilor naționale privind securitatea rețelelor și a sistemelor informatice, la solicitarea acestora în temeiul articolului 7 alineatul (2) din Directiva (UE) 2016/1148 și promovează difuzarea acestor strategii în întreaga Uniune și constată progresele înregistrate în punerea lor în aplicare, pentru a promova bunele practici;

(f) instituțiilor Uniunii, în ceea ce privește elaborarea și revizuirea strategiilor Uniunii referitoare la securitatea cibernetică, promovarea difuzării acestora, precum și urmărirea progreselor înregistrate în punerea lor în aplicare;

(g) echipelor CSIRT naționale și ale Uniunii, în ceea ce privește creșterea nivelului capacităților proprii, inclusiv prin promovarea dialogului și a schimbului de informații, pentru a garanta că, având în vedere stadiul actual al tehnologiei, fiecare echipă CSIRT dispune de un set comun de capacități minime și funcționează în conformitate cu cele mai bune practici;

(h) statelor membre, prin organizarea în mod regulat a exercițiilor în materie de securitate cibernetică la nivelul Uniunii menționate la articolul 7 alineatul (5) cel puțin o dată la doi ani și prin formularea de recomandări de politici bazate pe procesul de evaluare a exercițiilor și pe învățămintele desprinse în urma acestora;

(i) organismelor publice relevante, prin oferirea de cursuri de formare privind securitatea cibernetică, în cooperare cu părțile interesate acolo unde este cazul;

(j) grupului de cooperare, în ceea ce privește schimbul de bune practici, în special în ceea ce privește identificarea de către statele membre a operatorilor de servicii esențiale, în temeiul articolului 11 alineatul (3) litera (l) din Directiva (UE) 2016/1148, inclusiv în legătură cu dependența transfrontalieră legată de riscuri și incidente.

(2) ENISA sprijină schimbul de informații în cadrul sectoarelor și între acestea, mai ales în sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, prin furnizarea de bune practici și de orientări privind instrumentele disponibile, proceduri, precum și privind modul de abordare a aspectelor de reglementare legate de schimbul de informații.

Articolul 7

Cooperarea operațională la nivelul Uniunii

(1) ENISA sprijină cooperarea operațională între statele membre, instituțiile, organele, oficiile și agențiile Uniunii, precum și între părțile interesate.

(2) ENISA cooperează la nivel operațional și stabilește sinergii cu instituțiile, organele, oficiile și agențiile Uniunii, inclusiv cu CERT-UE, cu serviciile care au atribuții de combatere a criminalității informatice și cu autoritățile de supraveghere care au atribuții de protecție a vieții private și a datelor cu caracter personal, în vederea abordării problemelor de interes comun, inclusiv prin:

(a) schimbul de know-how și de bune practici;

(b) furnizarea de consiliere și emiterea de orientări privind chestiunile relevante legate de securitatea cibernetică;

(c) stabilirea modalităților practice pentru executarea unor atribuții specifice, după consultarea Comisiei.

(3) ENISA asigură secretariatul rețelei CSIRT în temeiul articolului 12 alineatul (2) din Directiva (UE) 2016/1148 și, în această capacitate, sprijină activ schimbul de informații și cooperarea între membrii acesteia.

(4) ENISA sprijină statele membre în cooperarea operațională cu rețeaua CSIRT:

(a) acordându-le consiliere cu privire la modul în care își pot îmbunătăți capacitățile de a preveni, de a detecta incidentele și de a răspunde la acestea, precum și acordându-le consiliere, la cererea unuia sau mai multor state membre, în legătură cu o amenințare cibernetică specifică;

(b) acordându-le asistență, la cererea unuia sau mai multor state membre, la evaluarea incidentelor cu un impact semnificativ sau substanțial prin furnizarea de expertiză și prin facilitarea administrării din punct de vedere tehnic a respectivelor incidente, mai ales susținând schimbul voluntar de informații relevante și de soluții tehnice între statele membre;

(c) analizând vulnerabilitățile și incidentele pe baza informațiilor disponibile public sau a informațiilor furnizate în mod voluntar de statele membre în acest scop; și

(d) la cererea unuia sau mai multor state membre, oferind sprijin în legătură cu anchetele tehnice *ex post* privind incidentele cu un impact semnificativ sau substanțial în înțelesul Directivei (UE) 2016/1148.

În îndeplinirea acestor atribuții, ENISA și CERT-UE desfășoară o cooperare structurată pentru a beneficia de sinergii și pentru a evita dublarea activităților.

(5) ENISA organizează exerciții periodice de securitate cibernetică la nivelul Uniunii și sprijină statele membre și instituțiile, organele, oficiile și agențiile Uniunii în ceea ce privește organizarea de exerciții de securitate cibernetică, la cererea acestora. Aceste exerciții de securitate cibernetică la nivelul Uniunii pot include elemente tehnice, operaționale sau strategice. Din doi în doi ani, ENISA organizează un exercițiu cuprinzător la scară largă.

După caz, ENISA contribuie, de asemenea, la exercițiile sectoriale de securitate cibernetică și sprijină organizarea acestora, împreună cu organizațiile relevante care participă, de asemenea, la exercițiile de securitate cibernetică desfășurate la nivelul Uniunii.

(6) În strânsă cooperare cu statele membre, ENISA întocmește periodic un raport aprofundat asupra situației tehnice în materie de securitate cibernetică la nivelul UE referitor la incidente și amenințări cibernetice, pe baza informațiilor disponibile public, a propriei sale analize și pe baza unor rapoarte transmise de echipele CSIRT ale statelor membre sau punctele unice de contact instituite prin Directiva (UE) 2016/1148, în ambele cazuri în mod voluntar, EC3 și CERT-UE, printre altele.

(7) ENISA contribuie la pregătirea unui răspuns bazat pe cooperare, atât la nivelul Uniunii, cât și la cel al statelor membre, la incidentele sau crizele transfrontaliere de mare amploare legate de securitatea cibernetică, în principal prin:

(a) agregarea și analizarea rapoartelor autorităților naționale care fac parte din domeniul public sau sunt puse la dispoziție în mod voluntar, cu scopul de a contribui la o conștientizare comună a situației;

(b) asigurarea unui flux eficient de informații și furnizarea de mecanisme decizionale de activare între rețeaua CSIRT și factorii de decizie la nivel politic și tehnic ai Uniunii;

(c) facilitarea, la cerere, a administrării din punct de vedere tehnic a acestor incidente sau crize, mai ales prin sprijinirea partajării voluntare a soluțiilor tehnice între statele membre;

(d) sprijinirea instituțiilor, organelor, oficiilor și agențiilor Uniunii precum și, la cererea acestora, a statelor membre, în ceea ce privește comunicarea publică referitoare la astfel de incidente sau crize;

(e) testarea planurilor de cooperare menite să răspundă la aceste incidente sau crize la nivelul Uniunii și, la cerere, sprijinirea statelor membre în ceea ce privește testarea respectivelor planuri la nivel național.

Articolul 8

Piața, certificarea securității cibernetice și standardizarea

(1) ENISA sprijină și promovează elaborarea și punerea în aplicare a politicii Uniunii privind certificarea securității cibernetice a produselor TIC, a serviciilor TIC și a proceselor TIC, astfel cum se prevede în titlul III din prezentul regulament, prin:

(a) monitorizarea permanentă a evoluțiilor din domenii conexe standardizării și recomandarea unor specificații tehnice adecvate pentru a fi utilizate la dezvoltarea unor sisteme europene de certificare a securității cibernetice, în temeiul articolului 54 alineatul (1) litera (c), în cazurile în care standardele nu sunt disponibile;

(b) pregătirea propunerilor de sisteme europene de certificare a securității cibernetice (denumite în continuare „propuneri de sisteme") pentru produsele TIC, serviciile TIC și procesele TIC, în conformitate cu articolul 49;

(c) evaluarea sistemelor europene de certificare a securității cibernetice adoptate, în conformitate cu articolul 49 alineatul (8);

(d) participarea la evaluările *inter pares* în temeiul articolului 59 alineatul (4);

(e) oferirea de asistență Comisiei în ceea ce privește asigurarea secretariatului ECCG, în temeiul articolului 62 alineatul (5).

(2) ENISA asigură secretariatului Grupului părților interesate pentru certificarea securității cibernetice, în temeiul articolului 22 alineatul (4).

(3) ENISA compilează și publică orientări și dezvoltă bune practici în ceea ce privește cerințele în materie de securitate cibernetică pentru produsele TIC, serviciile TIC și procesele TIC, în cooperare cu autoritățile naționale de certificare de securitate și cu industria, în cadrul unui proces oficial, standardizat și transparent.

(4) ENISA contribuie la consolidarea capacităților în legătură cu procesele de evaluare și certificare prin compilarea și emiterea unor orientări, precum și oferind sprijin statelor membre, la cererea lor.

(5) ENISA facilitează elaborarea și adoptarea de standarde europene și internaționale pentru gestionarea riscurilor și pentru securitatea produselor TIC, serviciilor TIC și proceselor TIC.

(6) ENISA elaborează, în colaborare cu statele membre și industria, avize și orientări în ceea ce privește domeniile tehnice legate de cerințele de securitate pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale, precum și în ceea ce privește standardele deja existente, inclusiv standardele naționale ale statelor membre, în temeiul articolului 19 alineatul (2) din Directiva (UE) 2016/1148.

(7) ENISA efectuează și diseminează analize periodice privind principalele tendințe de pe piața securității cibernetice, atât din punctul de vedere al cererii, cât și al ofertei, în vederea stimulării pieței securității cibernetice în cadrul Uniunii.

Articolul 9

Cunoștințe și informare

ENISA:

(a) efectuează analize ale tehnologiilor emergente și furnizează evaluări tematice privind impactul preconizat din punct de vedere societal, juridic, economic și de reglementare al inovațiilor tehnologice în materie de securitate cibernetică;

(b) efectuează analize strategice pe termen lung ale amenințărilor cibernetice și incidentelor, pentru a identifica tendințele emergente și a contribui la prevenirea incidentelor;

(c) în cooperare cu experți ai autorităților statelor membre și cu părțile interesate relevante, furnizează consiliere, orientări și bune practici pentru securitatea rețelelor și a sistemelor informatice, în special pentru securitatea infrastructurilor care sprijină sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, precum și a celor utilizate de furnizorii de servicii digitale enumerați în anexa III la respectiva directivă;

(d) culege, organizează și pune la dispoziția publicului, prin intermediul unui portal dedicat, informații privind securitatea cibernetică furnizate de instituțiile, organele, oficiile și agențiile Uniunii și informații privind securitatea cibernetică furnizate, în mod voluntar, de statele membre și de părțile interesate private și publice;

(e) culege și analizează informațiile disponibile public cu privire la incidentele semnificative și compilează rapoarte, cu scopul de a oferi orientări pentru cetățenii, organizațiile și întreprinderile din întreaga Uniune.

Articolul 10

Sensibilizare și educare

ENISA:

(a) sensibilizează publicul în legătură cu riscurile pentru securitatea cibernetică și oferă orientări cu privire la bune practici pentru utilizatorii individuali, inclusiv cu privire la igiena cibernetică și alfabetizarea cibernetică, destinate cetățenilor, organizațiilor și întreprinderilor;

(b) în cooperare cu statele membre și cu instituțiile, organele, oficiile și agențiile Uniunii, precum și cu industria, organizează campanii periodice de informare pentru sporirea securității cibernetice și a vizibilității acesteia în Uniune și stimulează o amplă dezbatere publică;

(c) oferă asistență statelor membre în eforturile acestora de a sensibiliza publicul în legătură cu securitatea cibernetică și de a promova educarea în privința securității cibernetice;

(d) susține coordonarea mai strânsă și schimbul de bune practici între statele membre privind sensibilizarea și educarea în domeniul securității cibernetice.

Articolul 11

Cercetare și inovare

În ceea ce privește cercetarea și inovarea, ENISA:

(a) consiliază instituțiile, organele, oficiile și agențiile Uniunii și statele membre cu privire la necesitățile și prioritățile în materie de cercetare în domeniul securității cibernetice pentru a face posibile răspunsuri eficace la riscurile și amenințările cibernetice actuale și emergente, inclusiv în privința tehnologiilor informației și comunicațiilor noi și emergente, și pentru o folosire eficace a tehnologiilor de prevenire a riscurilor;

(b) participă, în cazul în care Comisia i-a conferit competențele relevante, la etapa de punere în aplicare a programelor de finanțare a cercetării și inovării sau în calitate de beneficiar al acestora.

(c) contribuie la agenda strategică în privința cercetării și inovării în domeniul securității cibernetice la nivelul Uniunii.

Articolul 12

Cooperarea internațională

ENISA contribuie la eforturile Uniunii de cooperare cu țări terțe și cu organizații internaționale, precum și în cadrele internaționale de cooperare relevante, pentru a promova cooperarea internațională privind aspecte legate de securitatea cibernetică prin:

(a) participarea ca observator la organizarea de exerciții internaționale și realizarea de analize și de rapoarte destinate consiliului de administrație privind rezultatele acestor exerciții, după caz;

(b) facilitarea, la solicitarea Comisiei, a schimbului de bune practici;

(c) furnizarea de expertiză Comisiei, la cererea acesteia;

(d) consilierea și sprijinirea Comisiei în legătură cu chestiuni privind acorduri cu țări terțe pentru recunoașterea reciprocă a certificatelor de securitate cibernetică, în colaborare cu ECCG instituit în temeiul articolului 62.

CAPITOLUL III

Organizarea agenției

Articolul 13

Structura ENISA

Structura administrativă și de conducere a ENISA este compusă din următoarele:

(a) un consiliu de administrație;

(b) un comitet executiv;

(c) un director executiv;

(d) un grup consultativ al ENISA;

(e) o rețea a ofițerilor naționali de legătură.

Secțiunea 1

Consiliul de administrație

Articolul 14

Componența consiliului de administrație

(1) Consiliul de administrație este compus din câte un membru numit de fiecare stat membru, și din doi membri numiți de Comisie. Toți membrii au drept de vot.

