

Miercuri, 17 aprilie 2019

P8\_TA(2019)0419

## **Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și Rețeaua de centre naționale de coordonare \*\*\*I**

**Rezoluția legislativă a Parlamentului European din 17 aprilie 2019 referitoare la propunerea de regulament al Parlamentului European și al Consiliului de instituire a Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare (COM(2018)0630 – C8-0404/2018 – 2018/0328(COD))**

**(Procedura legislativă ordinară: prima lectură)**

(2021/C 158/66)

Parlamentul European,

- având în vedere propunerea Comisiei prezentată Parlamentului European și Consiliului (COM(2018)0630),
  - având în vedere articolul 294 alineatul (2), articolul 173 alineatul (3) și articolul 188 primul paragraf din Tratatul privind funcționarea Uniunii Europene, în temeiul cărora propunerea a fost prezentată Parlamentului de către Comisie (C8-0404/2018),
  - având în vedere articolul 294 alineatul (3) din Tratatul privind funcționarea Uniunii Europene,
  - având în vedere avizul Comitetului Economic și Social European din 23 ianuarie 2019 <sup>(1)</sup>,
  - având în vedere articolul 59 din Regulamentul său de procedură,
  - având în vedere raportul Comisiei pentru industrie, cercetare și energie și avizul Comisiei pentru piața internă și protecția consumatorilor (A8-0084/2019),
1. adoptă poziția sa în primă lectură prezentată în continuare <sup>(2)</sup>;
  2. solicită Comisiei să îl sesizeze din nou în cazul în care își înlocuiește, își modifică în mod substanțial sau intenționează să-și modifice în mod substanțial propunerea;
  3. încredințează Președintelui sarcina de a transmite Consiliului și Comisiei, precum și parlamentelor naționale poziția Parlamentului.

## **P8\_TC1-COD(2018)0328**

**Poziția Parlamentului European adoptată în primă lectură la 17 aprilie 2019 în vederea adoptării Regulamentului (UE) .../... al Parlamentului European și al Consiliului de instituire a Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare**

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 173 alineatul (3) și articolul 188 primul paragraf,

<sup>(1)</sup> Nepublicat încă în Jurnalul Oficial.

<sup>(2)</sup> Prezenta poziție corespunde amendamentelor adoptate la 13 martie 2019 (Texte adoptate, P8\_TA(2019)0189).

Miercuri, 17 aprilie 2019

având în vedere propunerea Comisiei Europene,

având în vedere avizul Comitetului Economic și Social European <sup>(1)</sup>,

având în vedere avizul Comitetului Regiunilor <sup>(2)</sup>,

hotărând în conformitate cu procedura legislativă ordinară <sup>(3)</sup>,

întrucât:

- (1) ~~Viața~~ **Peste 80 % din populația Uniunii este conectată la internet și viața** noastră de zi cu zi și economiile noastre devin din ce în ce mai dependente de tehnologiile digitale, iar cetățenii sunt din ce în ce mai expuși la incidente cibernetice grave. Viitorul securității depinde, printre altele, de **ameliorarea rezilienței globale, de consolidarea capacității tehnologice și industriale de a proteja Uniunea împotriva amenințărilor cibernetice, mereu în evoluție**, întrucât atât infrastructura ~~civilă~~, cât și capacitățile ~~militare~~ **în materie de securitate** depind de sisteme digitale sigure. **O astfel de securitate poate fi realizată prin sensibilizarea publicului cu privire la amenințările la adresa securității cibernetice, prin dezvoltarea competențelor, a capacităților și a capabilităților în întreaga UE, ținând seama cu atenție de interdependențele care caracterizează infrastructura hardware și software, rețelele, produsele și procesele, precum și de implicațiile și de preocupările societale și etice.** [AM 1]
- (1a) **Criminalitatea cibernetică constituie o amenințare în creștere rapidă la adresa Uniunii, a cetățenilor și a economiei sale. În 2017, 80 % dintre întreprinderile europene s-au confruntat cu cel puțin un incident cibernetic. Atacul WannaCry, produs în mai 2017, a afectat peste 150 de țări și 230 000 de sisteme informatice și a avut un impact semnificativ asupra infrastructurilor critice, cum ar fi spitalele. Această situație evidențiază necesitatea de a deține cele mai înalte standarde de securitate cibernetică și soluții holistice de securitate cibernetică, implicând oamenii, produsele, procesele și tehnologia din Uniune, precum și necesitatea poziției de lider al Uniunii în domeniu și nevoia de autonomie digitală.** [AM 2]
- (2) Uniunea și-a intensificat în mod constant activitățile pentru a răspunde provocărilor din ce în ce mai mari în materie de securitate cibernetică, în urma Strategiei de securitate cibernetică din 2013 <sup>(4)</sup>, care vizează promovarea unui ecosistem cibernetic fiabil, sigur și deschis. În 2016, Uniunea a adoptat primele măsuri în domeniul securității cibernetice prin Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului <sup>(5)</sup> privind securitatea rețelilor și a sistemelor informatice.
- (3) În septembrie 2017, Comisia și Înalțul Reprezentant al Uniunii pentru afaceri externe și politica de securitate au prezentat o comunicare comună <sup>(6)</sup> intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”, cu scopul de a consolida și mai mult reziliența, capacitatea de descurajare și răspunsul UE la atacurile cibernetice.
- (4) În cadrul summitului digital de la Tallinn din septembrie 2017, șefii de stat și de guvern au lansat Uniunii apelul de a ocupa „o poziție de lider mondial în domeniul securității cibernetice până în 2025, pentru a asigura protecția cetățenilor, a consumatorilor și a întreprinderilor noastre online, precum și pentru a câștiga încrederea acestora, dar și pentru a permite un internet liber, **mai sigur** și aflat sub incidența legii.” **și s-au declarat pentru „utilizarea mai intensă a soluțiilor cu sursă deschisă și/sau a standardelor deschise atunci când se (re)construiesc sisteme și soluții informatice (printre altele pentru a evita situațiile în care cumpărătorul depinde de vânzător), inclusiv cele dezvoltate și/sau promovate de programele UE pentru interoperabilitate și standardizare, cum ar fi ISA<sup>2</sup>”.** [AM 3]

<sup>(1)</sup> JO C, p. .

<sup>(2)</sup> JO C , , p. .

<sup>(3)</sup> Poziția Parlamentului European din 17 aprilie 2019.

<sup>(4)</sup> Comunicare comună către Parlamentul European și Consiliu: Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat, JOIN(2013) 1 final.

<sup>(5)</sup> Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelilor și a sistemelor informatice în Uniune (JO L 194, 19.7.2016, p. 1).

<sup>(6)</sup> Comunicare comună către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”, JOIN(2017)0450 final.

Miercuri, 17 aprilie 2019

- (4a) *Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică („Centrul de competențe”) ar trebui să contribuie la sporirea rezilienței și fiabilității infrastructurii rețelelor și a sistemelor informatice, inclusiv a internetului și a altor infrastructuri critice pentru funcționarea societății, cum ar fi sistemele de transport, de sănătate și cele bancare.* [AM 4]
- (4b) *Centrul de competențe și acțiunile sale ar trebui să țină seama de punerea în aplicare a Regulamentului (UE) 2019/XXX [reformare a Regulamentului (CE) nr. 428/2009 în conformitate cu propunerea COM(2016)0616] (<sup>7</sup>).* [AM 5]
- (5) O perturbare semnificativă a rețelelor și a sistemelor informatice poate afecta statele membre și Uniunea în ansamblu. Prin urmare, **securitatea cel mai înalt nivel de securitate a rețelelor și a sistemelor informatice este esențială pentru buna funcționare a pieței interne la nivelul Uniunii este deopotrivă esențial pentru societate și economie.** În prezent, Uniunea depinde de furnizorii de securitate cibernetică din afara Europei. Cu toate acestea, este în interesul strategic al Uniunii să se asigure că păstrează și dezvoltă capacitățile tehnologice esențiale în materie de securitate cibernetică pentru a-și securiza piața unică digitală și, în special, pentru a proteja rețelele și sistemele informatice critice **protecția datelor și a rețelelor și sistemelor informatice critice ale cetățenilor și întreprinderilor europene, inclusiv infrastructurile critice pentru funcționarea societății, cum ar fi sistemele de transport, de sănătate și bancare, precum și pe cele ale pieței unice digitale,** și pentru a furniza servicii de securitate cibernetică esențiale. [AM 6]
- (6) Uniunea deține o multitudine de cunoștințe de specialitate și o vastă experiență în ceea ce privește cercetarea, tehnologia și dezvoltarea industrială în materie de securitate cibernetică, însă eforturile comunităților industriale și de cercetare sunt fragmentate, nu există o aliniere între acestea și o misiune comună, fapt care împiedică competitivitatea și **protecția eficace a datelor, a rețelelor și a sistemelor critice** în acest domeniu. Aceste eforturi și cunoștințe de specialitate trebuie să fie puse în comun, interconectate și utilizate în mod eficient pentru a consolida și a completa capacitățile și competențele de cercetare, tehnologice și industriale existente la nivelul Uniunii și la nivel național. **Întrucât sectorul tehnologiei informației și comunicațiilor (TIC) se confruntă cu provocări importante, cum ar fi satisfacerea cererii de lucrători calificați, poate beneficia de reprezentarea diversității societății în general și de asigurarea unei reprezentări echilibrate a genurilor, a diversității etnice și a persoanelor cu handicap, precum și de facilitarea accesului la cunoștințe și la formare pentru viitorii experți în materie de securitate cibernetică, inclusiv pentru educația lor în contexte non-formale, de exemplu, în proiecte informatice privind programe gratuite și cu sursă deschisă, proiecte de tehnologie civică, întreprinderi nou-înființate și microîntreprinderi.** [AM 7]
- (6a) *Datorită agilității lor, întreprinderile mici și mijlocii (IMM-uri) joacă un rol central în sectorul securității cibernetică al Uniunii, având capacitatea de a furniza soluții de vârf. Cu toate acestea, IMM-urile care nu sunt specializate în securitate cibernetică sunt predispuse la o vulnerabilitate mai mare la incidente cibernetică, din cauza investițiilor mari și a cerințelor privind cunoștințele necesare în vederea aplicării unor soluții eficace de securitate cibernetică. Prin urmare, este necesar ca Centrul de competențe și Rețeaua de competențe în materie de securitate cibernetică („Rețeaua”) să acorde sprijin special IMM-urilor prin facilitarea accesului acestora la cunoștințe și formare profesională, pentru a le permite acestora să își asigure o securitate suficientă și pentru a le permite celor care desfășoară activități în domeniul securității cibernetică să consolideze poziția de lider al Uniunii în acest domeniu.* [AM 8]
- (6b) *Expertiza depășește contextele industriale și de cercetare. Proiectele necomerciale sau precomerciale, denumite proiecte tehnologice civice, utilizează standarde deschise, date deschise și software gratuit și cu sursă deschisă în interesul societății și al binelui public. Acestea contribuie la reziliența, conștientizarea și dezvoltarea competențelor în materie de securitate cibernetică și joacă un rol important în construirea de capacități pentru acest sector și cercetarea în domeniu.* [AM 9]