(2) Fiecare membru al consiliului de administrație are un supleant. Supleantul reprezintă membrul în absența acestuia din urmă.

(3) Membrii consiliului de administrație și supleanții acestora sunt numiți pe baza cunoștințelor lor în domeniul securității cibernetice, ținând cont de competențele lor manageriale, administrative și bugetare relevante. Comisia și statele membre depun eforturi pentru a limita rotația reprezentanților lor în cadrul consiliului de administrație, cu scopul de a asigura continuitatea activității acestuia. Comisia și statele membre urmăresc obținerea unei reprezentări echilibrate din perspectiva genului în consiliul de administrație.

(4) Durata mandatului membrilor consiliului de administrație și al membrilor supleanți este de patru ani. Acest mandat se poate reînnoi.

Articolul 15

Funcțiile consiliului de administrație

(1) Consiliul de administrație:

(a) stabilește direcția generală de funcționare a ENISA și se asigură că ENISA funcționează în conformitate cu normele și principiile stabilite în prezentul regulament; acesta asigură în același timp coerența activității ENISA cu activitățile desfășurate de statele membre și cu cele de la nivelul Uniunii;

(b) adoptă proiectul de document unic de programare al ENISA menționat la articolul 24, înainte de transmiterea acestuia Comisiei spre avizare;

(c) adoptă documentul unic de programare al ENISA, ținând seama de avizul Comisiei;

(d) supraveghează punerea în aplicare a programării multianuale și anuale cuprinse în documentul unic de programare;

(e) adoptă bugetul anual al ENISA și exercită alte funcții privind bugetul ENISA în conformitate cu capitolul IV;

(f) evaluează și adoptă raportul anual consolidat privind activitățile ENISA, care include conturile ENISA și descrierea modului în care aceasta și-a atins indicatorii de performanță, transmite Parlamentului European, Consiliului, Comisiei și Curții de Conturi, până la data de 1 iulie a anului următor, atât raportul anual, cât și evaluarea acestuia, și publică raportul anual;

(g) adoptă normele financiare aplicabile ENISA în conformitate cu articolul 32;

(h) adoptă o strategie de combatere a fraudei care să fie proporțională cu riscurile de fraudă, ținând seama de analiza cost-beneficiu a măsurilor care urmează să fie puse în aplicare;

(i) adoptă norme de prevenire și gestionare a conflictelor de interese în cazul membrilor săi;

(j) asigură luarea măsurilor adecvate pentru a da curs concluziilor și recomandărilor care rezultă din investigațiile efectuate de Oficiul European de Luptă Antifraudă (OLAF) și din diferitele rapoarte și evaluări de audit intern sau extern;

(k) adoptă regulamentul de procedură, inclusiv norme pentru decizii provizorii privind delegarea unor atribuții specifice în temeiul articolului 19 alineatul (7);

(l) exercită, în ceea ce privește personalul ENISA, competențele conferite autorității împuternicite să facă numiri și autorității abilitate să încheie contracte de muncă (denumite în continuare „competențele de autoritate împuternicită să facă numiri") prin Statutul funcționarilor Uniunii Europene (Statutul funcționarilor) și Regimul aplicabil celorlalți agenți ai Uniunii Europene (Regimul aplicabil celorlalți agenți), stabilite prin Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului ([24]), în conformitate cu alineatul (2) din prezentul articol;

(m) adoptă norme de aplicare a Statutului funcționarilor și a Regimului aplicabil celorlalți agenți în conformitate cu procedura prevăzută la articolul 110 din Statutul funcționarilor;

(n) numește directorul executiv și, după caz, îi prelungește mandatul sau îl demite din funcție, în conformitate cu articolul 36;

(o) numește un contabil, care poate fi contabilul Comisiei și care este pe deplin independent în îndeplinirea îndatoririlor sale;

(p) ia toate deciziile privind instituirea structurilor interne ale ENISA și, dacă este necesar, privind modificarea acestora, luând în considerare nevoile activității agenției și având în vedere buna gestiune bugetară;

(q) autorizează stabilirea acordurilor de lucru în ceea ce privește articolul 7;

(r) autorizează stabilirea sau încheierea acordurilor de lucru în conformitate cu articolul 42.

(2) În conformitate cu articolul 110 din Statutul funcționarilor, consiliul de administrație adoptă o decizie în baza articolului 2 alineatul (1) din Statutul funcționarilor și a articolului 6 din Regimul aplicabil celorlalți agenți, prin care competențele relevante de autoritate împuternicită să facă numiri sunt delegate directorului executiv și în care sunt stabilite condițiile în care această delegare de competențe poate fi suspendată. Directorul executiv poate să subdelege aceste competențe.

([24]) Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului din 29 februarie 1968 (JO L 56, 4.3.1968, p. 1).

(3) În cazul în care apar împrejurări excepționale care impun acest lucru, consiliul de administrație poate adopta o decizie pentru a suspenda temporar delegarea competențelor de autoritate împuternicită să facă numiri către directorul executiv și delegarea competențelor subdelegate de către directorul executiv și să le exercite el însuși sau să le delege unuia dintre membrii săi ori unui alt membru al personalului decât directorul executiv.

Articolul 16

Președintele Consiliului de administrație

Consiliul de administrație alege cu o majoritate de două treimi din membrii săi un președinte și un vicepreședinte dintre membrii săi. Mandatul acestora este de patru ani și poate fi reînnoit o dată. Cu toate acestea, dacă pe durata mandatului încetează calitatea acestora de membri ai consiliului de administrație, mandatul lor expiră automat la aceeași dată. Vicepreședintele îl înlocuiește pe președinte din oficiu în cazul în care acesta din urmă nu își poate exercita prerogativele.

Articolul 17

Reuniunile consiliului de administrație

(1) Reuniunile consiliului de administrație sunt convocate de președintele acestuia.

(2) Consiliul de administrație se reunește în ședință ordinară cel puțin de două ori pe an. De asemenea, consiliul se reunește în ședință extraordinară la cererea președintelui acestuia, a Comisiei sau la cererea a cel puțin o treime din membrii săi.

(3) Directorul executiv ia parte la ședințele consiliului de administrație, dar nu are drept de vot.

(4) Membrii Grupului consultativ al ENISA pot lua parte la reuniunile consiliului de administrație, la invitația președintelui, dar nu au drept de vot.

(5) Membrii consiliului de administrație și supleanții lor pot să fie asistați în cursul reuniunilor consiliului de administrație de consilieri sau de experți, sub rezerva regulamentului de procedură al consiliului de administrație.

(6) ENISA asigură secretariatul consiliului de administrație.

Articolul 18

Regulile de vot ale consiliului de administrație

(1) Consiliul de administrație își adoptă deciziile cu majoritatea membrilor săi.

(2) Pentru adoptarea documentului unic de programare și a bugetului anual, precum și pentru numirea, prelungirea mandatului sau demiterea din funcție a directorului executiv, este necesară o majoritate de două treimi din membrii consiliului de administrație.

(3) Fiecare membru dispune de un vot. În absența unui membru, dreptul său de vot poate fi exercitat de supleantul său.

(4) Președintele consiliului de administrație participă la vot.

(5) Directorul executiv nu participă la vot.

(6) Regulamentul de procedură al consiliului de administrație stabilește în mod detaliat modalitățile de vot, în special condițiile în care un membru poate acționa în numele altui membru.

Secțiunea 2

Comitetul executiv

Articolul 19

Comitetul executiv

(1) Consiliul de administrație este asistat de un comitet executiv.

(2) Comitetul executiv:

(a) pregătește deciziile care urmează să fie adoptate de consiliul de administrație;

(b) asigură, împreună cu consiliul de administrație, luarea măsurilor adecvate pentru a da curs concluziilor și recomandărilor provenite din investigațiile OLAF și diferitele rapoarte și evaluări de audit intern sau extern;

(c) fără a aduce atingere responsabilităților directorului executiv, prevăzute la articolul 20, îl asistă și îl consiliază pe directorul executiv în ceea ce privește punerea în aplicare a deciziilor consiliului de administrație privind aspecte administrative și bugetare în temeiul articolului 20.

(3) Comitetul executiv este format din cinci membri. Membrii comitetului executivi sunt numiți dintre membrii consiliului de administrație. Dintre membri, unul este președintele Consiliului de administrație, care poate prezida și comitetul executiv, și unul este unul dintre reprezentanții Comisiei. Numirile membrilor comitetului executiv urmăresc asigurarea unei reprezentări echilibrate din perspectiva genului în comitetul executiv. Directorul executiv ia parte la reuniunile comitetului executiv, dar nu are drept de vot.

(4) Durata mandatului membrilor comitetului executiv este de patru ani. Acest mandat se poate reînnoi.

(5) Comitetul executiv se întrunește cel puțin o dată la trei luni. Președintele comitetului executiv convoacă reuniuni suplimentare la cererea membrilor săi.

(6) Consiliul de administrație stabilește regulamentul de procedură al comitetului executiv.

(7) Atunci când este necesar din motive de urgență, comitetul executiv poate lua anumite decizii provizorii în numele consiliului de administrație, îndeosebi cu privire la aspecte legate de gestionarea administrativă, inclusiv la suspendarea delegării competențelor de autoritate împuternicită să facă numiri, precum și cu privire la aspecte bugetare. Astfel de decizii provizorii se notifică consiliului de administrație fără întârzieri nejustificate. Consiliul de administrație decide dacă aprobă sau respinge decizia provizorie în termen de cel mult trei luni de la luarea deciziei. Comitetul executiv nu ia decizii în numele consiliului de administrație care necesită pentru aprobare o majoritate de două treimi din membrii consiliului de administrație.

Secțiunea 3

Directorul executiv

Articolul 20

Responsabilitățile directorului executiv

(1) ENISA este condusă de un director executiv care este independent în îndeplinirea atribuțiilor sale. Directorul executiv răspunde în fața consiliului de administrație.

(2) Directorul executiv prezintă Parlamentului European un raport privind modul în care și-a îndeplinit atribuțiile, atunci când este invitat să facă acest lucru. Consiliul poate solicita directorului executiv să prezinte un raport cu privire la îndeplinirea atribuțiilor sale.

(3) Directorul executiv răspunde de:

(a) administrarea curentă a ENISA;

(b) punerea în aplicare a deciziilor adoptate de consiliul de administrație;

(c) elaborarea unui proiect de document unic de programare și prezentarea acestuia consiliului de administrație spre aprobare, înainte de a fi trimis Comisiei;

(d) punerea în aplicare a documentului unic de programare și raportarea către consiliul de administrație cu privire la aceasta;

(e) pregătirea raportului anual consolidat privind activitățile ENISA, inclusiv punerea în aplicare a programului anual de activitate al ENISA, și prezentarea acestuia consiliului de administrație, spre evaluare și adoptare;

(f) pregătirea unui plan de acțiune pentru a da curs concluziilor evaluărilor retrospective și trimiterea către Comisie, din doi în doi ani, a unui raport privind progresele înregistrate;

(g) elaborarea unui plan de acțiune pentru a da curs concluziilor rapoartelor de audit intern sau extern, precum și a investigațiilor desfășurate de OLAF și prezentarea, de două ori pe an Comisiei și periodic consiliului de administrație, a unui raport privind progresele înregistrate;

(h) elaborarea proiectului de norme financiare aplicabile ENISA, astfel cum se menționează la articolul 32;

(i) întocmirea proiectului de situație a estimărilor de venituri și cheltuieli ale ENISA și execuția bugetului acesteia;

(j) protejarea intereselor financiare ale Uniunii prin aplicarea de măsuri preventive de combatere a fraudei, a corupției și a altor activități ilegale, prin realizarea de controale eficace și, dacă se constată nereguli, prin recuperarea sumelor plătite nejustificat și, dacă este cazul, prin sancțiuni administrative și financiare eficace, proporționale și disuasive;

(k) pregătirea unei strategii antifraudă pentru ENISA și prezentarea acesteia consiliului de administrație, spre adoptare;

(l) stabilirea și menținerea contactului cu comunitatea de afaceri și cu organizațiile consumatorilor, în vederea asigurării unui dialog periodic cu părțile interesate relevante;

(m) desfășurarea de schimburi periodice de opinii și de informații cu instituțiile, organele, oficiile și agențiile Uniunii în ceea ce privește activitățile lor referitoare la securitatea cibernetică, pentru a asigura coerența în dezvoltarea și punerea în aplicare a politicii Uniunii;

(n) îndeplinirea altor atribuții care îi sunt încredințate directorului executiv prin prezentul regulament.

(4) După caz, în limitele obiectivelor și atribuțiilor ENISA, directorul executiv poate înființa grupuri de lucru ad-hoc compuse din experți, inclusiv experți din rândul autorităților competente ale statelor membre. Directorul executiv informează în prealabil Consiliul de administrație cu privire la acest aspect. Procedurile referitoare în special la componența grupurilor de lucru, la numirea experților acestora de către directorul executiv și la funcționarea lor sunt prevăzute în regulamentul intern de funcționare al ENISA.

(5) Dacă este necesar, în scopul îndeplinirii atribuțiilor ENISA în mod eficient și eficace și pe baza unei analize cost-beneficiu adecvate, directorul executiv poate decide înființarea unuia sau mai multor birouri locale într-unul sau mai multe state membre. Înainte de a decide să înființeze un birou local, directorul executiv cere opinia statului membru sau a statelor membre în cauză, inclusiv a statului membru în care este situat sediul ENISA, și obține acordul prealabil al Comisiei și al consiliului de administrație. În cazurile de dezacord în cursul procesului de consultare între directorul executiv și statele membre în cauză, chestiunea este supusă Consiliului spre dezbatere. Numărul total al personalului din toate birourile locale este păstrat la minimum și nu depășește 40 % din numărul total al personalului ENISA care se află în statul membru în care este situat sediul ENISA. Numărul personalului din fiecare birou local nu depășește 10 % din numărul total al personalului ENISA care se află în statul membru în care este situat sediul ENISA.

Decizia de înființare a unui birou local precizează domeniul de aplicare al activităților care urmează să fie efectuate în cadrul respectivului birou local, astfel încât să se evite costurile inutile și dublarea funcțiilor administrative ale ENISA.

Secțiunea 4

Grupul consultativ al ENISA, grupul părților interesate pentru certificarea securității cibernetice și rețeaua ofițerilor naționali de legătură

Articolul 21

Grupul consultativ al ENISA

(1) La propunerea directorului executiv, consiliul de administrație stabilește, în mod transparent, grupul consultativ al ENISA, alcătuit din experți recunoscuți care reprezintă părțile interesate relevante, cum ar fi industria TIC, furnizorii de rețele comunicații electronice sau de servicii de destinate publicului, IMM-urile, operatorii de servicii esențiale, grupurile de consumatori, experții din mediul academic în domeniul securității cibernetice și reprezentanți ai autorităților competente notificate în conformitate cu Directiva (UE) 2018/1972, organizațiile de standardizare europene, precum și autoritățile de aplicare a legii și cele de supraveghere a protecției datelor. Consiliul de administrație depune eforturi pentru a asigura un echilibru adecvat din punct de vedere geografic și al genului, precum și un echilibru între diversele grupuri de părți interesate.

(2) Procedurile privind Grupul consultativ al ENISA, în special cele referitoare la componența sa, la propunerea directorului executiv menționată la alineatul (1), la numărul și numirea membrilor săi și la funcționarea grupului consultativ al ENISA, se detaliază în normele interne de funcționare ale ENISA și se fac publice.

(3) Grupul consultativ al ENISA este prezidat de directorul executiv sau de orice persoană numită de acesta de la caz la caz.

(4) Mandatul membrilor grupului consultativ al ENISA este de doi ani și jumătate. Membrii consiliului de administrație nu pot fi membri ai grupului consultativ al ENISA. Experții Comisiei și ai statelor membre au dreptul de a participa la reuniunile grupului consultativ al ENISA și la activitățile acestuia. Reprezentanții altor organisme considerate relevante de către directorul executiv, care nu au calitatea de membri ai grupului consultativ al ENISA, pot fi invitați să participe la reuniunile grupului consultativ al ENISA și la activitățile acestuia.

(5) Grupul consultativ al ENISA acordă consiliere ENISA în exercitarea atribuțiilor sale, cu excepția aplicării dispozițiilor titlului III din prezentul regulament. Acesta acordă consiliere în special directorului executiv în ceea ce privește elaborarea unei propuneri de program anual de activitate al ENISA și asigurarea comunicării cu părțile interesate relevante referitor la aspecte legate de programul anual de activitate.

(6) Grupul consultativ al ENISA informează periodic consiliul de administrație despre activitățile sale.

Articolul 22

Grupul părților interesate pentru certificarea securității cibernetice

(1) Se instituie Grupul părților interesate pentru certificarea securității cibernetice.

(2) Grupul părților interesate pentru certificarea securității cibernetice este alcătuit din membri selecționați din rândul experților recunoscuți care reprezintă părți interesate relevante. Comisia selecționează membrii Grupului părților interesate pentru certificarea securității cibernetice pe baza unei propuneri din partea ENISA, printr-o cerere deschisă și transparentă care asigură echilibrul între diferitele grupuri de părți interesate, precum și un echilibru adecvat din punct de vedere geografic și al genului.

(3) Grupul părților interesate pentru certificarea securității cibernetice are următoarele atribuții:

(a) să acorde Comisiei consiliere în legătură cu aspecte strategice referitoare la cadrul european de certificare a securității cibernetice;

(b) la cerere, să acorde consiliere ENISA în legătură cu chestiuni generale și strategice referitoare la atribuțiile ENISA în legătură cu piața, certificarea securității cibernetice și standardizarea;

(c) să asiste Comisia la pregătirea programul de activitate etapizat la nivelul Uniunii menționat la articolul 47;

(d) să emită un aviz referitor la programul de activitate etapizat la nivelul Uniunii în temeiul articolului 47 alineatul (4); și

(e) în cazuri urgente, să acorde consiliere Comisiei și ECCG în legătură cu necesitatea unor sisteme de certificare suplimentare față de cele incluse în programul de activitate etapizat la nivelul Uniunii, astfel cum se menționează la articolele 47 și 48.

(4) Grupul părților interesate pentru certificarea securității cibernetice este coprezidat de reprezentanții Comisiei și ai ENISA, iar secretariatul acestuia este asigurat de ENISA.

Articolul 23

Rețeaua ofițerilor naționali de legătură

(1) Consiliul de administrație, acționând la propunerea directorului executiv, instituie o rețea a ofițerilor naționali de legătură, formată din reprezentanți ai tuturor statelor membre (ofițeri naționali de legătură). Fiecare stat membru numește un reprezentant în rețeaua ofițerilor naționali de legătură. Reuniunile rețelei ofițerilor naționali de legătură pot fi ținute în diverse configurații ale experților dintr-un anumit domeniu.

(2) Rețeaua ofițerilor naționali de legătură facilitează în special schimbul de informații între ENISA și statele membre și sprijină ENISA la diseminarea activităților, constatărilor și recomandărilor sale părților interesate relevante din întreaga Uniune.

(3) Ofițerii naționali de legătură acționează drept punct de contact la nivel național pentru a facilita cooperarea între ENISA și experții naționali în contextul punerii în aplicare a programului anual de activitate al ENISA.

(4) Deși ofițerii naționali de legătură cooperează strâns cu reprezentanții statelor membre respective în cadrul consiliului de administrație, rețeaua ofițerilor naționali de legătură însăși nu dublează activitatea consiliului de administrație, și nici a altor foruri ale Uniunii.

(5) Funcțiile și procedurile pentru rețeaua ofițerilor naționali de legătură sunt specificate în normele interne de funcționare ale ENISA și se fac publice.

Secțiunea 5

Funcționare

Articolul 24

Documentul unic de programare

(1) ENISA își desfășoară activitatea în conformitate cu documentul său unic de programare care conține programarea sa anuală și multianuală și care include toate activitățile sale planificate.

(2) În fiecare an, directorul executiv elaborează un proiect de document unic de programare care conține programarea anuală și multianuală cu planificarea corespunzătoare a resurselor financiare și umane în conformitate cu articolul 32 din Regulamentul delegat (UE) nr. 1271/2013 al Comisiei ([25]) și luând în considerare orientările stabilite de Comisie.

(3) Până la data de 30 noiembrie a fiecărui an, consiliul de administrație adoptă documentul unic de programare menționat la alineatul (1) și îl transmite Parlamentului European, Consiliului și Comisiei până la data de 31 ianuarie a anului următor, împreună cu orice altă versiune ulterioară actualizată a documentului respectiv.

(4) Documentul unic de programare se definitivează după adoptarea definitivă a bugetului general al Uniunii și, dacă este necesar, se ajustează în mod corespunzător.

([25]) Regulamentul delegat (UE) nr. 1271/2013 al Comisiei din 30 septembrie 2013 privind regulamentul financiar cadru pentru organismele menționate la articolul 208 din Regulamentul (UE, Euratom) nr. 966/2012 al Parlamentului European și al Consiliului (JO L 328, 7.12.2013, p. 42).

(5) Programul anual de activitate cuprinde obiectivele detaliate și rezultatele preconizate, inclusiv indicatorii de performanță. Acesta include și o descriere a acțiunilor care urmează să fie finanțate și informații care indică resursele financiare și umane alocate fiecărei acțiuni, în conformitate cu principiile întocmirii bugetului și ale gestionării pe activități. Programul anual de activitate concordă cu programul multianual de activitate menționat la alineatul (7). Acesta indică în mod clar atribuțiile care au fost adăugate, modificate sau eliminate față de exercițiul financiar precedent.

(6) Consiliul de administrație modifică programul anual de activitate adoptat atunci când o nouă atribuție este încredințată ENISA. Orice modificare substanțială a programului anual de activitate se adoptă prin aceeași procedură ca cea utilizată în cazul programului inițial. Consiliul de administrație poate să îi delege directorului executiv competența de a aduce modificări nesubstanțiale programului anual de activitate.

(7) Programul multianual de activitate stabilește programarea strategică globală, inclusiv obiectivele, rezultatele preconizate și indicatorii de performanță. De asemenea, acesta stabilește programarea resurselor, inclusiv bugetul multianual și personalul.

(8) Programarea resurselor se actualizează anual. Programarea strategică se actualizează după caz, în special pentru a ține seama de rezultatul evaluării menționate la articolul 67.

Articolul 25

Declarația de interese

(1) Membrii consiliului de administrație, directorul executiv și funcționarii detașați temporar de statele membre întocmesc, fiecare în parte, o declarație de angajamente și o declarație în care menționează absența sau prezența oricăror interese directe sau indirecte despre care s-ar putea considera că aduc atingere independenței lor. Declarațiile sunt exacte și complete, se fac anual în scris și se actualizează ori de câte ori este nevoie.

(2) Membrii consiliului de administrație, directorul executiv și experții externi care participă la grupurile de lucru ad-hoc declară, fiecare în parte, precis și complet, cel târziu la începutul fiecărei reuniuni, toate interesele care ar putea fi considerate ca aducând atingere independenței lor în ceea ce privește punctele înscrise pe ordinea de zi și se abțin de la participarea la dezbaterile referitoare la punctele respective și de la votul în legătură cu acestea.

(3) ENISA stabilește, în regulamentul său intern de funcționare, modalitățile practice pentru normele referitoare la declarațiile de interese menționate la alineatele (1) și (2).

Articolul 26

Transparență

(1) ENISA își desfășoară activitățile cu un nivel ridicat de transparență și în conformitate cu articolul 28.

(2) ENISA se asigură că publicului și tuturor părților interesate li se furnizează informații adecvate, obiective, fiabile și ușor accesibile, în special în ceea ce privește rezultatele activității sale. De asemenea, agenția face publice declarațiile de interese întocmite în conformitate cu articolul 25.

(3) Consiliul de administrație, pe baza unei propuneri din partea directorului executiv, poate autoriza părțile interesate să participe ca observatori la unele dintre activitățile ENISA.

(4) ENISA stabilește, în regulamentul său intern de funcționare, modalitățile practice de punere în aplicare a normelor privind transparența menționate la alineatele (1) și (2).

Articolul 27

Confidențialitate

(1) Fără a aduce atingere articolului 28, ENISA nu divulgă terților informațiile pe care le prelucrează sau pe care le primește și pentru care s-a cerut, printr-o solicitare motivată, un tratament confidențial.

(2) Membrii consiliului de administrație, directorul executiv, membrii Grupului consultativ al ENISA, experții externi care participă la grupurile de lucru ad-hoc și membrii personalului ENISA, inclusiv funcționarii detașați temporar de statele membre, respectă cerințele de confidențialitate prevăzute la articolul 339 din TFUE, chiar și după încetarea atribuțiilor lor.

(3) ENISA stabilește, în regulamentul său intern de funcționare, modalitățile practice de punere în aplicare a normelor de confidențialitate menționate la alineatele (1) și (2).

(4) Dacă este necesar pentru realizarea atribuțiilor ENISA, consiliul de administrație decide să acorde ENISA permisiunea de a gestiona informații clasificate. În acest caz, ENISA, cu acordul serviciilor Comisiei, adoptă norme de securitate care să aplice principiile de securitate cuprinse în Deciziile (UE, Euratom) 2015/443 ([26]) și 2015/444 ([27]) ale Comisiei. Respectivele norme de securitate includ dispoziții privind schimbul, prelucrarea și stocarea informațiilor clasificate.

Articolul 28

Accesul la documente

(1) Regulamentul (CE) nr. 1049/2001 se aplică documentelor deținute de ENISA.

(2) Consiliul de administrație adoptă modalitățile de punere în aplicare a Regulamentului (CE) nr. 1049/2001 până la 28 decembrie 2019.

(3) Deciziile adoptate de ENISA în temeiul articolului 8 din Regulamentul (CE) nr. 1049/2001 pot face obiectul unei plângeri adresate Ombudsmanului European în temeiul articolului 228 din TFUE sau al unei acțiuni înaintate Curții de Justiție a Uniunii Europene în temeiul articolului 263 din TFUE.

CAPITOLUL IV

Întocmirea și structura bugetului ENISA

Articolul 29

Întocmirea bugetului ENISA

(1) În fiecare an, directorul executiv întocmește un proiect de situație a estimărilor de venituri și cheltuieli ale ENISA pentru următorul exercițiu financiar și îl transmite consiliului de administrație, împreună cu un proiect de schemă de personal. Se asigură un echilibru între venituri și cheltuieli.

(2) În fiecare an, pe baza proiectului de situație a estimărilor, consiliul de administrație adoptă situația estimărilor de venituri și cheltuieli ale ENISA pentru următorul exercițiu financiar.

(3) În fiecare an, până la data de 31 ianuarie, consiliul de administrație transmite situația estimărilor, care face parte din documentul unic de programare, Comisiei și țărilor terțe cu care Uniunea a încheiat acorduri astfel cum se menționează la articolul 42 alineatul (2).

(4) Pe baza situației estimărilor, Comisia înscrie în proiectul de buget general al Uniunii estimările pe care le consideră necesare pentru schema de personal și valoarea contribuției care urmează să fie suportată din bugetul general al Uniunii, pe care le prezintă Parlamentului European și Consiliului în conformitate cu articolul 314 din TFUE.

(5) Parlamentul European și Consiliul autorizează creditele reprezentând contribuția Uniunii alocată ENISA.

(6) Parlamentul European și Consiliul adoptă schema de personal a ENISA.

([26]) Decizia (UE, Euratom) 2015/443 a Comisiei din 13 martie 2015 privind securitatea în cadrul Comisiei (JO L 72, 17.3.2015, p. 41).
([27]) Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 72, 17.3.2015, p. 53).

(7) Consiliul de administrație adoptă bugetul ENISA odată cu documentul unic de programare. Bugetul ENISA se definitivează după adoptarea definitivă a bugetului general al Uniunii. Dacă este necesar, consiliul de administrație ajustează bugetul ENISA și documentul unic de programare în conformitate cu bugetul general al Uniunii.