(<sup>7</sup>) Regulamentul (UE) 2019/... al Parlamentului European și al Consiliului din ... de instituire a unui regim al Uniunii pentru controlul exporturilor, transferului, serviciilor de intermediere, asistenței tehnice și tranzitului în ceea ce privește produsele cu dublă utilizare (JO L ..., ..., p. ...).

Miercuri, 17 aprilie 2019

- (6c) **Termenul „părți interesate”, atunci când este folosit în contextul prezentului regulament, se referă, printre altele la entități din sector, entități publice și alte entități care abordează aspecte operaționale și tehnice în domeniul securității cibernetice, precum și la societatea civilă, de exemplu sindicate, asociații de consumatori, comunitatea implicată în dezvoltarea de software gratuit și cu sursă deschisă, comunitatea academică și de cercetare. [AM 10]**
- (7) În concluziile sale adoptate în noiembrie 2017, Consiliul a invitat Comisia să prezinte rapid o evaluare a impactului cu privire la opțiunile posibile pentru crearea unei rețele a centrelor de competențe în materie de securitate cibernetică și a unui Centru european de competențe și de cercetare și să propună, până la jumătatea anului 2018, instrumentul juridic relevant.
- (8) Centrul de competențe ar trebui să fie principalul instrument de care dispune Uniunea pentru a pune în comun investițiile în cercetarea, tehnologia și dezvoltarea industrială în materie de securitate cibernetică și pentru a pune în aplicare proiectele și inițiativele relevante, împreună cu Rețeaua de competențe în materie de securitate cibernetică. Acesta ar trebui să ofere sprijin financiar în materie de securitate cibernetică din programele Orizont Europa și Europa digitală, **precum și din Fondul european de apărare pentru acțiuni și costuri administrative din domeniul apărării**, și ar trebui să fie deschis, după caz, Fondului european de dezvoltare regională și altor programe. Această abordare ar trebui să contribuie la crearea de sinergii și la coordonarea sprijinului financiar pentru **inițiativele Uniunii în cercetarea și dezvoltarea**, inovarea, tehnologia și dezvoltarea industrială în domeniul securității cibernetice și la evitarea suprapunerilor. [AM 11]
- (8a) **Principiul „securității de la stadiul conceperii”, astfel cum este stabilit în Comunicarea comună a Comisiei din 13 septembrie 2017, intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”, include metode de ultimă generație pentru creșterea securității, în toate etapele ciclului de viață al unui produs sau al unui serviciu, începând cu metode securizate de concepere și dezvoltare, reducând amploarea atacurilor și încorporând teste și audituri adecvate ale securității. Pe durata funcționării și a menținerii, este necesar ca producătorii sau furnizorii să pună la dispoziție, fără întârziere, actualizări care să remedieze vulnerabilitățile sau amenințările noi, pe toată durata de viață estimată a unui produs și după încheierea acesteia. Acest lucru se poate realiza și permițându-le terților să creeze și să furnizeze astfel de actualizări. Furnizarea de actualizări este necesară în special în cazul infrastructurilor, al produselor și al proceselor care sunt utilizate în mod obișnuit. [AM 12]**
- (8b) **Având în vedere amploarea problemelor de securitate cibernetică și investițiile realizate în capacitățile de securitate cibernetică în alte părți ale lumii, Uniunea și statele sale membre ar trebui să își intensifice sprijinul financiar acordat cercetării, dezvoltării și implementării în acest domeniu. Pentru a realiza economii de scară și a atinge un nivel comparabil de protecție în întreaga Uniune, statele membre ar trebui să își concentreze eforturile pentru realizarea unui cadru european, investind prin intermediul mecanismului Centrului de competențe, acolo unde este relevant. [AM 13]**
- (8c) **Pentru a încuraja competitivitatea la nivelul Uniunii și cele mai înalte standarde de securitate cibernetică la nivel internațional, Centrul de competențe și Comunitatea de competențe în materie de securitate cibernetică ar trebui să vizeze schimbul de produse și procese cibernetice, standarde și standarde tehnice cu comunitatea internațională. Standardele tehnice includ crearea unor mecanisme de punere în aplicare de referință, publicate în cadrul licențelor standard deschise. Conceperea securizată în special a mecanismelor de punere în aplicare de referință este esențială pentru fiabilitatea și reziliența infrastructurii rețelelor și a sistemelor informatice uzuale, precum internetul și infrastructurile critice. [AM 14]**
- (9) Ținând seama de faptul că obiectivele prezentei inițiative pot fi cel mai bine realizate dacă ~~participă~~ **contribuie** toate statele membre sau un număr cât mai mare de state membre și pentru a stimula participarea acestora, numai statele membre care contribuie financiar la costurile administrative și operaționale ale Centrului de competențe ar trebui să dețină drepturi de vot. [AM 15]
- (10) Participarea financiară a statelor membre participante ar trebui să fie proporțională cu contribuția financiară a Uniunii la această inițiativă.