Articolul 30

Structura bugetului ENISA

(1) Fără a aduce atingere altor resurse, veniturile ENISA sunt alcătuite astfel:

(a) dintr-o contribuție de la bugetul general al Uniunii;

(b) din venituri alocate unor cheltuieli specifice în conformitate cu normele sale financiare menționate la articolul 32;

(c) dintr-o finanțare din partea Uniunii sub forma unor acorduri de delegare sau de granturi ad-hoc, în conformitate cu normele sale financiare menționate la articolul 32 și cu dispozițiile instrumentelor relevante care sprijină politicile Uniunii;

(d) din eventuale contribuții din partea țărilor terțe care participă la lucrările ENISA, astfel cum se menționează la articolul 42;

(e) din orice contribuție voluntară din partea statelor membre, în bani sau în natură.

Statele membre care oferă contribuții voluntare în temeiul primului paragraf litera (e) nu pot solicita niciun drept sau serviciu specific ca rezultat al acelor contribuții.

(2) Cheltuielile ENISA cuprind cheltuieli cu personalul, cheltuieli administrative și de suport tehnic, cheltuieli cu infrastructura și operaționale, precum și cheltuieli rezultate din contracte cu părți terțe.

Articolul 31

Execuția bugetară a ENISA

(1) Directorul executiv răspunde de execuția bugetului ENISA.

(2) Auditorul intern al Comisiei exercită asupra ENISA aceleași prerogative ca și asupra serviciilor Comisiei.

(3) Contabilul ENISA trimite conturile provizorii contabilului Comisiei și Curții de Conturi pentru exercițiul financiar (exercițiul N) până la data de 1 martie a următorului exercițiu financiar (exercițiul N + 1).

(4) După primirea observațiilor formulate de Curtea de Conturi privind conturile provizorii ale ENISA în temeiul articolului 246 din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului ([28]), contabilul ENISA întocmește conturile finale ale ENISA pe răspunderea sa și le prezintă consiliului de administrație în vederea avizării.

(5) Consiliul de administrație emite un aviz cu privire la conturile finale ale ENISA.

(6) Până la data de 31 martie a exercițiului N + 1, directorul executiv transmite Parlamentului European, Consiliului, Comisiei și Curții de Conturi raportul privind gestiunea bugetară și financiară.

(7) Până la data de 1 iulie a exercițiului N + 1, contabilul ENISA transmite Parlamentului European, Consiliului, contabilului Comisiei și Curții de Conturi conturile finale ale ENISA, împreună cu avizul consiliului de administrație.

([28]) Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii, de modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012 (JO L 193, 30.7.2018, p. 1).

(8) La aceeași dată la care transmite conturile finale ale ENISA, contabilul ENISA transmite, de asemenea, Curții de Conturi și, în copie, contabilului Comisiei, o scrisoare cuprinzând declarațiile conducerii cu privire la conturile finale respective.

(9) Până la data de 15 noiembrie a exercițiului N + 1, directorul executiv publică conturile finale ale ENISA în *Jurnalul Oficial al Uniunii Europene*.

(10) Până la data de 30 septembrie a exercițiului N + 1, directorul executiv transmite Curții de Conturi un răspuns la observațiile acesteia și transmite, de asemenea, o copie a răspunsului respectiv consiliului de administrație și Comisiei.

(11) Directorul executiv prezintă Parlamentului European, la cererea acestuia, orice informații necesare pentru buna desfășurare a procedurii de descărcare de gestiune pentru exercițiul financiar în cauză în conformitate cu articolului 261 alineatul (3) din Regulamentul (UE, Euratom) 2018/1046.

(12) La recomandarea Consiliului, Parlamentul European acordă, înaintea datei de 15 mai a exercițiului N + 2, descărcarea de gestiune directorului executiv în ceea ce privește execuția bugetului pentru exercițiul N.

Articolul 32

Reglementări financiare

Normele financiare aplicabile ENISA se adoptă de către consiliul de administrație după consultarea Comisiei. Acestea nu derogă de la Regulamentul delegat (UE) nr. 1271/2013, cu excepția cazului o astfel de derogare se impune în mod special pentru funcționarea ENISA, iar Comisia și-a dat acordul prealabil.

Articolul 33

Combaterea fraudei

(1) Pentru a facilita combaterea fraudei, a corupției și a altor activități ilegale, în temeiul Regulamentului (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului ([29]), până la 10 decembrie 2019, ENISA aderă 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) ([30]). ENISA adoptă dispozițiile corespunzătoare care se aplică tuturor angajaților ENISA, folosind modelul prevăzut în anexa la respectivul acord.

(2) Curtea de Conturi are competența de a-i audita, pe baza documentelor și a inspecțiilor la fața locului, pe toți beneficiarii de granturi, contractanții și subcontractanții care au primit fonduri ale Uniunii din partea ENISA.

(3) OLAF poate efectua investigații, inclusiv controale și inspecții la fața locului, în conformitate cu dispozițiile și procedurile prevăzute în Regulamentul nr. 883/2013 și în Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului ([31]), pentru a stabili existența unei fraude, a unui act de corupție sau dacă a avut loc orice altă activitate ilegală care afectează interesele financiare ale Uniunii în legătură cu un grant sau un contract finanțat de ENISA.

(4) Fără a aduce atingere alineatelor (1), (2) și (3), acordurile de cooperare cu țările terțe sau cu organizațiile internaționale, contractele, acordurile de grant și deciziile de acordare a unui grant ale ENISA conțin dispoziții care împuternicesc în mod expres Curtea de Conturi și OLAF să efectueze astfel de audituri și investigații, în conformitate cu competențele care le revin.

([29]) Regulamentul (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului din 11 septembrie 2013 privind investigațiile efectuate de Oficiul European de Luptă Antifraudă (OLAF) și de abrogare a Regulamentului (CE) nr. 1073/1999 al Parlamentului European și al Consiliului și a Regulamentului (Euratom) nr. 1074/1999 al Consiliului (JO L 248, 18.9.2013, p. 1).

([30]) JO L 136, 31.5.1999, p. 15.

([31]) Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului din 11 noiembrie 1996 privind controalele și inspecțiile la fața locului efectuate de Comisie în scopul protejării intereselor financiare ale Comunităților Europene împotriva fraudei și a altor abateri (JO L 292, 15.11.1996, p. 2).

CAPITOLUL V

Personalul

Articolul 34

Dispoziții generale

Personalului ENISA i se aplică Statutul funcționarilor și Regimul aplicabil celorlalți agenți, precum și normele adoptate de comun acord de instituțiile Uniunii pentru punerea în aplicare a Statutului funcționarilor și a Regimului aplicabil celorlalți agenți.

Articolul 35

Privilegii și imunități

Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene, anexat la TUE și la TFUE, se aplică ENISA și personalului acesteia.

Articolul 36

Directorul executiv

(1) Directorul executiv este angajat ca agent temporar al ENISA în temeiul articolului 2 litera (a) din Regimul aplicabil celorlalți agenți.

(2) Directorul executiv este numit de consiliul de administrație dintr-o listă de candidați propusă de Comisie, în urma unei proceduri de selecție deschise și transparente.

(3) În scopul încheierii contractului de muncă al directorului executiv, ENISA este reprezentată de președintele Consiliului de administrație.

(4) Înainte de a fi numit în funcție, candidatul selectat de consiliul de administrație este invitat să facă o declarație în fața comisiei competente a Parlamentului European și să răspundă întrebărilor adresate de membrii acesteia.

(5) Durata mandatului directorului executiv este de cinci ani. Până la sfârșitul perioadei respective, Comisia realizează o evaluare a rezultatelor obținute de directorul executiv și viitoarele atribuții și provocări ale ENISA.

(6) Consiliul de administrație adoptă deciziile privind numirea, prelungirea mandatului sau demiterea din funcție a directorului executiv în conformitate cu articolul 18 alineatul (2).

(7) La propunerea Comisiei, care ia în considerare evaluarea menționată la alineatul (5), consiliul de administrație poate reînnoi mandatul directorului executiv o singură dată, cu o perioadă de cinci ani.

(8) Consiliul de administrație informează Parlamentul European în legătură cu intenția sa de a prelungi mandatul directorului executiv. În cursul perioadei de trei luni care precedă prelungirea mandatului său, directorul executiv, dacă este invitat, face o declarație în fața comisiei relevante a Parlamentului European și răspunde întrebărilor deputaților.

(9) Un director executiv al cărui mandat a fost prelungit nu poate să participe la o nouă procedură de selecție pentru același post.

(10) Directorul executiv poate fi demis din funcție numai printr-o decizie a consiliului de administrație care acționează la propunerea Comisiei.

Articolul 37

Experții naționali detașați și alte categorii de personal

(1) ENISA poate face apel la experți naționali detașați sau alte categorii de personal care nu sunt angajați ai ENISA. Acestor categorii de personal nu li se aplică Statutul funcționarilor și Regimul aplicabil celorlalți agenți.

(2) Consiliul de administrație adoptă o decizie de stabilire a normelor aplicabile detașării experților naționali la ENISA.

CAPITOLUL VI

Dispoziții generale privind ENISA

Articolul 38

Statutul juridic al ENISA

(1) ENISA este un organ al Uniunii și are personalitate juridică.

(2) În fiecare stat membru, ENISA dispune de cea mai extinsă capacitate juridică acordată persoanelor juridice în temeiul dreptului intern. Aceasta poate, în special, să dobândească sau să înstrăineze bunuri mobile și imobile și să se constituie parte în proceduri judiciare.

(3) ENISA este reprezentată de directorul său executiv.

Articolul 39

Răspunderea ENISA

(1) Răspunderea contractuală a ENISA este reglementată de legea aplicabilă contractului în cauză.

(2) Curtea de Justiție a Uniunii Europene este competentă să se pronunțe în temeiul oricărei clauze compromisorii cuprinse într-un contract încheiat de ENISA.

(3) În materie de răspundere necontractuală, ENISA, repară orice prejudiciu cauzat de personalul său în cursul exercitării atribuțiilor acestuia, în conformitate cu principiile generale comune legislațiilor statelor membre.

(4) Curtea de Justiție a Uniunii Europene este competentă în ceea ce privește orice litigiu privind repararea prejudiciilor astfel cum se menționează la alineatul (3).

(5) Răspunderea personală a personalului ENISA față de ENISA este reglementată de condițiile relevante care se aplică personalului ENISA.

Articolul 40

Regimul lingvistic

(1) Regulamentul nr. 1 al Consiliului ([32]) se aplică ENISA. Statele membre și celelalte organisme desemnate de către statele membre se pot adresa ENISA și pot primi răspunsuri în una dintre limbile oficiale ale instituțiilor Uniunii, la alegerea acestora.

(2) Serviciile de traducere necesare funcționării ENISA sunt asigurate de către Centrul de Traduceri pentru Organismele Uniunii Europene.

Articolul 41

Protecția datelor cu caracter personal

(1) Prelucrarea datelor cu caracter personal de către ENISA face obiectul Regulamentului (UE) 2018/1725.

(2) Consiliul de administrație adoptă normele de punere în aplicare astfel cum se menționează la articolul 45 alineatul (3) din Regulamentul (UE) 2018/1725. Consiliul de administrație poate adopta dispozițiile suplimentare necesare pentru aplicarea de către ENISA a Regulamentului (UE) 2018/1725.

([32]) Regulamentul nr. 1 al Consiliului de stabilire a regimului lingvistic al Comunității Economice Europene (JO 17, 6.10.1958, p. 385/58).

Articolul 42

Cooperarea cu țările terțe și cu organizațiile internaționale

(1) În măsura în care este necesar pentru atingerea obiectivelor stabilite în prezentul regulament, ENISA poate coopera cu autoritățile competente din țările terțe sau cu organizațiile internaționale sau cu ambele. În acest scop, ENISA poate stabili acorduri de lucru cu autoritățile din țări terțe și cu organizații internaționale, sub rezerva aprobării prealabile a Comisiei. Respectivele acorduri de lucru nu creează obligații legale pentru Uniune și nici pentru statele sale membre.

(2) ENISA este deschisă participării țărilor terțe care au încheiat acorduri cu Uniunea în acest sens. În baza dispozițiilor relevante ale acestor acorduri, se stabilesc acorduri de lucru care specifică, în special, caracterul, amploarea și modalitatea participării acestor țări terțe la activitatea ENISA, inclusiv dispoziții referitoare la participarea la inițiativele puse în practică de ENISA, la contribuțiile financiare și la personal. În ceea ce privește chestiunile legate de personal, aceste acorduri de lucru respectă, în orice caz, Statutul funcționarilor și Regimul aplicabil celorlalți agenți.

(3) Consiliul de administrație adoptă o strategie pentru relațiile cu țări terțe și cu organizații internaționale, în ceea ce privește aspectele pentru care ENISA este competentă. Comisia se asigură că ENISA își desfășoară activitatea în limitele mandatului său și în cadrul instituțional existent prin încheierea de acorduri de lucru adecvate cu directorul agenției.

Articolul 43

Norme de securitate privind protecția informațiilor sensibile neclasificate și a informațiilor clasificate

După consultarea Comisiei, ENISA adoptă norme de securitate care pun în aplicare principiile de securitate cuprinse în normele de securitate ale Comisiei pentru protecția informațiilor sensibile neclasificate și a IUEC, astfel cum sunt prevăzute în Deciziile (UE, Euratom) 2015/443 și (UE, Euratom) 2015/444. Normele de securitate ale ENISA includ dispoziții privind schimbul, prelucrarea și stocarea unor astfel de informații.

Articolul 44

Acordul privind sediul și condițiile de funcționare

(1) Prevederile necesare referitoare la sediul care urmează să fie pus la dispoziția ENISA în statul membru gazdă și la facilitățile care urmează să fie oferite de statul membru respectiv, precum și normele specifice aplicabile în statul membru gazdă directorului executiv, membrilor consiliului de administrație, personalului ENISA și membrilor familiilor acestora se stabilesc într-un acord privind sediul, încheiat între ENISA și statul membru gazdă după obținerea aprobării consiliului de administrație.

(2) Statul membru care găzduiește ENISA pune la dispoziție cele mai bune condiții posibile pentru a asigura buna funcționare a ENISA, ținând cont de accesibilitatea amplasamentului, existența unor facilități adecvate de educație pentru copiii personalului, un acces corespunzător la piața muncii, la securitate socială și la asistență medicală atât pentru copiii, cât și pentru soții sau soțiile personalului.

Articolul 45

Controlul administrativ

Activitățile ENISA fac obiectul supravegherii de către Ombudsmanul European, în conformitate cu articolul 228 din TFUE.

TITLUL III

CADRUL DE CERTIFICARE A SECURITĂȚII CIBERNETICE

Articolul 46

Cadrul european de certificare a securității cibernetice

(1) Se instituie cadrul european de certificare a securității cibernetice pentru a îmbunătăți condițiile de funcționare a pieței interne prin creșterea nivelului de securitate cibernetică în Uniune și prin permiterea unei abordări armonizate la nivelul Uniunii în privința sistemelor europene de certificare a securității cibernetice, în scopul creării unei piețe unice digitale pentru produsele TIC, serviciile TIC și procesele TIC.

(2) Cadrul european de certificare a securității cibernetice prevede un mecanism pentru instituirea unor sisteme europene de certificare a securității cibernetice și pentru a atesta că produsele TIC, serviciile TIC și procesele TIC, care au fost evaluate în conformitate cu sistemele respective sunt conforme cu cerințele de securitate specificate, cu scopul de a proteja disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise ori prelucrate sau funcțiile ori serviciile oferite de aceste produse, servicii și procese sau accesibile prin intermediul acestora pe întregul lor ciclu de viață.

Articolul 47

Programul de activitate etapizat la nivelul Uniunii pentru certificarea europeană a securității cibernetice

(1) Comisia publică un program de activitate etapizat la nivelul Uniunii pentru certificarea europeană a securității cibernetice (denumit în continuare „programul de activitate etapizat la nivelul Uniunii") în care se identifică prioritățile strategice pentru viitoarele sisteme europene de certificare a securității cibernetice.

(2) Programul de activitate etapizat la nivelul Uniunii include îndeosebi o listă a produselor TIC, serviciilor TIC și proceselor TIC sau a categoriilor acestora care pot beneficia de includerea în sfera de aplicare a unui sistem european de certificare a securității cibernetice.

(3) Includerea unui anumit produs TIC, serviciu TIC și proces TIC sau a unei categorii a acestora în programul de activitate etapizat la nivelul Uniunii se justifică în baza unuia sau a mai multora dintre considerentele următoarele:

(a) disponibilitatea și dezvoltarea sistemelor naționale de certificare a securității cibernetice care se aplică oricărei categorii specifice de produse TIC, servicii TIC și procese TIC, cu precădere în ceea ce privește riscul de fragmentare;

(b) politica sau dreptul relevant al Uniunii sau al statelor membre;

(c) cererea de pe piață;

(d) dezvoltările din aria amenințărilor cibernetice;

(e) solicitarea de pregătire a unei propuneri de sistem specifice de către ECCG.

(4) Comisia ține seama în mod corespunzător de avizele emise în privința proiectului de program de activitate etapizat la nivelul Uniunii de către ECCG și de către Grupul părților interesate pentru certificare.

(5) Primul program de activitate etapizat la nivelul Uniunii se publică până la 28 iunie 2020. Programul de activitate etapizat la nivelul Uniunii se actualizează cel puțin o dată la trei ani sau mai des, dacă este necesar.

Articolul 48

Solicitarea unui sistem european de certificare a securității cibernetice

(1) Comisia îi poate solicita ENISA să pregătească o propunere de sistem sau să revizuiască un sistem european de certificare a securității cibernetice existent, pe baza programului de activitate etapizat la nivelul Uniunii.

(2) În cazuri justificate în mod corespunzător, Comisia sau ECCG îi poate solicita ENISA să pregătească o propunere de sau să revizuiască un sistem european de certificare a securității cibernetice existent, fără ca acestea să fie incluse în programul de activitate etapizat la nivelul Uniunii. Programul de activitate etapizat la nivelul Uniunii se actualizează în consecință.

Articolul 49

Pregătirea, adoptarea și revizuirea unui sistem european de certificare a securității cibernetice

(1) În urma unei solicitări din partea Comisiei în temeiul articolului 48, ENISA pregătește o propunere de sistem care îndeplinește cerințele prevăzute la articolele 51, 52 și 54.

(2) În urma unei solicitări din partea ECCG în temeiul articolului 48 alineatul (2), ENISA poate pregăti o propunere de sistem care îndeplinește cerințele prevăzute la articolele 51, 52 și 54. În cazul în care refuză o altfel de solicitare, ENISA prezintă motivele de refuz. Orice decizie de refuzare a unei astfel de solicitări se ia de către consiliul de administrație.

(3) Atunci când pregătește propunerile de sisteme, ENISA consultă toate părțile interesate relevante printr-un proces de consultare formal, deschis, transparent și cuprinzător.

(4) Pentru fiecare propunere de sistem, ENISA instituie un grup de lucru ad-hoc în conformitate cu articolul 20 cu scopul de a-i oferi ENISA consiliere și expertiză specifice.

(5) ENISA cooperează strâns cu ECCG. ECCG furnizează ENISA asistență și consiliere de specialitate în legătură cu pregătirea propunerii de sistem și adoptă un aviz privind propunerea de sistem.

(6) ENISA ține seama în cea mai mare măsură posibilă de avizul ECCG înainte de a transmite Comisiei propunerea de sistem pregătită în conformitate cu alineatele (3), (4) și (5). Avizul ECCG nu este obligatoriu pentru ENISA, iar lipsa unui astfel de aviz nu împiedică ENISA să transmită Comisiei propunerea de sistem.

(7) Pe baza propunerii de sistem pregătite de ENISA, Comisia poate adopta acte de punere în aplicare care să prevadă sisteme europene de certificare a securității cibernetice pentru produsele TIC, serviciile TIC și procesele TIC care îndeplinesc cerințele prevăzute la articolele 51, 52 și 54. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 66 alineatul (2).

(8) ENISA evaluează cel puțin o dată la cinci ani fiecare sistem european de certificare a securității cibernetice adoptat, ținând seama de observațiile primite de la părțile interesate. Dacă este necesar, Comisia sau ECCG îi pot solicita ENISA să demareze procesul de elaborare a unei propuneri revizuite de sistem în conformitate cu articolul 48 și cu prezentul articol.

Articolul 50

Site-ul referitor la sistemele europene de certificare a securității cibernetice

(1) ENISA întreține un site dedicat care oferă informații despre sistemele europene de certificare a securității cibernetice, certificatele europene de securitate cibernetică și declarațiile de conformitate UE, și le asigură publicitatea, inclusiv informații în ceea ce privește sistemele europene de certificare a securității cibernetice care nu mai sunt valabile, certificatele europene de securitate cibernetică și declarațiile de conformitate UE retrase sau expirate și registrul conținând legături către informații despre securitatea cibernetică furnizate în conformitate cu articolul 55.

(2) După caz, site-ul menționat la alineatul (1) indică și sistemele naționale de certificare a securității cibernetice care au fost înlocuite de un sistem european de certificare a securității cibernetice.

Articolul 51

Obiectivele de securitate ale sistemelor europene de certificare a securității cibernetice

Un sistem european de certificare a securității cibernetice este conceput pentru a îndeplini, după caz, cel puțin următoarele obiective de securitate:

(a) să protejeze datele stocate, transmise sau prelucrate într-un alt mod împotriva stocării, prelucrării, accesului sau divulgării accidentale sau neautorizate pe întregul ciclu de viață al produsului TIC, serviciului TIC sau procesului TIC;

(b) să protejeze datele stocate, transmise sau prelucrate într-un alt mod împotriva distrugerii, pierderii sau modificării accidentale sau neautorizate ori lipsei de disponibilitate pe întregul ciclu de viață al produsului TIC, serviciului TIC sau procesului TIC;

(c) să asigure faptul că persoanele, programele sau dispozitivele autorizate pot avea acces numai la datele, serviciile sau funcțiile la care se referă drepturile lor de acces;

(d) să identifice și să documenteze dependențele și vulnerabilitățile cunoscute;

(e) să înregistreze care sunt datele, serviciile sau funcțiile care au fost accesate, utilizate sau procesate în alt mod, în ce moment și de către cine;

(f) să facă posibil să se verifice care sunt datele, serviciile sau funcțiile care au fost accesate, utilizate sau procesate în alt mod, în ce moment și de către cine;

(g) să verifice că produsele TIC, serviciile TIC și procesele TIC nu conțin vulnerabilități cunoscute;

(h) să restabilească disponibilitatea datelor, serviciilor și funcțiilor și accesul la acestea în timp util în cazul unui incident fizic sau tehnic;

(i) să asigure că produsele TIC, serviciile TIC și procesele TIC sunt securizate implicit și începând cu momentul conceperii;

(j) să asigure că produsele TIC, serviciile TIC și procesele TC sunt furnizate cu software și hardware actualizate care nu conțin vulnerabilități cunoscute public și că sunt prevăzute cu mecanisme pentru actualizări securizate.

Articolul 52

Niveluri de asigurare ale sistemelor europene de certificare a securității cibernetice

(1) Un sistem european de certificare a securității cibernetice poate stabili unul sau mai multe dintre următoarele niveluri de asigurare pentru produsele TIC, serviciile TIC și procesele TIC: „de bază”, „substanțial” sau „ridicat”. Nivelul de asigurare este corespunzător nivelului riscului asociat cu utilizarea preconizată a unui produs TIC, serviciu TIC sau proces TIC, înțeles ca probabilitate și impact al unui incident.

(2) Certificatele europene de securitate cibernetică și declarațiile de conformitate UE fac trimitere la orice nivel de asigurare prevăzut în sistemul european de certificare a securității cibernetice în temeiul căruia a fost emis certificatul european de securitate cibernetică sau declarația de conformitate UE.

(3) Cerințele de securitate corespunzătoare fiecărui nivel de asigurare sunt prevăzute de sistemul european de certificare a securității cibernetice relevant, inclusiv funcțiile de securitate corespunzătoare și rigoarea și profunzimea corespunzătoare ale evaluării la care a fost supus produsul TIC, serviciul TIC sau procesul TIC.

(4) Certificatul sau declarația de conformitate UE face trimitere la specificații tehnice, standarde și proceduri conexe acestora, inclusiv controale tehnice, al căror scop este de a diminua riscul de incidente de securitate cibernetică sau de a le preîntâmpina.

(5) Un certificat european de securitate cibernetică sau o declarație de conformitate UE care face trimitere la nivelul de asigurare „de bază” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC și procesele TIC pentru care se eliberează certificatul respectiv sau declarația de conformitate UE respectivă îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor de bază cunoscute de incidente și atacuri cibernetice. Activitățile de evaluare includ cel puțin o examinare a documentației tehnice. În cazurile în care o astfel de examinare nu este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.

(6) Un certificat european de securitate cibernetică care face trimitere la nivelul de asigurare „substanțial” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC și procesele TIC pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor pentru securitatea cibernetică cunoscute și a riscurilor de incidente și atacuri cibernetice desfășurate de actori cu competențe și resurse limitate. Activitățile de evaluare includ cel puțin următoarele: o examinare pentru a demonstra absența vulnerabilităților cunoscute public și testarea faptului că produsele TIC, serviciile TIC și procesele TIC implementează corect funcțiile de securitate necesare. În cazurile în care oricare dintre aceste activități de evaluare nu este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.

(7) Un certificat european de securitate cibernetică care face trimitere la nivelul de asigurare „ridicat” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC și procesele TIC pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscului de atacuri cibernetice de ultimă generație desfășurate de actori cu competențe și resurse substanțiale. Activitățile de evaluare includ cel puțin următoarele: o examinare pentru a demonstra absența vulnerabilităților cunoscute public; testarea pentru a demonstra că produsele TIC, serviciile TIC și procesele TIC implementează corect funcțiile de securitate necesare, la nivel de ultimă generație, și o evaluare a rezistenței acestora la atacatori competenți prin teste de rezistență la intruziuni. În cazurile în care oricare dintre aceste activități de evaluare nu este adecvată, se desfășoară activități înlocuitoare cu efect echivalent.

(8) Un sistem european de certificare a securității cibernetice poate specifica mai multe niveluri de evaluare în funcție de rigoarea și profunzimea metodologiei de evaluare utilizate. Fiecare dintre nivelurile de evaluare corespunde unuia dintre nivelurile de asigurare și este definit printr-o combinație corespunzătoare de componente ale asigurării.

Articolul 53

Autoevaluarea conformității

(1) Un sistem european de certificare a securității cibernetice poate permite efectuarea unei autoevaluări a conformității pe răspunderea exclusivă a producătorului sau a furnizorului de produse TIC, servicii TIC și procese TIC. O astfel de autoevaluare a conformității este permisă numai în cazul produselor TIC, serviciilor TIC și proceselor TIC care prezintă un risc redus corespunzând nivelului de asigurare „de bază”.

(2) Producătorul sau furnizorul de produse TIC, servicii TIC și procese TIC poate elibera o declarație de conformitate UE care menționează că s-a demonstrat îndeplinirea cerințelor prevăzute în sistem. Prin eliberarea unei astfel de declarații, producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC își asumă responsabilitatea pentru conformitatea produsului TIC, a serviciului TIC sau a procesului TIC cu cerințele stabilite în sistemul respectiv.

(3) Producătorul sau furnizorul de produse TIC, servicii TIC și procese TIC pun la dispoziția autorității naționale de certificare a securității cibernetice menționată la articolul 58, pe durata stabilită în sistemul european de certificare a securității cibernetice corespunzător, declarația de conformitate UE, documentația tehnică și toate celelalte informații relevante legate de conformitatea produselor TIC sau a serviciilor TIC cu sistemul. O copie a declarației de conformitate UE se transmite către autoritatea națională de certificare a securității cibernetice și către ENISA.