Miercuri, 17 aprilie 2019

- (11) Centrul de competențe ar trebui să faciliteze și să contribuie la coordonarea activității Rețelei de competențe în materie de securitate cibernetică („rețeaua”), formată din centre naționale de coordonare din fiecare stat membru. Centrele naționale de coordonare ar trebui să beneficieze de sprijin financiar direct din partea Uniunii, inclusiv granturi acordate fără o cerere de propuneri, pentru a desfășura activități legate de prezentul regulament.
- (12) Centrele naționale de coordonare ar trebui selectate de către statele membre. Pe lângă capacitatea administrativă necesară, centrele ar trebui fie să dețină, fie să aibă acces direct la expertiză tehnologică în materie de securitate cibernetică, în special în domeniul precum criptografia, serviciile de securitate TIC, detectarea intruziunilor, securitatea sistemelor, securitatea rețelelor, securitatea programelor informatice și a aplicațiilor sau aspectele umane și, etice, societale și de mediu ale securității și ale protecției vieții private. Acestea ar trebui, de asemenea, să aibă capacitatea de a-și asuma efectiv angajamente și de a-și coordona acțiunile cu sectorul industrial, cu sectorul public, inclusiv cu autoritățile desemnate în temeiul Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului<sup>(8)</sup>, precum și cu comunitatea de cercetare **pentru a stabili un dialog public-privat continuu privind securitatea cibernetică. În plus, ar fi necesară sensibilizarea opiniei publice cu privire la securitatea cibernetică prin mijloace de comunicare adecvate.** [AM 16]
- (13) În cazul în care sprijinul financiar este acordat centrelor naționale de coordonare în vederea sprijinirii părților terțe la nivel național, acesta este transferat părților interesate relevante prin acorduri de grant în cascadă.
- (14) Tehnologiile emergente, cum ar fi inteligența artificială, internetul obiectelor, calculul de înaltă performanță (HPC) și informatica cuantică, ~~tehnologia blockchain~~ **precum** și concepte precum identitățile digitale sigure, creează noi provocări pentru securitatea cibernetică și, în același timp, oferă ~~soluții~~ **soluții produse și procese**. Evaluarea și validarea solidității sistemelor TIC existente sau viitoare va necesita testarea ~~soluțiilor~~ **produselor și a proceselor** de securitate împotriva atacurilor îndreptate împotriva echipamentelor HPC și cuantice. Centrul de competențe, rețeaua, **centrele europene de inovare digitală** și Comunitatea de competențe în materie de securitate cibernetică ar trebui să contribuie la progresul și la diseminarea celor mai recente ~~soluții~~ **soluții produse și procese de securitate cibernetică, inclusiv cu utilizare dublă, în special a celor care ajută organizațiile să se mențină într-o stare permanentă de consolidare a capacității, a rezilienței și a guvernantei corespunzătoare. Centrul de competențe și rețeaua ar trebui să stimuleze întregul ciclu al inovării și să creeze o punte pentru a trece de această „vale a morții” în ceea ce privește inovarea în domeniul tehnologiilor și al serviciilor de securitate cibernetică. În același timp, Centrul de competențe și rețeaua și Comunitatea ar trebui să se afle în serviciul dezvoltatorilor și al operatorilor din sectoare critice, cum ar fi transporturile, energia, sănătatea, sectorul financiar, administrația, telecomunicațiile, industria prelucrătoare, apărarea și spațiul, pentru a-i ajuta să își rezolve problemele în materie de securitate cibernetică, precum și să cerceteze diversele motivații ale atacurilor asupra integrității rețelelor și a sistemelor informatice, cum ar fi criminalitatea, spionajul industrial, defăimarea și dezinformarea.** [AM 17]
- (14a) **Ca urmare a naturii în rapidă schimbare a amenințărilor cibernetică și a securității cibernetică, Uniunea trebuie să fie capabilă să se adapteze rapid și continuu la noile evoluții în domeniu. De aceea, Centrul de competențe, Rețeaua și Comunitatea de competențe în materie de securitate cibernetică ar trebui să fie suficient de flexibile pentru a asigura viteza de răspuns necesară. Acestea ar trebui să faciliteze soluții care să ajute entitățile să își poată consolida permanent capacitatea de a-și îmbunătăți reziliența proprie și pe cea a Uniunii.** [AM 18]
- (14b) **Centrul de competențe ar trebui să aibă ca obiective stabilirea poziției de lider și a expertizei Uniunii în materie de securitate cibernetică și, cu ajutorul acestei garanții, stabilirea celor mai înalte standarde de securitate în Uniune, asigurarea protecției datelor, a sistemelor informatice, a rețelelor și a infrastructurilor critice din Uniune, crearea de noi locuri de muncă de înaltă calitate în domeniu, prevenirea exodului creierelor în rândul experților europeni în materie de securitate cibernetică către țări terțe și adăugarea valorii europene la măsurile naționale în materie de securitate cibernetică deja existente.** [AM 19]
- (15) Centrul de competențe ar trebui să dețină mai multe funcții-cheie. În primul rând, acesta ar trebui să faciliteze și să contribuie la coordonarea activității Rețelei ~~europene de competențe în materie de securitate cibernetică~~ și să promoveze Comunitatea de competențe în materie de securitate cibernetică. Centrul ar trebui să promoveze agenda

<sup>(8)</sup> 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).

Miercuri, 17 aprilie 2019

tehnologică în materie de securitate cibernetică și să **pună în comun, să partajeze și să faciliteze** accesul la expertiza acumulată în cadrul rețelei și al Comunității de competențe în materie de **securitate cibernetică, precum și la infrastructura** de securitate cibernetică. În al doilea rând, ar trebui să pună în aplicare părțile relevante din programele Europa digitală și Orizont Europa prin alocarea de granturi, în general în urma unei cereri de propuneri concurențiale. În al treilea rând, centrul de competențe ar trebui să faciliteze investițiile comune din partea Uniunii, a statelor membre și/sau a industriei, **precum și oportunitățile de formare comună și campaniile de sensibilizare, în conformitate cu programul Europa digitală pentru cetățeni și întreprinderi, pentru a se depăși deficitul de competențe. Acesta ar trebui să acorde o atenție specială capacitării IMM-urilor în domeniul securității cibernetică.** [AM 20]

- (16) Centrul de competențe ar trebui să stimuleze și să sprijine cooperarea și coordonarea **strategice și pe termen lung** a activităților Comunității de competențe în materie de securitate cibernetică, care ar implica un grup mare, deschis, **interdisciplinar** și diversificat de actori **europeni** implicați în tehnologia privind securitatea cibernetică. Această comunitate ar trebui să includă în special entități de cercetare, **inclusiv cele active în domeniul eticii în securitate cibernetică**, sectoarele furnizoare, sectoarele cererii (**inclusiv IMM-uri**), precum și sectorul public. Comunitatea de competențe în materie de securitate cibernetică ar trebui să contribuie la activitățile și la planul de lucru ale Centrului de competențe și ar trebui, de asemenea, să beneficieze de activitățile de consolidare a comunității desfășurate de Centrul de competențe și de rețea, dar nu ar trebui să beneficieze de privilegii în ceea ce privește cererile de propuneri sau procedurile de ofertare. [AM 21]
- (16a) **Centrul de competențe ar trebui să acorde sprijinul corespunzător ENISA în îndeplinirea sarcinilor acesteia, definite în Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului<sup>(9)</sup> („Legea privind securitatea cibernetică”). Prin urmare, ENISA ar trebui să ofere contribuții relevante Centrului de competențe la îndeplinirea sarcinii sale de definire a priorităților de finanțare.** [AM 22]
- (17) Pentru a răspunde nevoilor **sectorului public** și atât ale sectoarelor cererii, cât și ale sectoarelor furnizoare, sarcina Centrului de competențe de a oferi cunoștințe și asistență tehnică în materie de securitate cibernetică pentru **sectorul public** și aceste sectoare ar trebui să se refere atât la produsele, **procesele** și serviciile TIC, cât și la toate celelalte produse și ~~soluții~~ **proces** industriale și tehnologice care ar trebui să includă o componentă de securitate cibernetică. **În special, Centrul de competențe ar trebui să faciliteze implementarea unor soluții dinamice la nivelul întreprinderilor, axate pe consolidarea capacităților organizațiilor în ansamblu, inclusiv ale persoanelor, proceselor și tehnologiei, pentru a proteja în mod eficace organizațiile împotriva amenințărilor cibernetică în continuă schimbare.** [AM 23]
- (17a) **Centrul de competențe ar trebui să contribuie la utilizarea pe scară largă a unor produse și soluții de securitate cibernetică de ultimă generație, în special a celor recunoscute la nivel internațional.** [AM 24]
- (18) Având în vedere că Centrul de competențe și rețeaua ar trebui să depună eforturi pentru a realiza sinergii și **coordonare** între domeniile civile și de apărare ale securității cibernetică, proiectele finanțate prin programul Orizont Europa vor fi puse în aplicare în conformitate cu Regulamentul XXX [Regulamentul privind programul Orizont Europa], care prevede că activitățile de cercetare și inovare desfășurate în cadrul programului Orizont Europa se concentrează asupra aplicațiilor civile. [AM 25]
- (19) Pentru a asigura o colaborare structurată și durabilă, relația dintre Centrul de competențe și centrele naționale de coordonare ar trebui să se bazeze pe un acord contractual, **care ar trebui armonizat la nivelul Uniunii.** [AM 26]
- (20) Ar trebui prevăzute dispoziții adecvate pentru a garanta răspunderea și transparența Centrului de competențe și **a acelor întreprinderi care primesc finanțare.** [AM 27]
- (20a) **Punerea în aplicare a proiectelor de implementare, în special a celor privind infrastructurile și capacitățile implementate la nivel european sau în acțiuni comune de achiziții publice, poate fi împărțită în diferite etape ale punerii în aplicare, cum ar fi licitații separate pentru arhitectura hardware și software, pentru producția acestora și pentru operarea și întreținerea lor, în timp ce întreprinderile pot să participe numai la una dintre etape, fiind necesar ca beneficiarii dintr-una sau mai multe etape să îndeplinească anumite condiții în ceea ce privește dreptul de proprietate sau controlul european.** [AM 28]

<sup>(9)</sup> Regulamentul (UE) 2019/... al Parlamentului European și al Consiliului din... privind ENISA (Agenția Uniunii Europene pentru securitate cibernetică) și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentul (UE) nr. 526/2013 (Legea privind securitatea cibernetică) (JO L...) (2017/0225(COD)) .