(4) Eliberarea unei declarații de conformitate UE este voluntară, cu excepția cazului în care se prevede altfel în dreptul Uniunii sau dreptul statelor membre.

(5) Declarația de conformitate UE este recunoscută în toate statele membre.

Articolul 54

Elemente ale sistemelor europene de certificare a securității cibernetice

(1) Un sistem european de certificare a securității cibernetice include cel puțin următoarele elemente:

(a) obiectul și sfera de aplicare a sistemului de certificare, inclusiv tipul sau categoriile de produse TIC, servicii TIC și procese TIC acoperite;

(b) o descriere clară a scopului sistemului și a modului în care standardele selectate, metodele de evaluare și nivelurile de asigurare corespund nevoilor utilizatorilor preconizați ai sistemului;

(c) trimiteri la standardele internaționale, europene sau naționale aplicate în cadrul evaluării sau, în cazul în care astfel de standarde nu sunt disponibile sau nu sunt adecvate, la specificațiile tehnice care îndeplinesc cerințele prevăzute în anexa II la Regulamentul (UE) nr. 1025/2012 sau, dacă astfel de specificații nu sunt disponibile, la specificații tehnice sau la alte cerințe de securitate cibernetică definite în sistemul european de certificare a securității cibernetice;

(d) după caz, unul sau mai multe niveluri de asigurare;

(e) o precizare care indică dacă autoevaluarea conformității este permisă în cadrul sistemului;

(f) după caz, cerințe specifice sau suplimentare cărora se supun organismele de evaluare a conformității pentru a garanta competența tehnică a acestora de a evalua cerințele de securitate cibernetică;

(g) criteriile și metodele specifice de evaluare, inclusiv tipurile de evaluări, utilizate pentru a demonstra că obiectivele de securitate menționate la articolul 51 sunt îndeplinite;

(h) după caz, informațiile necesare pentru certificare care trebuie furnizate sau puse în alt mod la dispoziția organismelor de evaluare a conformității de către solicitant;

(i) în cazul în care sistemul prevede mărci sau etichete, condițiile în care pot fi utilizate aceste mărci sau etichete;

(j) normele pentru monitorizarea conformității produselor TIC, serviciilor TIC și proceselor TIC cu cerințele certificatelor europene de securitate cibernetică sau ale declarațiilor de conformitate UE, inclusiv mecanisme care să demonstreze conformitatea neîntreruptă cu cerințele de securitate cibernetică specificate;

(k) după caz, condițiile de eliberare, de menținere, de continuare și de reînnoire a certificatelor europene de securitate cibernetică, precum și condițiile de extindere sau de restrângere a domeniului de aplicare a certificării;

(l) normele privind consecințele neconformității produselor TIC, serviciilor TIC și proceselor TIC care au fost certificare sau pentru care a fost eliberată o declarație de conformitate UE, dar care nu sunt conforme cu cerințele sistemului;

(m) normele privind modalitățile de raportare și soluționare a vulnerabilităților în materie de securitate cibernetică nedetectate anterior ale produselor TIC, serviciilor TIC și proceselor TIC;

(n) după caz, normele privind păstrarea evidențelor de către organismele de evaluare a conformității;

(o) identificarea sistemelor naționale sau internaționale de certificare a securității cibernetice care se referă la aceleași tipuri sau categorii de produse TIC, servicii TIC și procese TIC, cerințele de securitate și criteriile și metodele de evaluare și nivelurile de asigurare;

(p) conținutul și formatul certificatelor europene de securitate cibernetică și ale declarațiilor de conformitate UE care urmează să fie eliberate;

(q) perioada de valabilitate a declarației de conformitate UE, documentația tehnică și toate celelalte informații relevante care sunt puse la dispoziție de producătorul sau de furnizorul de produse TIC, de servicii TIC sau de procese TIC;

(r) perioada maximă de valabilitate a certificatelor europene de securitate cibernetică eliberate în temeiul sistemului;

(s) politica de divulgare pentru certificatele europene de securitate cibernetică eliberate modificate sau retrase în temeiul sistemului;

(t) condițiile pentru recunoașterea reciprocă a sistemelor de certificare cu țări terțe;

(u) după caz, normele privind orice mecanism de evaluare *inter pares* instituit în cadrul sistemului pentru autoritățile sau organismele care eliberează certificate europene de securitate cibernetică pentru nivelul de asigurare „ridicat” în temeiul articolului 56 alineatul (6). Un astfel de mecanism nu aduce atingere evaluării *inter pares* prevăzute la articolul 59;

(v) formatul și procedurile care trebuie urmate de producători sau de furnizori de produse TIC, de servicii TIC sau de procese TIC atunci când furnizează și actualizează informațiile suplimentare privind securitatea cibernetică în conformitate cu articolul 55.

(2) Cerințele specificate ale sistemului european de certificare a securității cibernetice sunt în concordanță cu cerințele legale aplicabile, în special cu cerințele care decurg din dreptul armonizat al Uniunii.

(3) În cazul în care un act juridic specific al Uniunii prevede astfel, un certificat sau o declarație de conformitate UE eliberată în cadrul unui sistem european de certificare a securității cibernetice poate fi utilizată pentru a demonstra prezumția de conformitate cu cerințele din acel act juridic.

(4) În absența unui drept armonizat al Uniunii, dreptul unui stat membru poate prevedea, de asemenea, că se poate folosi un sistem european de certificare a securității cibernetice pentru a stabili prezumția de conformitate cu cerințele legale.

Articolul 55

Informații suplimentare privind securitatea cibernetică pentru produsele TIC, serviciile TIC și procesele TIC certificate

(1) Producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC certificate sau de produse TIC, servicii TIC sau procese TIC pentru care a fost eliberată o declarație de conformitate UE pune la dispoziția publicului următoarele informații suplimentare privind securitatea cibernetică:

(a) orientări și recomandări care să le servească utilizatorilor finali la configurarea, instalarea, derularea, funcționarea și întreținerea securizate a produselor TIC sau serviciilor TIC;

(b) perioada în timpul căreia se oferă asistență în materie de securitate utilizatorilor finali, mai ales în ceea ce privește disponibilitatea actualizărilor legate de securitatea cibernetică;

(c) informații de contact ale producătorului sau furnizorului și metode acceptate pentru primirea informațiilor despre vulnerabilitate de la utilizatorii finali și de la cercetători din domeniul securității;

(d) o trimitere la registrele online care conțin vulnerabilitățile divulgate public legate de produsul TIC, de serviciul TIC sau de procesul TIC și orice avertismente relevante în materie de securitate cibernetică.

(2) Informațiile menționate la alineatul (1) se pun la dispoziție în format electronic și rămân disponibile și se actualizează după cum este necesar cel puțin până la expirarea certificatului european de securitate cibernetică sau a declarației de conformitate UE aferente.

Articolul 56

Certificarea securității cibernetice

(1) Produsele TIC, serviciile TIC și procesele TIC care au fost certificate în cadrul unui sistem european de certificare a securității cibernetice adoptat în temeiul articolului 49 sunt considerate a fi conforme cu cerințele acestui sistem.

(2) Certificarea securității cibernetice este voluntară, cu excepția cazului în care se prevede altfel în dreptul Uniunii sau în dreptul unui stat membru.

(3) Comisia evaluează periodic eficiența și utilizarea sistemelor europene de certificare a securității cibernetice adoptate și analizează dacă un anumit sistem european de certificare a securității cibernetice trebuie să devină obligatoriu prin dreptul relevant al Uniunii, pentru a se asigura un nivel adecvat de securitate cibernetică a produselor TIC, serviciilor TIC și proceselor TIC în Uniune și pentru a se îmbunătăți funcționarea pieței interne. Prima evaluare se efectuează până la 31 decembrie 2023, iar evaluările ulterioare se efectuează cel puțin din doi în doi ani după această dată. Pe baza rezultatelor evaluărilor respective, Comisia identifică produsele TIC, serviciile TIC și procesele TIC care fac obiectul unui sistem de certificare existent și care trebuie să fie incluse într-un sistem de certificare obligatoriu.

Comisia se concentrează cu prioritate pe sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, pe care le evaluează cel târziu la doi ani de la adoptarea primului sistem european de certificare a securității cibernetice.

Atunci când pregătește evaluarea, Comisia:

(a) ia în considerare impactul măsurilor asupra producătorilor sau furnizorilor de astfel de produse TIC, servicii TIC sau procese TIC, precum și asupra utilizatorilor în ceea ce privește costul măsurilor respective, avantajele societale sau economice care decurg din nivelul sporit de securitate preconizat pentru produsele TIC, serviciile TIC sau procesele TIC vizate;

(b) ține seama de existența și de punerea în aplicare a dreptului relevant al statelor membre și al țărilor terțe;

(c) desfășoară un proces de consultare deschis, transparent și cuprinzător cu toate părțile interesate relevante și cu statele membre;

(d) ia în considerare termenele de punere în aplicare, precum și măsurile și perioadele de tranziție, în special în ceea ce privește impactul posibil al măsurilor asupra producătorilor sau a furnizorilor de produse TIC, servicii TIC sau procese TIC, inclusiv asupra IMM-urilor;

(e) propune cea mai rapidă și mai eficace modalitate de punere în aplicare a tranziției de la un sistem de certificare voluntar la unul obligatoriu.

(4) Organismele de evaluare a conformității menționate la articolul 60 eliberează certificate europene de securitate cibernetică în temeiul prezentului articol, care fac trimitere la nivelul de asigurare „de bază" sau „substanțial" pe baza criteriilor incluse în sistemul european de certificare a securității cibernetice adoptat de Comisie în temeiul articolului 49.

(5) Prin derogare de la alineatul (4), în cazuri justificate în mod corespunzător, un sistem european de certificare a securității cibernetice poate prevedea că certificatele europene de securitate cibernetică ce rezultă din acel sistem pot fi emise numai de un organism public. Acest organism este una din următoarele entități:

(a) o autoritate națională de certificare a securității cibernetice astfel cum este menționată la articolul 58 alineatul (1); sau

(b) un organism public care este acreditat ca organism de evaluare a conformității în temeiul articolului 60 alineatul (1).

(6) În cazurile în care un sistem european de certificare a securității cibernetice adoptat în temeiul articolului 49 impune un nivel de asigurare „ridicat", certificatul european de securitate cibernetică în temeiul sistemului respectiv se eliberează numai de o autoritate națională de certificare a securității cibernetice sau, în următoarele cazuri, de un organism de evaluare a conformității:

(a) cu aprobarea prealabilă a autorității de certificare a securității cibernetice pentru fiecare certificat european de securitate cibernetică individual eliberat de un organism de evaluare a conformității; sau

(b) pe baza unei delegări generale a atribuției de eliberare a acestor certificate europene de securitate cibernetică către organismul de evaluare a conformității de către autoritatea națională de certificare a securității cibernetice.

(7) Persoana fizică sau juridică care își supune certificării produsele TIC, serviciile TIC sau procesele TIC pune la dispoziția autorității naționale de certificare a securității cibernetice menționată la articolul 58, în cazul în care această autoritate este organismul care eliberează certificatul european de securitate cibernetică, sau la dispoziția organismului de evaluare a conformității menționat la articolul 60 toate informațiile necesare pentru desfășurarea certificării.

(8) Deținătorul unui certificat european de securitate cibernetică informează autoritatea sau organismul menționat la alineatul (7) despre orice vulnerabilități sau nereguli detectate ulterior, legate de securitatea produsului TIC, a serviciului TIC sau a procesului TIC certificat, care pot avea un impact asupra conformității sale cu cerințele legate de certificare. Autoritatea sau organismul respectiv transmite aceste informații fără întârzieri nejustificate autorității naționale de certificare a securității cibernetice în cauză.

(9) Certificatele europene de securitate cibernetică se eliberează pentru durata prevăzută de sistemul european de certificare a securității cibernetice și pot fi reînnoite numai dacă sunt îndeplinite în continuare cerințele relevante.

(10) Un certificat european de securitate cibernetică eliberat în temeiul prezentului articol este recunoscut în toate statele membre.

Articolul 57

Sistemele și certificatele naționale de certificare de a securității cibernetice

(1) Fără a aduce atingere alineatului (3) din prezentul articol, sistemele naționale de certificare a securității cibernetice și procedurile aferente pentru produsele TIC, serviciile TIC și procesele TIC care fac obiectul unui sistem european de certificare a securității cibernetice încetează să mai producă efecte de la data stabilită în actul de punere în aplicare adoptat în temeiul articolului 49 alineatul (7). Sistemele naționale de certificare a securității cibernetice și procedurile aferente pentru produsele TIC, serviciile TIC și procesele TIC care nu fac obiectul unui sistem european de certificare a securității cibernetice continuă să existe.

(2) Statele membre nu introduc noi sisteme naționale de certificare a securității cibernetice pentru produsele TIC, serviciile TIC și procesele TIC care fac deja obiectul unui sistem european de certificare a securității cibernetice în vigoare.

(3) Certificatele existente care au fost eliberate în temeiul sistemelor naționale de certificare a securității cibernetice și care fac obiectul unui sistem european de certificare a securității cibernetice rămân valabile până la data expirării lor.

(4) Pentru a se evita fragmentarea pieței interne, statele membre informează Comisia și ECCG cu privire la orice intenție de a elabora noi sisteme naționale de certificare a securității cibernetice.

Articolul 58

Autoritățile naționale de certificare a securității cibernetice

(1) Fiecare stat membru desemnează pe teritoriul său una sau mai multe autorități naționale de certificare a securității cibernetice sau, cu acordul unui alt stat membru, desemnează una sau mai multe autorități naționale de certificare a securității cibernetice stabilite în celălalt stat membru pentru a fi responsabile de atribuțiile de supraveghere în statul membru care face desemnarea.

(2) Fiecare stat membru informează Comisia cu privire la identitatea autorităților naționale de certificare de securitate cibernetică desemnate. În cazul în care un stat membru desemnează mai multe autorități, acesta informează Comisia și cu privire la sarcinile atribuite fiecăreia dintre respectivele autorități.

(3) Fără a aduce atingere articolului 56 alineatul (5) litera (a) și articolului 56 alineatul (6), fiecare autoritate națională de certificare a securității cibernetice este independentă în ceea ce privește organizarea, deciziile de finanțare, structura juridică și luarea deciziilor, de entitățile pe care le supraveghează.

(4) Statele membre se asigură că activitățile autorităților naționale de certificare a securității cibernetice, care se referă la eliberarea de certificate europene de securitate cibernetică menționate la articolul 56 alineatul (5) litera (a) și la articolul 56 alineatul (6) sunt strict separate de activitățile de supraveghere prevăzute în prezentul articol și că activitățile respective sunt desfășurate independent una de cealaltă.

(5) Statele membre se asigură că autoritățile naționale de certificare a securității cibernetice dispun de resursele adecvate pentru a-și exercita competențele și pentru a-și îndeplini cu eficacitate și în mod eficient sarcinile.

(6) Pentru punerea efectivă în aplicare a prezentului regulament, este oportun ca autoritățile naționale de certificare a securității cibernetice să participe la ECCG în mod activ, eficace, eficient și sigur.

(7) Autoritățile naționale de certificare a securității cibernetice:

(a) supraveghează și asigură respectarea normelor incluse în sistemele europene de certificare a securității cibernetice în temeiul articolului 54 alineatul (1) litera (j) pentru monitorizarea conformității produselor TIC, serviciilor TIC și proceselor TIC cu cerințele certificatelor europene de securitate cibernetică eliberate pe teritoriile lor respective, în cooperare cu alte autorități relevante de supraveghere a pieței;

(b) monitorizează respectarea obligațiilor producătorilor sau furnizorilor de produse TIC, servicii TIC sau procese TIC care sunt stabiliți pe teritoriile lor respective și care desfășoară autoevaluări ale conformității, și pun în aplicare aceste obligații, în special a obligațiilor unor astfel de producători sau furnizori prevăzute la articolul 53 alineatele (2) și (3) și în sistemele europene de certificare a securității cibernetice corespunzătoare;

(c) fără a aduce atingere articolului 60 alineatul (3), asistă și sprijină activ organismele naționale de acreditare la monitorizarea și supravegherea activităților organismelor de evaluare a conformității în sensul prezentului regulament;

(d) monitorizează și supraveghează activitățile organismelor publice menționate la articolul 56 alineatul (5);

(e) după caz, autorizează organismele de evaluare a conformității în conformitate cu articolul 60 alineatul (3) și restricționează, suspendă sau retrag autorizația existentă atunci când organismele de evaluare a conformității încalcă cerințele prezentului regulament;

(f) tratează plângerile persoanelor fizice sau juridice în legătură cu certificatele europene de securitate cibernetică eliberate de autoritățile naționale de certificare a securității cibernetice sau cu cele eliberate de organismele de evaluare a conformității în conformitate cu articolul 56 alineatul (6), sau în legătură cu declarațiile de conformitate UE eliberate în temeiul articolului 53, și investighează, în măsura în care este oportun, subiectul plângerii și informează reclamantul despre stadiul și rezultatul investigației, într-un termen rezonabil;

(g) prezintă ENISA și ECCG un raport anual de sinteză privind măsurile întreprinse în temeiul literelor (b), (c) și (d) din prezentul alineat sau în temeiul alineatului (8);

(h) cooperează cu alte autorități naționale de certificare a securității cibernetice sau cu alte autorități publice, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor TIC, serviciilor TIC și proceselor TIC cu cerințele prezentului regulament sau cu cerințele sistemului european de certificare a securității cibernetice specific; și

(i) monitorizează evoluțiile relevante din domeniul certificării securității cibernetice.

(8) Fiecare autoritate națională de certificare a securității cibernetice dispune cel puțin de următoarele competențe:

(a) competența de a cere organismelor de evaluare a conformității, deținătorilor de certificate europene de securitate cibernetică și entităților care eliberează declarații de conformitate UE să furnizeze toate informațiile care îi sunt necesare pentru îndeplinirea atribuțiilor sale;

(b) competența de a efectua investigații, sub formă de audituri, asupra organismelor de evaluare a conformității, a titularilor de certificate europene de securitate cibernetică și a entităților care eliberează declarații de conformitate UE pentru a verifica conformitatea acestora cu prezentul titlu;

(c) competența de a lua măsuri adecvate, în conformitate cu dreptul intern, pentru a se asigura că organismele de evaluare a conformității, titularii de certificate europene de securitate cibernetică și entitățile care eliberează declarații de conformitate UE respectă prezentul regulament sau un sistem european de certificare a securității cibernetice;

(d) competența de a obține acces la sediile oricărui organism de evaluare a conformității sau al titularilor de certificate europene de securitate cibernetică cu scopul de a desfășura investigații în conformitate cu dreptul procedural al Uniunii sau al statului membru;

(e) competența de a retrage, în conformitate cu dreptul intern, certificatele europene de securitate cibernetică eliberate de autoritățile naționale de certificare a securității cibernetice sau cele eliberate de organismele de evaluare a conformității în conformitate cu articolul 56 alineatul (6), atunci când astfel de certificate nu sunt conforme cu prezentul regulament sau cu un sistem european de certificare a securității cibernetice;

(f) competența de a impune sancțiuni, în conformitate cu dreptul intern, astfel cum se prevede la articolul 65, și de a cere încetarea imediată a încălcărilor obligațiilor prevăzute de prezentul regulament.

(9) Autoritățile naționale de certificare a securității cibernetice cooperează între ele și cu Comisia în special prin schimb de informații, de experiență și de bune practici în ceea ce privește certificarea securității cibernetice și aspectele tehnice privind securitatea cibernetică a produselor TIC, a serviciilor TIC și proceselor TIC.

Articolul 59

Evaluarea *inter pares*

(1) Pentru a se ajunge la standarde echivalente pe întreg teritoriul Uniunii cu privire la certificatele europene de securitate cibernetică și la declarațiile de conformitate UE, autoritățile naționale de certificare a securității cibernetice fac obiectul unei evaluări *inter pares*.

(2) Evaluarea *inter pares* se efectuează pe baza unor criterii și proceduri de evaluare clare și transparente, în special în privința cerințelor structurale, de resurse umane și de proces, a confidențialității și a plângerilor.

(3) Evaluarea *inter pares* examinează următoarele aspecte:

(a) după caz, dacă activitățile autorităților naționale de certificare a securității cibernetice legate de eliberarea certificatelor europene de securitate cibernetică menționate la articolul 56 alineatul (5) litera (a) și la articolul 56 alineatul (6) sunt strict separate de activitățile de supraveghere prevăzute la articolul 58 și dacă activitățile respective sunt desfășurate independent una de cealaltă;

(b) procedurile de supraveghere și de asigurare a respectării normelor de monitorizare a conformității produselor TIC, serviciilor TIC și proceselor TIC cu certificatele europene de securitate cibernetică în temeiul articolului 58 alineatul (7) litera (a);

(c) procedurile de monitorizare și de asigurare a respectării obligațiilor producătorilor și ale furnizorilor de produse TIC, de servicii TIC sau de procese TIC în conformitate cu articolul 58 alineatul (7) litera (b);

(d) procedurile de monitorizare, de autorizare și de supraveghere a activităților desfășurate de organismele de evaluare a conformității;

(e) după caz, dacă personalul autorităților sau organismelor care eliberează certificate pentru nivelul de asigurare „ridicat” în temeiul articolului 56 alineatul (6) deține expertiza corespunzătoare.

(4) Evaluarea *inter pares* se desfășoară cel puțin o dată la cinci ani de către cel puțin două autorități naționale de certificare a securității cibernetice din alte state membre și de către Comisie. ENISA poate participa la evaluarea *inter pares*.

(5) Comisia poate adopta acte de punere în aplicare prin care să stabilească un plan pentru evaluarea *inter pares*, care acoperă o perioadă de cel puțin cinci ani, și să definească criterii privind componența echipei de evaluare *inter pares*, metodologia utilizată pentru evaluarea *inter pares*, calendarul, frecvența și alte atribuții legate de aceasta. Atunci când adoptă respectivele acte de punere în aplicare, Comisia ține seama în mod corespunzător de observațiile formulate de ECCG. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 66 alineatul (2).

(6) Rezultatele evaluării *inter pares* sunt examinate de ECCG, care întocmește un rezumat ce poate fi făcut public, și care, atunci când este necesar, formulează orientări sau recomandări cu privire la acțiunile sau măsurile care trebuie întreprinse de entitățile în cauză.

Articolul 60

Organisme de evaluare a conformității

(1) Organismele de evaluare a conformității sunt acreditate de organismele naționale de acreditare desemnate în temeiul Regulamentului (CE) nr. 765/2008. Acreditarea respectivă se eliberează numai dacă organismul național de acreditare îndeplinește cerințele stabilite în anexa la prezentul regulament.

(2) În cazurile în care un certificat european de securitate cibernetică este eliberat de o autoritate națională de certificare a securității cibernetice în temeiul articolului 56 alineatul (5) litera (a) și al articolului 56 alineatul (6), organismul de certificare al autorității naționale de certificare a securității cibernetice este acreditat ca organism de evaluare a conformității în temeiul alineatului (1) din prezentul articol.

(3) În cazul în care sistemele europene de certificare a securității cibernetice stabilesc cerințe specifice sau suplimentare în temeiul articolului 54 alineatul (1) litera (f), numai organismele de evaluare a conformității care îndeplinesc aceste cerințe sunt autorizate de autoritatea națională de certificare a securității cibernetice pentru îndeplinirea atribuțiilor în temeiul sistemelor respective.

(4) Acreditarea menționată la alineatul (1) se eliberează organismelor de evaluare a conformității pentru o perioadă de maximum cinci ani și poate fi reînnoită în aceleași condiții numai dacă organismul de evaluare a conformității îndeplinește în continuare cerințele prevăzute la prezentul articol. Organismele naționale de acreditare iau toate măsurile corespunzătoare într-un termen rezonabil pentru a restricționa, a suspenda sau a revoca acreditarea unui organism de evaluare a conformității eliberată în temeiul alineatului (1) în cazul în care condițiile de acreditare nu sunt sau nu mai sunt îndeplinite sau în cazul în care organismul de evaluare a conformității încalcă prezentul regulament.

Articolul 61

Notificare

(1) Pentru fiecare sistem european de certificare a securității cibernetice, autoritățile naționale de certificare a securității cibernetice îi notifică Comisiei organismele de evaluare a conformității care au fost acreditate și, după caz, autorizate în temeiul articolului 60 alineatul (3) să elibereze certificate europene de securitate cibernetică la nivelurile de asigurare specificate menționate la articolul 52. Autoritățile naționale de certificare a securității cibernetice îi notifică Comisiei, fără nicio întârziere nejustificată, orice modificare ulterioară referitoare la acestea.

(2) La un an de la intrarea în vigoare a unui sistem european de certificare a securității cibernetice, Comisia publică în *Jurnalul Oficial al Uniunii Europene* o listă a organismelor de evaluare a conformității notificate în temeiul sistemului respectiv.

(3) În cazul în care primește o notificare după expirarea perioadei menționate la alineatul (2), Comisia publică în *Jurnalul Oficial al Uniunii Europene* modificările listei a organismelor de evaluare a conformității notificate, în termen de două luni de la data primirii notificării respective.

(4) O autoritate națională de certificare a securității cibernetice poate înainta Comisiei o cerere de retragere a unui organism de evaluare a conformității notificat de autoritatea respectivă din lista menționată la alineatul (2). Comisia publică în *Jurnalul Oficial al Uniunii Europene* modificările corespunzătoare aduse listei respective, în termen de o lună de la data primirii cererii adresate de autoritatea națională de certificare a securității cibernetice.

(5) Comisia poate adopta acte de punere în aplicare prin care să stabilească circumstanțele, formatele și procedurile pentru notificările menționate la alineatul (1) din prezentul articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 66 alineatul (2).

Articolul 62

Grupul european pentru certificarea securității cibernetice

(1) Se instituie Grupul european pentru certificarea securității cibernetice (ECCG).

(2) ECCG este compus din reprezentanți ai autorităților naționale de certificare a securității cibernetice sau din reprezentanți ai altor autorități naționale relevante. Niciun membru ECCG nu poate reprezenta mai mult de două state membre.

(3) Părțile interesate și părțile terțe relevante pot fi invitate să participe la reuniunile ECCG și la activitățile acestuia.

(4) ECCG are următoarele atribuții:

(a) să acorde consiliere și asistență Comisiei în activitatea sa de asigurare a punerii în practică și a aplicării coerente a prezentului titlu, în special în ceea ce privește programul de activitate etapizat la nivelul Uniunii, chestiunile legate de politica în materie de certificare a securității cibernetice, coordonarea abordărilor privind politicile și pregătirea unor sisteme europene de certificare a securității cibernetice;

(b) să acorde asistență și consiliere ENISA și să coopereze cu aceasta în legătură cu pregătirea unei propuneri de sistem în temeiul articolului 49;

(c) să adopte un aviz cu privire la propunerea de sistem pregătită de ENISA în temeiul articolului 49;

(d) să solicite ENISA să pregătească propuneri de sistem în temeiul articolului 48 alineatul (2);

(e) să adopte avize adresate Comisiei cu privire la întreținerea și revizuirea sistemelor europene de certificare a securității cibernetice existente;

(f) să examineze evoluțiile relevante din domeniul securității cibernetice și să facă schimb de informații și de bune practici privind sistemele de certificare a securității cibernetice;

(g) să faciliteze cooperarea dintre autoritățile naționale de certificare a securității cibernetice desfășurată în temeiul prezentului titlu prin consolidarea capacităților și prin schimbul de informații, în special prin stabilirea unor metode care să permită schimbul eficient de informații referitoare la chestiunile privind certificarea securității cibernetice;

(h) să sprijine punerea în aplicare a mecanismelor de evaluare *inter pares* în conformitate cu normele stabilite în cadrul unui sistem european de certificare a securității cibernetice în temeiul articolului 54 alineatul (1) litera (u);

(i) să faciliteze alinierea sistemelor europene de certificare a securității cibernetice la standardele recunoscute pe plan internațional, inclusiv prin revizuirea actualelor sisteme europene de certificare a securității cibernetice și, după caz, recomandând ENISA să colaboreze cu organizațiile internaționale de standardizare relevante pentru a remedia insuficiențele sau lacunele care afectează standardele internaționale recunoscute care sunt în vigoare.