Miercuri, 17 aprilie 2019

- (20b) *Având în vedere faptul că ENISA este agenția Uniunii dedicată securității cibernetice, Centrul de competențe ar trebui să încerce să obțină cele mai bune sinergii cu aceasta, iar Consiliul de conducere al Centrului ar trebui să consulte ENISA, dată fiind experiența acesteia în domeniul securității cibernetice, în special în ceea ce privește proiectele legate de cercetare.* [AM 29]
- (20c) *În procesul de numire a reprezentantului său în Consiliul de conducere, Parlamentul European ar trebui să includă detalii privind mandatul, inclusiv obligația de a raporta periodic Parlamentului European sau comisiilor responsabile.* [AM 30]
- (21) *Având în vedere expertiza lor în materie de securitate cibernetică și pentru a asigura sinergii maxime, Centrul Comun de Cercetare al Comisiei și Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) ar trebui să joace un rol activ în cadrul Comunității de competențe în materie de securitate cibernetică și al Consiliului consultativ pe probleme industriale și științifice. ENISA ar trebui să își îndeplinească în continuare obiectivele strategice, în special în domeniul certificării de securitate cibernetică, astfel cum sunt definite în Regulamentul (UE) 2019/XXX [Legea privind securitatea cibernetică] <sup>(10)</sup>, iar Centrul de competențe ar trebui să acționeze ca organism operațional în domeniul securității cibernetice.* [AM 31]
- (22) *În cazul în care primesc o contribuție financiară din bugetul general al Uniunii, centrele naționale de coordonare și entitățile care fac parte din Comunitatea de competențe în materie de securitate cibernetică ar trebui să aducă în atenția publicului faptul că activitățile respective sunt întreprinse în contextul prezentei inițiative.*
- (23) *Contribuția Uniunii la Centrul de competențe ar trebui să finanțeze jumătate din costurile rezultate din activitățile de înființare, administrative și de coordonare ale Centrului de competențe. Pentru a evita dubla finanțare, activitățile respective nu ar trebui să beneficieze simultan de o contribuție din alte programe ale Uniunii.*
- (24) *Consiliul de conducere al Centrului de competențe, alcătuit din reprezentanți ai statelor membre și ai Comisiei, ar trebui să traseze direcția generală de activitate a Centrului de competențe și să se asigure că acesta își îndeplinește sarcinile în conformitate cu prezentul regulament. Consiliului de conducere ar trebui să 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 Centrul de competențe, adoptarea planului de lucru și al planului strategic multianual al Centrului de competențe, care reflectă prioritățile în ceea ce privește îndeplinirea obiectivelor și a sarcinilor centrului, adoptarea regulamentului său de procedură, numirea directorului executiv și luarea deciziei cu privire la prelungirea sau încetarea mandatului directorului executiv. Pentru a beneficia de sinergii, ENISA ar trebui să fie observator permanent în consiliul de conducere și să contribuie la activitatea Centrului de competențe, inclusiv să fie consultată cu privire la planul strategic multianual, planul de lucru și lista de acțiuni selectate pentru finanțare.* [AM 32]
- (24a) *Consiliul de conducere are ca obiectiv să promoveze Centrul de competențe la nivel mondial, astfel încât acesta să își sporească atractivitatea și să devină un organism de talie mondială pentru excelență în materie de securitate cibernetică.* [AM 33]
- (25) *Pentru buna funcționare în condiții de eficacitate a Centrului de competențe, Comisia și statele membre ar trebui să se asigure că persoanele care urmează să fie numite în consiliul de conducere au nivelul adecvat de competență și experiență profesională în domeniile funcționale. Comisia și statele membre ar trebui, de asemenea, să depună eforturi pentru a limita rotația reprezentanților lor în consiliul de conducere, cu scopul de a asigura continuitatea activității acestuia și a urmări asigurarea echilibrului de gen.* [AM 34]
- (25a) *Ponderele votului Comisiei în deciziile consiliului de conducere ar trebui să fie în concordanță cu contribuția din bugetul Uniunii la Centrul de competențe, în conformitate cu responsabilitatea Comisiei de a asigura o gestionare corespunzătoare a bugetului Uniunii în interesul Uniunii, astfel cum se prevede în tratate.* [AM 35]

<sup>(10)</sup> *Regulamentul (UE) 2019/... al Parlamentului European și al Consiliului din... privind ENISA (Agenția Uniunii Europene pentru securitate cibernetică) și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentul (UE) nr. 526/2013 (Legea privind securitatea cibernetică) (JO L...) (2017/0225(COD)).*

Miercuri, 17 aprilie 2019

- (26) Pentru buna funcționare a Centrului de competențe, este necesar ca numirea directorului executiv să fie făcută **într-o manieră transparentă** pe baza meritelor și a aptitudinilor sale administrative și manageriale atestate, precum și a competenței și a experienței relevante în domeniul securității cibernetice și, de asemenea, este necesar ca directorul executiv să își ducă la îndeplinire atribuțiile în deplină independență. [AM 36]
- (27) Centrul de competențe ar trebui să aibă drept organism consultativ un Consiliu consultativ pe probleme industriale și științifice, pentru a asigura un dialog regulat **și transparent în mod corespunzător** cu sectorul privat, cu organizațiile de consumatori și cu alte părți interesate relevante. **Ar trebui totodată să furnizeze directorului executiv și consiliului de conducere consiliere independentă cu privire la dezvoltare și achiziții publice.** Consiliul consultativ pe probleme industriale și științifice ar trebui să se concentreze pe chestiunile relevante pentru părțile interesate și să le aducă în atenția consiliului de conducere al Centrului de competențe. Componenta Consiliului consultativ pe probleme industriale și științifice și sarcinile care îi revin, cum ar fi consultarea cu privire la planul de lucru, ar trebui să asigure o reprezentare suficientă a părților interesate în activitatea Centrului de competențe. **Un număr minim de locuri ar trebui alocat fiecărei categorii de părți interesate din industrie, acordând o atenție specială reprezentării IMM-urilor.** [AM 37]
- (28) Centrul de competențe **și activitățile acestuia** ar trebui să beneficieze de expertiza specifică și de reprezentarea extinsă și relevantă a părților interesate realizată prin intermediul parteneriatului public-privat contractual privind securitatea cibernetică pe durata programului Orizont 2020 **și a proiectelor-pilot din cadrul programului Orizont 2020 privind Rețeaua de competențe în materie de securitate cibernetică**, prin intermediul Consiliului său consultativ pe probleme industriale și științifice. **Centrul de competențe și Consiliul consultativ pe probleme industriale și științifice ar trebui să ia în considerare, dacă este cazul, reproducerea structurilor existente, de exemplu, sub forma unor grupuri de lucru.** [AM 38]
- (28a) **Centrul de competențe și organismele acestuia ar trebui să utilizeze experiența și contribuțiile oferite de inițiativele actuale și din trecut, cum ar fi parteneriatul public-privat contractual privind securitatea cibernetică, Organizația Europeană de Securitate Cibernetică (ECISO), precum și proiectul-pilot și acțiunea pregătitoare privind auditurile programelor informatice gratuite și cu sursă deschisă („EU FOSSA”).** [AM 39]
- (29) Centrul de competențe ar trebui să dispună de norme de prevenire, **identificare și gestionare soluționare** a conflictelor de interese **în rândul membrilor, organismelor și personalului său, precum și în rândul membrilor consiliului de conducere, ai Consiliului consultativ pe probleme industriale și științifice și ai comunității. Statele membre ar trebui să asigure prevenirea, identificarea și rezolvarea conflictelor de interese în cadrul centrelor naționale de coordonare.** De asemenea, Centrul de competențe 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<sup>(1)</sup>. Prelucrarea datelor cu caracter personal de către Centrul de competențe face obiectul Regulamentului (UE) nr. XXX/2018 al Parlamentului European și al Consiliului. Centrul de competențe ar trebui să se conformeze dispozițiilor aplicabile instituțiilor Uniunii, precum și dispozițiilor legislațiilor naționale privind gestionarea informațiilor, în special a informațiilor sensibile neclasificate și a informațiilor UE clasificate. [AM 40]
- (30) Interesele financiare ale Uniunii și ale statelor membre ar trebui să fie protejate prin măsuri proporționale pe tot parcursul ciclului de cheltuieli, inclusiv prin prevenirea, depistarea și investigarea neregulilor, prin recuperarea fondurilor pierdute, plătite în mod necuvenit sau incorect utilizate și, dacă este cazul, prin aplicarea de sancțiuni administrative și financiare în conformitate cu Regulamentul XXX (UE, Euratom) al Parlamentului European și al Consiliului<sup>(2)</sup> [Regulamentul financiar].
- (31) Centrul de competențe ar trebui să funcționeze într-un mod deschis și transparent, furnizând ~~toate informațiile relevante~~ **informații cuprinzătoare** în timp util și promovându-și activitățile, inclusiv activitățile de informare și diseminare destinate publicului larg. Regulamentul de procedură al organismelor Centrului de competențe ar trebui să fie pus la dispoziția publicului. **Acesta ar trebui să pună la dispoziția publicului și a oricărei părți interesate o listă a membrilor Comunității de competențe în materie de securitate cibernetică și ar trebui să publice declarațiile de interese întocmite de aceștia în conformitate cu articolul 42.** Regulamentul de procedură al organismelor Centrului de competențe ar trebui să fie pus la dispoziția publicului. [AM 41]

<sup>(1)</sup> 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).