(5) Comisia prezidează ECCG cu asistență din partea ENISA și asigură secretariatul acestuia în conformitate cu articolul 8 alineatul (1) litera (e).

Articolul 63

Dreptul de a depune o plângere

(1) Persoanele fizice sau juridice au dreptul să depună o plângere la entitatea care a eliberat un certificat european de securitate cibernetică sau, dacă plângerea se referă la un certificat european de securitate cibernetică eliberat de un organism de evaluare a conformității în temeiul articolului 56 alineatul (6), la autoritatea națională relevantă de certificare a securității cibernetice.

(2) Autoritatea sau organismul la care s-a depus plângerea informează reclamantul despre evoluția procedurilor și despre decizia luată, și despre dreptul de a exercita o cale de atac eficientă în temeiul articolului 64.

Articolul 64

Dreptul la o cale de atac eficientă

(1) În pofida oricăror căi de atac administrative sau a altor căi de atac fără caracter judiciar, persoanele fizice și juridice au dreptul să exercite o cale de atac eficientă cu privire la:

(a) deciziile luate de autoritatea sau organismul menționat la articolul 63 alineatul (1), inclusiv, după caz, în legătură cu emiterea necorespunzătoare, omisiunea de a emite sau recunoașterea unui certificat european de securitate cibernetică deținut de respectivele persoane fizice și juridice;

(b) omisiunea de a da curs unei plângeri depuse la o autoritate sau un organism menționat la articolul 63 alineatul (1).

(2) Acțiunile în temeiul prezentului articol se introduc în fața instanțelor din statul membru în care este situată autoritatea sau organismul împotriva căruia se exercită calea de atac.

Articolul 65

Sancțiuni

Statele membre stabilesc normele privind sancțiunile care se aplică în cazul încălcării prezentului titlu și a încălcării sistemelor europene de certificare a securității cibernetice și iau toate măsurile necesare pentru a asigura punerea în aplicare a acestora. Sancțiunile prevăzute sunt eficace, proporționale și cu efect de descurajare. Statele membre informează Comisia fără întârziere cu privire la normele și măsurile respective și notifică acesteia orice modificare ulterioară care le afectează.

TITLUL IV

DISPOZIȚII FINALE

Articolul 66

Procedura comitetului

(1) Comisia este asistată de un comitet. Comitetul respectiv reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 alineatul (4) litera (b) din Regulamentul (UE) nr. 182/2011.

Articolul 67

Evaluare și revizuire

(1) Până la 28 iunie 2024 și la fiecare cinci ani după aceea, Comisia evaluează impactul, eficacitatea și eficiența activității ENISA și a practicilor sale de lucru, posibila necesitate de a modifica mandatul ENISA și implicațiile financiare ale unei astfel de modificări. Evaluarea ține seama de orice punct de vedere comunicat ENISA ca răspuns la activitățile sale. În cazul în care Comisia consideră că nu se mai justifică continuarea activității ENISA în raport cu obiectivele, mandatul și atribuțiile încredințate acesteia, Comisia poate propune modificarea prezentului regulament în ceea ce privește dispozițiile referitoare la ENISA.

(2) Evaluarea analizează, de asemenea, impactul, eficacitatea și eficiența dispozițiilor din titlul III din prezentul regulament în ceea ce privește obiectivele de asigurare a unui nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC și a proceselor TIC în Uniune și de îmbunătățire a funcționării pieței interne.

(3) Evaluarea examinează dacă sunt necesare cerințe esențiale de securitate cibernetică pentru a avea acces la piața internă, cu scopul de a împiedica ca produsele TIC, serviciile TIC și procesele TIC care nu respectă cerințele de bază în materie de securitate cibernetică să intre pe piața Uniunii.

(4) Până la 28 iunie 2024, și ulterior din cinci în cinci ani Comisia trimite raportul de evaluare împreună cu concluziile sale, Parlamentului European, Consiliului și consiliului de administrație. Concluziile raportului respectiv sunt făcute publice.

Articolul 68

Abrogare și succesiune

(1) Regulamentul (UE) nr. 526/2013 se abrogă cu efect de la 27 iunie 2019.

(2) Trimiterile la Regulamentul (UE) nr. 526/2013 și la ENISA astfel cum este instituită prin regulamentul respectiv se interpretează ca trimiteri la prezentul regulament și la ENISA astfel cum e instituită prin prezentul regulament.

(3) ENISA astfel cum e instituită de prezentul regulament succedă ENISA astfel cum este instituită prin Regulamentul (UE) nr. 526/2013 în ceea ce privește toate aspectele legate de proprietate, acorduri, obligații juridice, contracte de muncă, angajamente financiare și răspunderi. Toate deciziile consiliului de administrație și ale comitetului executiv adoptate cu conformitate cu Regulamentul (UE) nr. 526/2013 rămân valabile, cu condiția ca acestea să respecte prezentul regulament.

(4) ENISA se înființează pentru o perioadă nedeterminată de la 27 iunie 2019.

(5) Directorul executiv numit în temeiul articolului 24 alineatul (4) din Regulamentul (UE) nr. 526/2013 rămâne în funcție și exercită funcțiile directorului executiv astfel cum sunt menționate la articolul 20 din prezentul regulament pentru perioada rămasă din mandatul său. Celelalte condiții ale contractului său rămân neschimbate.

(6) Membrii consiliului de administrație și supleanții acestora numiți în temeiul articolului 6 din Regulamentul (UE) nr. 526/2013 rămâne în funcție și exercită funcțiile consiliului de administrație astfel cum sunt menționate la articolul 15 din prezentul regulament și supleanții acestora pentru perioada rămasă din mandatul lor.

Articolul 69

Intrare în vigoare

(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

(2) Articolele 58, 60, 61, 63, 64 și 65 se aplică de la 28 iunie 2021.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Strasbourg, 17 aprilie 2019.

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*
A. TAJANI	G. CIAMBA

ANEXĂ

CERINȚE CARE TREBUIE ÎNDEPLINITE DE ORGANISMELE DE EVALUARE A CONFORMITĂȚII

Organismele de evaluare a conformității care doresc să fie acreditate îndeplinesc următoarele cerințe:

1. Un organism de evaluare a conformității trebuie să fie înființat în temeiul dreptului intern și să aibă personalitate juridică.

2. Un organism de evaluare a conformității trebuie să fie un organism terț care este independent de organizația sau de produsele TIC, de serviciile TIC sau de procesele TIC pe care le evaluează.

3. Un organism care aparține unei asociații de întreprinderi sau unei federații profesionale care reprezintă întreprinderile implicate în conceperea, producerea, furnizarea, asamblarea, utilizarea sau întreținerea produselor TIC, serviciilor TIC sau procesele TIC pe care le evaluează poate fi considerat un organism de evaluare a conformității, cu condiția să demonstreze că este independent și că nu există conflicte de interese.

4. Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu pot fi proiectantul, producătorul, furnizorul, instalatorul, cumpărătorul, proprietarul, utilizatorul sau operatorul de întreținere al produsului TIC, al serviciului TIC sau al procesului TIC care este evaluat sau reprezentantul autorizat al vreuneia dintre aceste părți. Această interdicție nu împiedică utilizarea produselor TIC evaluate care sunt necesare pentru operațiunile organismului de evaluare a conformității sau utilizarea acestor produse TIC în scopuri personale.

5. Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu pot fi direct implicați în conceperea, producerea sau construcția, comercializarea, instalarea, utilizarea sau întreținerea produselor TIC, serviciilor TIC sau proceselor TIC care sunt evaluate și nu pot reprezenta părțile angajate în acele activități. Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu se implică în activități care le-ar putea afecta imparțialitatea sau integritatea în ceea ce privește activitățile de evaluare a conformității. Această interdicție se aplică în special serviciilor de consultanță.

6. Dacă un organism de evaluare a conformității este deținut sau gestionat de o entitate sau de o instituție publică, se asigură și se documentează independența și absența oricărui conflict de interese între autoritatea națională de certificare a securității cibernetice, pe de o parte, și organismul de evaluare a conformității, pe de altă parte.

7. Organismele de evaluare a conformității se asigură că activitățile filialelor și ale subcontractanților lor nu afectează confidențialitatea, obiectivitatea sau imparțialitatea activităților lor de evaluare a conformității.

8. Organismele de evaluare a conformității și personalul acestora îndeplinesc activitățile de evaluare a conformității cu cel mai înalt grad de integritate profesională și cu competența tehnică necesară în domeniul respectiv și nu sunt supuse niciunei presiuni și niciunei persuasiuni, inclusiv de natură financiară, care le-ar putea influența deciziile sau rezultatele activităților lor de evaluare a conformității, în special în ceea ce privește persoanele sau grupurile de persoane având interese legate de rezultatele acelor activități.

9. Un organism de evaluare a conformității trebuie să fie capabil să efectueze toate atribuțiile de evaluare a conformității care îi sunt atribuite în temeiul prezentului regulament, indiferent dacă atribuțiile respective sunt realizate în mod direct de organismul de evaluare a conformității sau în numele său și pe răspunderea sa. Orice subcontractare sau consultare a personalului extern este documentată în mod adecvat, nu implică intermediari și face obiectul unui acord scris care vizează, între altele, confidențialitatea și conflictele de interese. Organismul de evaluare a conformității în cauză își asumă întreaga răspundere pentru atribuțiile îndeplinite.

10. În orice moment și pentru fiecare procedură de evaluare a conformității și fiecare tip, categorie sau subcategorie de produse TIC, servicii TIC sau procese TIC, organismul de evaluare a conformității dispune de:

    (a) personalul necesar având cunoștințele tehnice necesare și experiența suficientă și corespunzătoare pentru a efectua atribuțiile de evaluare a conformității;

    (b) descrierile necesare ale procedurilor pe baza cărora se realizează evaluarea conformității, asigurându-se transparența acelor proceduri și posibilitatea de a le reproduce. Acesta prevede politicile și procedurile adecvate care fac distincție între atribuțiile îndeplinite ca organism notificat în temeiul articolului 61 și alte activități;

(c) procedurile necesare pentru a-și desfășura activitatea ținând seama în mod corespunzător de dimensiunea unei întreprinderi, de sectorul în care își desfășoară activitatea și de structura acesteia, de gradul de complexitate a tehnologiei produsului TIC, serviciului TIC sau procesului TIC în cauză, precum și de caracterul de serie sau de masă al procesului de producție.

11. Un organism de evaluare a conformității dispune de mijloacele necesare pentru a îndeplini în mod corespunzător atribuțiile tehnice și administrative legate de activitățile de evaluare a conformității și să aibă acces la toate echipamentele sau facilitățile necesare.

12. Personalul responsabil cu îndeplinirea activităților de evaluare a conformității posedă următoarele calități:

(a) o bună pregătire tehnică și profesională care acoperă toate activitățile de evaluare a conformității;

(b) cunoștințe satisfăcătoare ale cerințelor evaluărilor conformității pe care le realizează și autoritatea corespunzătoare pentru realizarea acestor evaluări;

(c) cunoștințe și o înțelegere corespunzătoare a cerințelor și standardelor de testare aplicabile;

(d) abilitatea necesară pentru a elabora certificate, evidențe și rapoarte care să demonstreze că evaluările conformității au fost realizate.

13. Se garantează imparțialitatea organismelor de evaluare a conformității, a personalului de conducere de nivel superior și a persoanelor responsabile cu îndeplinirea atribuțiilor de evaluare a conformității, precum și a subcontractanților.

14. Remunerația personalului de conducere de nivel superior și a persoanelor responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu depinde de numărul de evaluări ale conformității realizate sau de rezultatele evaluărilor respective.

15. Organismele de evaluare a conformității încheie o asigurare de răspundere civilă în cazul în care răspunderea nu este asumată de statul membru în conformitate cu dreptul intern sau statul membru nu este direct responsabil de evaluarea conformității.

16. Organismul de evaluare a conformității și personalul său, comitetele, filialele, subcontractanții și orice organism asociat sau personalul organismelor externe ale unui organism de evaluare a conformității păstrează confidențialitatea și secretul profesional în legătură cu toate informațiile obținute în îndeplinirea atribuțiilor de evaluare a conformității care le revin în temeiul prezentului regulament sau al oricărei dispoziții de drept intern care pune în aplicare prezentul regulament, cu excepția cazului în care divulgarea este cerută prin dreptul Uniunii sau al statului membru care se aplică respectivelor persoane și cu excepția relației cu autoritățile competente ale statului membru în care își îndeplinesc activitățile. Drepturile de autor sunt protejate. Organismul de evaluare a conformității dispune de proceduri documentate în ceea ce privește cerințele din prezentul punct.

17. Cu excepția punctului 16, cerințele din prezenta anexă nu împiedică în schimburile de informații tehnice și de orientări în materie de reglementare între un organism de evaluare a conformității și o persoană care solicită certificarea, sau care intenționează să solicite certificarea.

18. Organismele de evaluare a conformității funcționează în conformitate cu un ansamblu de termeni și condiții coerente, echitabile și rezonabile, ținând seama de interesele IMM-urilor, în ceea ce privește taxele.

19. Organismele de evaluare a conformității îndeplinesc cerințele standardului relevant care este armonizat în temeiul Regulamentului (CE) nr. 765/2008 pentru acreditarea organismelor de evaluare a conformității care efectuează certificarea produselor TIC, serviciilor TIC sau proceselor TIC.

20. Organismele de evaluare a conformității se asigură că laboratoarele de testare utilizate în scopul evaluării conformității respectă cerințele standardului relevant care este armonizat în temeiul Regulamentului (CE) nr. 765/2008 pentru acreditarea laboratoarelor care efectuează testări.