<sup>(2)</sup> [a se adăuga titlul și referința JO]

Miercuri, 17 aprilie 2019

- (31a) *Se recomandă ca atât Centrul de competențe, cât și centrele naționale de coordonare să monitorizeze și să respecte standardele internaționale cât mai mult posibil, pentru a încuraja evoluția către cele mai bune practici globale.* [AM 42]
- (32) Auditorul intern al Comisiei ar trebui să exercite în cadrul Centrului de competențe aceleași competențe pe care le exercită în cadrul Comisiei.
- (33) Comisia, Centrul de competențe, Curtea de Conturi și Oficiul European de Luptă Antifraudă ar trebui să aibă acces la toate informațiile și spațiile de lucru necesare pentru efectuarea de audituri și investigații privind granturile, contractele și acordurile semnate de Centrul de competențe.
- (33a) *Competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene ar trebui să fie delegată Comisiei în ceea ce privește definirea elementelor de acord contractual dintre centrul de competență și centrele naționale de coordonare, precum și în ceea ce privește specificarea criteriilor de evaluare și de acreditare a entităților ca membre ale Comunității Competențelor în materie de securitate cibernetică. Este deosebit de important ca, în cadrul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016<sup>(13)</sup>. În special, pentru a se asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.* [AM 43]
- (34) ~~Deoarece~~ *obiectivele Obiectivele prezentului regulament, și anume consolidarea competitivității și a capacităților Uniunii în domeniul securității cibernetice, reducând dependența sa digitală prin stimularea folosirii de produse, procese și servicii create în Uniune, prin* menținerea și dezvoltarea capacităților tehnologice și industriale ale Uniunii în materie de securitate cibernetică, creșterea competitivității sectorului securității cibernetice al Uniunii și transformarea securității cibernetice într-un avantaj competitiv al altor sectoare din Uniune, nu pot fi realizate în mod satisfăcător de către statele membre din cauza faptului că resursele limitate existente sunt dispersate, precum și din cauza amplorii investițiilor necesare, ci mai degrabă, pentru a se evita duplicarea inutilă a eforturilor, contribuind la atingerea unei mase critice a investițiilor și garantând utilizarea finanțării publice în cel mai bun mod posibil, pot fi mai bine realizate la nivelul Uniunii. *În plus, numai acțiunile de la nivelul Uniunii pot asigura cel mai înalt nivel de securitate cibernetică în toate statele membre și, prin urmare, pot acoperi lacunele în materie de securitate existente în unele state membre, care creează lacune în materie de securitate la nivelul întregii Uniuni. Astfel, Uniunea poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este definit stabilit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea obiectivului respectiv,* [AM 44]

ADOPTĂ PREZENTUL REGULAMENT:

## CAPITOLUL I

### DISPOZIȚII ȘI PRINCIPII GENERALE REFERITOARE LA CENTRUL DE COMPETENȚE ȘI LA REȚEA

#### Articolul 1

##### Obiect

1. Prezentul regulament instituie Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică („Centrul de competențe”), precum și Rețeaua de centre naționale de coordonare („**Rețeaua**”) și stabilește norme pentru numirea centrelor naționale de coordonare, precum și pentru instituirea Comunității de competențe în materie de securitate cibernetică („**Comunitatea**”). *Centrul de competențe și rețeaua contribuie la reziliența generală și la familiarizarea publicului din Uniune cu amenințările la adresa securității cibernetice, ținând seama în mod corect de implicațiile sociale.* [AM 45]

<sup>(13)</sup> JO L 123, 12.5.2016, p. 1.

Miercuri, 17 aprilie 2019

2. Centrul de competențe contribuie la punerea în aplicare a părții referitoare la securitatea cibernetică din programul Europa digitală, instituit prin Regulamentul nr. XXX <sup>(14)</sup> și, în special, a acțiunilor legate de articolul 6 din Regulamentul (UE) nr. XXX [programul Europa digitală] din acesta și a programului Orizont Europa, instituit prin Regulamentul nr. XXX <sup>(15)</sup> și, în special, a secțiunii 2.2.6 din pilonul II al anexei I la Decizia nr. XXX de instituire a programului specific de punere în aplicare a programului-cadru pentru cercetare și inovare Orizont Europa [numărul de referință al programului specific].

3. Centrul de competențe își are sediul la [Bruxelles, Belgia.] [AM 46]

4. Centrul de competențe are personalitate juridică. Acesta dispune, în fiecare stat membru, de cea mai extinsă capacitate juridică acordată persoanelor juridice în temeiul legislației statului membru respectiv. În special, acesta poate să achiziționeze sau să înstrăineze bunuri mobile și imobile și să se constituie parte în proceduri judiciare. [AM 47]

## Articolul 2

### Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

- (1) ~~„securitate~~ **securitatea** cibernetică” înseamnă **toate activitățile necesare pentru** protejarea rețelelor și a sistemelor informatice, a utilizatorilor acestora și a ~~altor persoane~~ **persoanelor afectate** împotriva amenințărilor cibernetică; [AM 48]
- (1a) **„apărare cibernetică” și „dimensiuni de apărare ale securității cibernetică” înseamnă tehnologii exclusiv defensive și reactive de apărare cibernetică ce vizează protejarea infrastructurilor critice, a rețelelor militare și a sistemelor informatice, a utilizatorilor acestora și a persoanelor afectate împotriva amenințărilor cibernetică, inclusiv conștientizarea situației, detectarea amenințărilor și criminalistica digitală;** [AM 183]
- (2) **„produse și soluții de securitate cibernetică procese”** înseamnă produse, servicii sau procese TIC **comerciale sau necomerciale**, care au drept scop specific protejarea **datelor**, a rețelelor și a sistemelor informatice, a utilizatorilor acestora și a altor persoane împotriva amenințărilor **la adresa securității** cibernetică; [AM 49]
- (2a) **„amenințare cibernetică” înseamnă orice circumstanță, eveniment sau acțiune potențială care poate cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor acestora și a persoanelor afectate, sau care poate avea un alt tip de impact negativ asupra acestora;** [AM 50]
- (3) „autoritate publică” înseamnă orice guvern sau altă administrație publică, inclusiv organismele publice consultative, la nivel național, regional sau local sau orice persoană fizică sau juridică ce îndeplinește funcții administrative publice în conformitate cu **dreptul Uniunii și** legislația națională, inclusiv sarcini specifice; [AM 51]
- (4) „stat membru ~~participanț~~ **contribuitor**” înseamnă un stat membru care contribuie financiar în mod voluntar la costurile administrative și operaționale ale Centrului de competențe; [AM 52]
- (4a) **„centre europene de inovare digitală” înseamnă o entitate juridică, astfel cum este definită în Regulamentul (UE) 2019/XXX al Parlamentului European și al Consiliului <sup>(16)</sup>.** [AM 53]

## Articolul 3

### Misiunea centrului și a rețelei

1. Centrul de competențe și rețeaua ajută Uniunea:

- (a) ~~să mențină și să dezvolte capacitățile tehnologice și industriale~~ **să și dezvolte capacitățile tehnologice, industriale, societale, academice și de expertiză în cercetare** în materie de securitate cibernetică necesare pentru crearea unei piețe unice digitale sigure **și pentru a avansa protecția datelor cetățenilor Uniunii, ale întreprinderilor și ale administrațiilor publice;** [AM 54]

<sup>(14)</sup> A se adăuga titlul complet și referința JO.

<sup>(15)</sup> A se adăuga titlul complet și referința JO.

<sup>(16)</sup> **Regulamentul (UE) 2019/XXX al Parlamentului European și al Consiliului din... de instituire a programului Europa digitală pentru perioada 2021-2027 (JO L ...) (2018/0227(COD)).**

Miercuri, 17 aprilie 2019

- (aa) să crească reziliența și fiabilitatea infrastructurii de rețele și de sisteme informatice din Uniune, mai ales a celei critice, a internetului și a echipamentelor hardware și software utilizate în mod obișnuit; [AM 55]
- (b) să sporească competitivitatea sectorului securității cibernetice al Uniunii și să transforme securitatea cibernetică într-un avantaj competitiv al altor sectoare ale Uniunii; [AM 56 Nu privește versiunea în limba română]
- (ba) să sensibilizeze publicul cu privire la amenințările la adresa securității cibernetice și la implicațiile și preocupările societale și etice legate de aceasta în Uniune, și totodată să reducă decalajul de competențe în domeniu. [AM 57]
- (bb) să vizeze o poziție de lider a Uniunii în domeniul securității cibernetice și să asigure cele mai înalte standarde de securitate cibernetică la nivelul Uniunii; [AM 58]
- (bc) să consolideze competitivitatea și capacitățile Uniunii, reducând în același timp dependența sa digitală prin creșterea gradului de utilizare a produselor, proceselor și serviciilor de securitate cibernetică dezvoltate în Uniune; [AM 59]
- (bd) să consolideze încrederea cetățenilor, a consumatorilor și a întreprinderilor în lumea digitală și, astfel, să contribuie la realizarea obiectivelor Strategiei privind piața unică digitală. [AM 60]
2. Centrul de competențe își îndeplinește sarcinile, după caz, în colaborare cu Rețeaua de centre naționale de coordonare și cu o Comunitate de competențe în materie de securitate cibernetică.

#### Articolul 4

##### Obiectivele și misiunile centrului

Centrul de competențe are următoarele obiective și sarcini conexe:

1. ~~crearea, gestionarea și~~ facilitarea și contribuția la coordonarea activității Rețelei de centre naționale de coordonare (denumită în continuare „rețeaua”) menționate la articolul 6 și a Comunității de competențe în materie de securitate cibernetică menționate la articolul 8; [AM 61]
2. ~~contribuția la punerea~~ **coordonarea punerii** în aplicare a părții referitoare la securitatea cibernetică din programul Europa digitală, instituit prin Regulamentul nr. XXX <sup>(17)</sup> și, în special, a acțiunilor legate de articolul 6 din Regulamentul (UE) nr. XXX [programul Europa digitală] și a părții referitoare la securitatea cibernetică din programul Orizont Europa, instituit prin Regulamentul nr. XXX <sup>(18)</sup> și, în special, a secțiunii 2.2.6 din pilonul II al anexei I la Decizia nr. XXX de instituire a programului specific de punere în aplicare a programului-cadru pentru cercetare și inovare Orizont Europa [numărul de referință al programului specific] și din alte programe ale Uniunii, atunci când acest lucru este prevăzut în actele juridice ale Uniunii și contribuția la punerea în aplicare a acțiunilor finanțate prin Fondul european de apărare instituit prin Regulamentul (UE) 2019/XXX; [AM 62]
3. consolidarea **rezilienței**, a capacităților, a cunoștințelor și a infrastructurilor în materie de securitate cibernetică în slujba **societății**, a sectoarelor industriale, a sectorului public și a comunităților de cercetare, prin îndeplinirea următoarelor sarcini, **având în vedere infrastructurile industriale și de cercetare de ultimă generație în materie de securitate cibernetică și serviciile conexe**: [AM 63]
  - (a) **având în vedere infrastructurile industriale și de cercetare de ultimă generație în materie de securitate cibernetică și serviciile conexe**, achiziționarea, modernizarea, utilizarea și punerea la dispoziție a unor astfel de infrastructuri și servicii conexe **resurselor Centrului de competențe și a serviciilor conexe într-un mod echitabil, deschis și transparent** pentru o gamă largă de utilizatori din sector din întreaga Uniune, inclusiv **îndeosebi IMM-uri, și din sectorul public și comunitatea științifică și de cercetare**; [AM 64]

<sup>(17)</sup> [a se adăuga titlul complet și referința JO]

<sup>(18)</sup> [a se adăuga titlul complet și referința JO]

Miercuri, 17 aprilie 2019

- (b) ~~având în vedere infrastructurile industriale și de cercetare de ultimă generație în materie de securitate cibernetică și serviciile conexe, oferirea de sprijin, inclusiv de sprijin financiar, altor entități pentru achiziționarea, modernizarea, utilizarea și punerea la dispoziție a unor astfel de infrastructuri~~ **resurse și servicii conexe** pentru o gamă largă de utilizatori din sector din întreaga Uniune, ~~inclusiv îndeosebi IMM-uri, și din~~ **sectorul public și comunitatea științifică și de cercetare;** [AM 65]
- (ba) **furnizarea de sprijin financiar și asistență tehnică pentru întreprinderile nou-înființate, IMM-uri, microîntreprinderi, asociații și experți individuali și proiecte tehnologice civice din domeniul securității cibernetică;** [AM 66]
- (bb) **finanțarea de audituri ale codurilor de securitate pentru software și îmbunătățiri conexe pentru proiectele care vizează dezvoltarea de software gratuit și cu sursă deschisă care este utilizat în mod obișnuit pentru infrastructură, produse și procese;** [AM 67]
- (c) ~~furnizarea~~ **facilitarea schimbului** de cunoștințe în materie de securitate cibernetică și de asistență tehnică, **printre altele, pentru societatea civilă, pentru sector, pentru autoritățile publice și pentru autoritățile publice comunitatea academică și de cercetare,** în special prin sprijinirea acțiunilor menite să faciliteze accesul la expertiza disponibilă în cadrul rețelei și al Comunității de competențe în materie de securitate cibernetică, **cu scopul îmbunătățirii cibernetică a Uniunii;** [AM 68]
- (ca) **promovarea principiului „securității de la stadiul conceperii” în procesul de dezvoltare, menținere, utilizare și actualizare a infrastructurilor, a produselor și a serviciilor, în special prin sprijinirea metodelor de dezvoltare securizate de ultimă generație, a testării adecvate a securității și a auditurilor care vizează securitatea, inclusiv angajamentul producătorului sau al furnizorului de a pune la dispoziție actualizări care să remedieze, fără întârziere, vulnerabilitățile sau amenințările noi, pe toată durata de viață estimată a produsului și după încheierea acesteia, sau permiterea ca un terț să creeze și să furnizeze astfel de actualizări;** [AM 69]
- (cb) **acordarea de asistență pentru politicile privind contribuțiile la codul sursă și dezvoltarea acestora, în special pentru autoritățile publice, în cazurile în care sunt utilizate proiecte informatice gratuite și cu sursă deschisă;** [AM 70]
- (cc) **reunirea părților interesate din sector, a sindicatelor, a mediului academic, a organizațiilor de cercetare și a entităților publice, pentru a asigura cooperarea pe termen lung cu privire la dezvoltarea și punerea în aplicare a produselor și proceselor de securitate cibernetică, inclusiv cu privire la punerea în comun și partajarea resurselor și a informațiilor referitoare la astfel de produse și procese, dacă este cazul;** [AM 71]
4. contribuția la dezvoltarea pe scară largă a unor produse și ~~soluții~~ **proceselor durabile** de securitate cibernetică de ultimă generație în întreaga ~~economie~~ **Uniune, prin îndeplinirea următoarelor sarcini:** [AM 72]
- (a) stimularea cercetării și dezvoltării legate de produsele și soluțiile de securitate cibernetică ale Uniunii și a **proceselor globale de-a lungul întregului ciclu de inovare, și a** adoptării lor, **printre altele** de către autoritățile publice și sectoarele ~~utilizatoare~~ **, industrie și piață;** [AM 73]
- (b) sprijinirea autorităților publice, a sectoarelor cererii și a altor utilizatori în **îmbunătățirea rezilienței prin** adoptarea și integrarea ~~celor mai recente soluții în materie de securitate cibernetică~~ **produselor și proceselor de securitate cibernetică de ultimă generație;** [AM 74]
- (c) sprijinirea, în special, a autorităților publice în ceea ce privește organizarea achizițiilor lor publice sau efectuarea de achiziții publice de produse și ~~soluții~~ **proceselor** de securitate cibernetică de ultimă generație în numele autorităților **publice, inclusiv prin furnizarea de sprijin pentru achiziții publice durabile, pentru a îmbunătăți siguranța și beneficiile rezultate din investițiile publice;** [AM 75]
- (d) furnizarea de sprijin financiar și de asistență tehnică pentru întreprinderi nou-înființate și ~~,~~ **IMM-uri, microîntreprinderi și experți individuali** din domeniul securității cibernetică, **precum și pentru proiecte care vizează dezvoltarea de software gratuit și cu sursă deschisă și proiecte tehnologice civice, pentru a crește expertiza în domeniu,** pentru a se conecta la piețe potențiale, **pentru a valorifica oportunități de dezvoltare și pentru a atrage investiții;** [AM 76]

Miercuri, 17 aprilie 2019

5. îmbunătățirea înțelegerii securității cibernetice și , contribuirea la reducerea lacunelor în materie **de competențe și consolidarea nivelului** de competențe din Uniune în ceea ce privește securitatea cibernetică, prin îndeplinirea următoarelor sarcini: [AM 77]
- (-a) **sprijinirea, dacă este cazul, a realizării obiectivului specific 4 privind competențele digitale avansate al programului Europa digitală, în cooperare cu centrele europene de inovare digitală;** [AM 78]
- (a) **sprijinirea dezvoltării în continuare, punerea în comun și partajarea competențelor și abilităților în materie de securitate cibernetică acolo unde este cazul, împreună la toate nivelurile educaționale relevante, sprijinirea obiectivului de realizare a echilibrului de gen, facilitarea unui nivel comun ridicat de cunoștințe în materie de securitate cibernetică și contribuția la reziliența utilizatorilor și a infrastructurilor în întreaga Uniune, în cooperare cu Rețeaua și, după caz, alinierea cu agențiile și organismele relevante ale UE, inclusiv cu ENISA;** [AM 79]
6. contribuția la consolidarea cercetării și dezvoltării în domeniul securității cibernetice în Uniune prin:
- (a) furnizarea de sprijin financiar pentru eforturile de cercetare în materie de securitate cibernetică bazate pe ~~o~~ **agendă industrială, tehnologică un plan industrial, tehnologic** și de cercetare comună multianuală strategică, evaluată și îmbunătățită în mod continuu, **menționat la articolul 13;** [AM 80]
- (b) **sprijinirea proiectelor de cercetare și demonstrative la scară largă în capacitățile tehnologice de securitate cibernetică de generație următoare, în colaborare cu industria, cu instituțiile academice și de cercetare, cu sectorul public și cu autoritățile, inclusiv cu rețeaua și cu comunitatea;** [AM 81]
- (ba) **asigurarea respectării drepturilor fundamentale și a comportamentului etic în proiectele de cercetare în domeniul securității cibernetice sprijinite de Centrul de competențe;** [AM 82]
- (bb) **rapoartele de monitorizare a vulnerabilităților descoperite de comunitate și care facilitează comunicarea vulnerabilităților, evoluția tiparelor, a soluțiilor și a soluțiilor și distribuția acestora;** [AM 83]
- (bc) **monitorizarea rezultatelor cercetării legate de algoritmi de autoînvățare utilizați în activități cibernetice răuvoitoare, în colaborare cu ENISA și prin sprijinirea punerii în aplicare a Directivei (UE) 2016/1148;** [AM 84]
- (bd) **sprijinirea cercetării în materie de securitate cibernetică;** [AM 85]
- (be) **sprijinirea cercetării și dezvoltării de produse și procese, care să poată fi studiate, partajate și valorificate în mod liber, în special în materie de hardware și software verificate și verificabile, în strânsă cooperare cu sectorul, cu rețeaua și cu comunitatea;** [AM 86]
- (c) **sprijinirea cercetării și a inovării pentru standardizarea tehnologiei în materie de securitate cibernetică inovării în materie de standardizare formală și non-formală și de certificare a tehnologiilor de securitate cibernetică, asigurând legătura cu activitatea existentă și, după caz, în strânsă cooperare cu organizațiile europene de standardizare, cu organismele de certificare și cu ENISA;** [AM 87]
- (ca) **furnizare de sprijin special IMM-urilor prin facilitarea accesului acestora la cunoștințe și la formare, printr-un acces adaptat la rezultatele cercetării și dezvoltării, consolidat de către Centrul de competențe și de către rețea, în vederea creșterii competitivității;** [AM 88]
7. consolidarea cooperării între domeniile civil și de apărare în ceea ce privește tehnologiile și aplicațiile cu dublă utilizare în materie de securitate cibernetică, prin îndeplinirea următoarelor sarcini, **care se limitează strict la tehnologia, aplicațiile și serviciile reactive și defensive de apărare cibernetică;** [AM 184]

Miercuri, 17 aprilie 2019

- (a) sprijinirea statelor membre și a părților interesate din sectorul industrial și din domeniul cercetării în ceea ce privește cercetarea, dezvoltarea și implementarea;
  - (b) contribuția la cooperarea dintre statele membre prin sprijinirea educației, a formării și a exercițiilor;
  - (c) reunirea părților interesate, pentru a promova sinergiile dintre cercetarea și piețele în materie de securitate cibernetică civile și de apărare;
8. consolidarea sinergiilor dintre dimensiunile civile și cele de apărare ale securității cibernetice în legătură cu Fondul european de apărare, prin îndeplinirea următoarelor sarcini, **care se limitează strict la tehnologia, aplicațiile și serviciile reactive și defensive de apărare cibernetică**: [AM 185]
- (a) furnizarea de consiliere, punerea în comun a expertizei și facilitarea colaborării între părțile interesate relevante;
  - (b) gestionarea de proiecte multinaționale în domeniul apărării cibernetice, atunci când statele membre solicită acest lucru, acționând astfel în calitate de manager de proiect în sensul Regulamentului XXX [Regulamentul de instituire a Fondului european de apărare];
- (ba) sprijinirea și consilierea Comisiei în ceea ce privește punerea în aplicare a Regulamentului (UE) 2019/XXX [reformare a Regulamentului (CE) nr. 428/2009 în conformitate cu propunerea COM(2016)0616].** [AM 89]
- 8a. contribuirea la eforturile Uniunii de a intensifica cooperarea internațională în ceea ce privește securitatea cibernetică prin:**
- (a) facilitarea participării Centrului de competență în cadrul conferințelor internaționale și al organizațiilor guvernamentale, precum și contribuția la organizațiile internaționale de standardizare;**
  - (b) cooperarea cu țări terțe și organizații internaționale în cadre relevante de cooperare internațională.** [AM 90]

## Articolul 5

Investiții în infrastructuri, capacități, produse sau ~~soluții~~ **procese** și utilizarea acestora [AM 91]

1. În cazul în care Centrul de competențe oferă finanțare pentru infrastructuri, capacități, produse sau ~~soluții~~ **procese** în conformitate cu articolul 4 alineatele (3) și (4), sub formă **de achiziție publică**, de grant sau de premiu, planul de lucru al Centrului de competențe poate preciza, în special: [AM 92]
- (a) normele **specifice** care reglementează exploatarea unei infrastructuri sau a unei capacități, inclusiv, după caz, încredințarea acestei sarcini unei entități-gazdă pe baza unor criterii definite de Centrul de competențe; [AM 93]
  - (b) normele care reglementează accesul la o infrastructură sau la o capacitate și utilizarea acesteia;
- (ba) normele specifice care reglementează diferite etape ale punerii în aplicare;** [AM 94]
- (bb) faptul că, drept urmare a contribuției Uniunii, accesul este cât mai deschis posibil și restrâns doar cât este necesar, iar reutilizarea este posibilă.** [AM 95]
2. Centrul de competențe poate fi responsabil de executarea generală a acțiunilor comune relevante de achiziții publice, inclusiv a achizițiilor înainte de comercializare în numele membrilor rețelei, ~~al membrilor Comunității de competențe în materie de securitate cibernetică sau al altor părți terțe care reprezintă utilizatorii produselor și soluțiilor de securitate cibernetică.~~ În acest scop, Centrul de competențe poate fi asistat de unul sau mai multe centre naționale de coordonare sau de către membri ai Comunității de competențe în materie de securitate cibernetică **sau ai centrelor europene de inovare digitală.** [AM 96]

## Articolul 6

Desemnarea centrelor naționale de coordonare

**-1. Un centru național de coordonare unic este instituit în fiecare stat membru.** [AM 97]

1. Până la [data], fiecare stat membru desemnează entitatea care acționează în calitate de centru național de coordonare în sensul prezentului regulament și o notifică Comisiei.

Miercuri, 17 aprilie 2019

2. Pe baza unei evaluări privind respectarea de către această entitate a criteriilor prevăzute la alineatul (4), Comisia emite o decizie în termen de 6 luni de la desemnarea transmisă de statul membru, prin care acreditează entitatea ca centru național de coordonare sau respinge desemnarea. Lista centrelor naționale de coordonare este publicată de către Comisie.
  3. Statele membre pot, în orice moment, să desemneze o nouă entitate în calitate de centru național de coordonare în sensul prezentului regulament. Alineatele (1) și (2) se aplică desemnării oricărei noi entități.
  4. Centrul național de coordonare desemnat are capacitatea de a sprijini Centrul de competențe și rețeaua în îndeplinirea misiunii lor prevăzute la articolul 3 din prezentul regulament. Centrele naționale de coordonare dețin sau au acces direct la expertiza tehnologică în materie de securitate cibernetică și sunt în măsură să interacționeze și să se coordoneze în mod eficiente cu industria, cu sectorul public și , cu comunitatea **academică și de cercetare și cu cetățenii. Comisia publică orientări care detaliază în mod suplimentar procedura de evaluare și care explică aplicarea criteriilor.** [AM 98]
  5. Relația dintre Centrul de competențe și centrele naționale de coordonare se bazează pe un acord contractual **standard** semnat între Centrul de competențe și fiecare dintre centrele naționale de coordonare. Acordul ~~prevede~~ **cuprinde același set de condiții generale armonizate care prevăd** norme care reglementează relația și repartizarea sarcinilor între Centrul de competențe și fiecare centru național de coordonare, **precum și condiții speciale, adaptate la centrul național de coordonare în cauză.** [AM 99]
- 5a. Comisia adoptă acte delegate în conformitate cu articolul 45a pentru a completa prezentul regulament, prin stabilirea condițiilor generale armonizate ale acordurilor contractuale menționate la alineatul (5) din prezentul articol, inclusiv formatul acestora.** [AM 100]
6. Rețeaua de centre naționale de coordonare este formată din toate centrele naționale de coordonare desemnate de statele membre.

#### Articolul 7

##### Sarcinile centrelor naționale de coordonare

1. Centrele naționale de coordonare au următoarele sarcini:
  - (a) sprijinirea Centrului de competențe în realizarea obiectivelor sale și, în special, în **instituirea și** coordonarea Comunității de competențe în materie de securitate cibernetică; [AM 101]
  - (b) **promovarea, încurajarea și** facilitarea participării **societății civile, a** industriei, **în special a întreprinderilor nou-înființate și a IMM-urilor, a comunității academice și de cercetare** și a altor actori la nivel de stat membru în cadrul proiectelor transfrontaliere; [AM 102]
  - (ba) **în cooperare cu alte entități cu sarcini similare, care funcționează ca un ghișeu unic pentru produsele și procesele de securitate cibernetică finanțate prin alte programe ale Uniunii, cum ar fi InvestEU sau prin programul privind piața unică, în special pentru IMM-uri;** [AM 103]
  - (c) contribuția, împreună cu Centrul de competențe, la identificarea și abordarea provocărilor ~~industriale~~ în materie de securitate cibernetică specifice sectorului; [AM 104]
  - (ca) **cooperarea strânsă cu organizațiile de standardizare naționale pentru a promova adoptarea standardelor existente și pentru a implica toate părțile interesate relevante, în special IMM-urile, în stabilirea de standarde noi;** [AM 105]
  - (d) îndeplinirea rolului de punct de contact la nivel național pentru Comunitatea de competențe în materie de securitate cibernetică și pentru Centrul de competențe;
  - (e) stabilirea de sinergie cu activitățile relevante la nivel național și , regional și local; [AM 106]

Miercuri, 17 aprilie 2019

- (f) punerea în aplicare a acțiunilor specifice pentru care au fost acordate granturi de către Centrul de competențe, inclusiv prin furnizarea de sprijin financiar unor terți în conformitate cu articolul 204 din Regulamentul XXX [noul Regulament financiar] în condițiile specificate în acordurile de grant în cauză;
- (fa) promovarea și diseminarea unor programe de învățământ comune minime în domeniul securității cibernetice, în cooperare cu organismele relevante din statele membre; [AM 107]**
- (g) promovarea și diseminarea rezultatelor relevante ale activității rețelei, ale Comunității de competențe în materie de securitate cibernetică și ale Centrului de competențe la nivel național ~~sau~~, regional **sau local**; [AM 108]
- (h) evaluarea cererilor de aderare la Comunitatea de competențe în materie de securitate cibernetică primite din partea entităților **și a persoanelor fizice** stabilite în același stat membru ca centrul de coordonare. [AM 109]
2. În sensul literei (f), sprijinul financiar pentru terți poate fi furnizat în oricare dintre formele specificate la articolul 125 din Regulamentul XXX [noul Regulament financiar], inclusiv sub formă de sume forfetare.
3. Centrele naționale de coordonare pot primi un grant din partea Uniunii în conformitate cu articolul 195 litera (d) din Regulamentul XXX [noul Regulament financiar] în legătură cu îndeplinirea sarcinilor prevăzute în prezentul articol.
4. Centrele naționale de coordonare cooperează, după caz, prin intermediul rețelei **și cu centrele europene de inovare digitală relevante** în scopul îndeplinirii sarcinilor menționate la alineatul (1) ~~literele (a), (b), (c), (e) și (g)~~. [AM 110]

## Articolul 8

## Comunitatea de competențe în materie de securitate cibernetică

1. Comunitatea de competențe în materie de securitate cibernetică contribuie la misiunea Centrului de competențe, astfel cum se prevede la articolul 3, ~~și~~ consolidează, **pune în comun** și diseminează expertiza în materie de securitate cibernetică în întreaga Uniune **și furnizează expertiză tehnică**. [AM 111]
2. Comunitatea de competențe în materie de securitate cibernetică este formată din ~~organizații de cercetare industriale, academice și non-profit,~~ **societatea civilă, sectorul industrial care reprezintă cererea și oferta, inclusiv IMM-urile, comunitatea academică și de cercetare, asociații de utilizatori, experți individuali, organizații europene de standardizare relevante**, precum și din **alte** asociații și entități publice și alte entități care se ocupă de chestiuni operaționale și tehnice **în domeniul securității cibernetice**. Aceasta reunește principalele părți interesate în ceea ce privește capacitățile tehnologice și ~~industriale în materie de securitate cibernetică din Uniune, implicând~~, **industriale, academice și de cercetare, precum și capacitățile și capabilitățile societale din Uniune și implică** centrele naționale de coordonare, **centrele europene de inovare digitală**, precum și instituțiile și organismele Uniunii cu expertiză relevantă, **astfel cum se menționează la articolul 10 din prezentul regulament**. [AM 112]
3. Numai entitățile **și persoanele fizice** stabilite, **respectiv rezidente pe teritoriul Uniunii**, în ~~Uniune~~ **Spațiul Economic European (SEE) sau în țările membre ale Asociației Europene a Liberului Schimb (AELS)** pot fi acreditate ca membri ai Comunității de competențe în materie de securitate cibernetică. ~~Acestea~~ **Solicitanții** trebuie să demonstreze că **pot furniza** expertiză în materie de securitate cibernetică în ceea ce privește cel puțin unul dintre următoarele domenii: [AM 113]
- (a) **academic sau de cercetare**; [AM 114]
- (b) dezvoltare industrială;
- (c) formare și educație;
- (ca) etică**; [AM 115]
- (cb) standardizare formală și tehnică și specificații formale și tehnice**; [AM 116]

Miercuri, 17 aprilie 2019

4. Centrul de competență acreditează entități instituite în temeiul dreptului național **sau persoane fizice** în calitate de membre ale Comunității de competențe în materie de securitate cibernetică în urma unei evaluări **armonizate** efectuate de Centrul național de **competențe, de centrul național de** coordonare al statului membru în care este stabilită entitatea **sau în care persoana fizică este rezidentă**, prin care se verifică îndeplinirea de către această entitate a criteriilor prevăzute la alineatul (3). O acreditare nu este limitată în timp, dar poate fi revocată de către Centrul de competențe în orice moment dacă acesta sau centrul național de coordonare consideră că entitatea **sau persoana fizică** nu îndeplinește criteriile prevăzute la alineatul (3) sau intră sub incidența dispozițiilor relevante prevăzute la articolul 136 din Regulamentul XXX [noul Regulament financiar]. **Centrele naționale de coordonare ale statelor membre urmăresc asigurarea unei reprezentări echilibrate a părților interesate în cadrul comunității, încurajând în mod activ participarea categoriilor și a grupurilor de persoane fizice subreprezentate, în special IMM-uri.** [AM 117]

**4a. Comisia adoptă acte delegate în conformitate cu articolul 45a pentru a completa prezentul regulament prin detalierea criteriilor prevăzute la alineatul (3) din prezentul articol pe baza cărora sunt selectați solicitanții, precum și a procedurilor de evaluare și de acreditare a entităților care îndeplinesc criteriile menționate la alineatul (4) din prezentul articol.** [AM 118]

5. Centrul de competențe acreditează organisme, agenții și oficii relevante ale Uniunii în calitate de membri ai Comunității de competențe în materie de securitate cibernetică după ce a evaluat dacă entitatea în cauză îndeplinește criteriile prevăzute la alineatul (3). O acreditare nu este limitată în timp, dar poate fi revocată de către Centrul de competențe în orice moment în cazul în care consideră că entitatea nu îndeplinește criteriile prevăzute la alineatul (3) sau intră sub incidența dispozițiilor relevante prevăzute la articolul 136 din Regulamentul XXX [noul Regulament financiar].

6. Reprezentanții Comisiei pot participa la activitatea comunității.

#### Articolul 9

Sarcinile membrilor Comunității de competențe în materie de securitate cibernetică

Membrii Comunității de competențe în materie de securitate cibernetică:

- (1) sprijină Centrul de competențe în ceea ce privește îndeplinirea misiunii și a obiectivelor prevăzute la articolele 3 și 4 și, în acest scop, colaborează îndeaproape cu Centrul de competențe și cu centrele naționale de coordonare relevante;
  - (2) participă la activitățile promovate de Centrul de competențe și de centrele naționale de coordonare;
  - (3) după caz, participă la grupurile de lucru instituite de consiliul de conducere al Centrului de competențe în vederea desfășurării unor activități specifice, astfel cum se prevede în planul de activitate al Centrului de competențe;
  - (4) după caz, sprijină Centrul de competențe și centrele naționale de coordonare în promovarea proiectelor specifice;
  - (5) promovează și difuzează rezultatele relevante ale activităților și proiectelor desfășurate în cadrul comunității;
- (5a) sprijină centrul de competențe prin raportarea și divulgarea vulnerabilităților, contribuind la atenuarea acestora și oferind consiliere cu privire la modalitățile de reducere a acestor vulnerabilități, inclusiv prin intermediul certificării în cadrul sistemelor adoptate în conformitate cu Regulamentul (UE) 2019/XXX [Legea privind securitatea cibernetică].** [AM 119]

#### Articolul 10

Cooperarea Centrului de competențe cu instituțiile, organele, oficiile și agențiile Uniunii

1. **Pentru a asigura coerența și complementaritatea**, Centrul de competențe cooperează cu instituțiile, organele, oficiile și agențiile relevante ale Uniunii, inclusiv cu ~~Agencia Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor~~ **ENISA**, cu Centrul de răspuns la incidente de securitate cibernetică (CERT-UE), cu Serviciul European de Acțiune Externă, cu Centrul Comun de Cercetare al Comisiei, cu Agenția Executivă pentru Cercetare, cu Agenția Executivă pentru Inovare și Rețele, cu **centrele europene de inovare digitală relevante**, cu Centrul european de combatere a criminalității informatice din cadrul Europol, precum și cu Agenția Europeană de Apărare, **în ceea ce privește proiectele, serviciile și competențele cu dublă utilizare.** [AM 120]

Miercuri, 17 aprilie 2019

2. O astfel de cooperare are loc în cadrul acordurilor de lucru. Aceste acorduri sunt ~~supuse aprobării prealabile~~ **adoptate de Consiliul de conducere cu aprobarea prealabilă** a Comisiei. [AM 121]

## CAPITOLUL II

## ORGANIZAREA CENTRULUI DE COMPETENȚE

## Articolul 11

## Componență și structură

1. Membrii Centrului de competențe sunt Uniunea, reprezentată de Comisie, și statele membre.
2. Structura Centrului de competențe cuprinde:
  - (a) un consiliu de conducere, care exercită sarcinile prevăzute la articolul 13;
  - (b) un director executiv, care exercită sarcinile prevăzute la articolul 16;
  - (c) un Consiliu consultativ pe probleme industriale și științifice, care exercită funcțiile prevăzute la articolul 20.

## SECȚIUNEA I

## CONSILIUL DE CONDUCERE

## Articolul 12

## Componența consiliului de conducere

1. Consiliul de conducere este alcătuit ~~dintr-un~~ **din câte un** reprezentant al fiecărui stat membru, **un reprezentant desemnat de Parlamentul European în calitate de observator și unei patru** reprezentanți ai Comisiei, în numele Uniunii, **cu scopul de a obține un echilibru de gen în rândul membrilor consiliului de administrație și al supleanților acestora.** [AM 122]
2. Fiecare membru al consiliului de conducere are un supleant care îl reprezintă în absența sa.
3. Membrii consiliului de conducere și supleanții acestora sunt numiți în funcție de cunoștințele lor în domeniul ~~tehnologiei~~ **securității cibernetice**, precum și în funcție de competențele lor manageriale, administrative și bugetare relevante. Comisia și statele membre depun eforturi pentru a limita rotația reprezentanților lor în cadrul consiliului de conducere, cu scopul de a asigura continuitatea activității acestuia. Comisia și statele membre urmăresc realizarea unei reprezentări echilibrate a bărbaților și femeilor în consiliul de conducere. [AM 123]
4. Durata mandatului membrilor consiliului de conducere și al membrilor supleanți este de patru ani. Acest mandat se poate reînnoi.
5. Membrii consiliului de conducere acționează în interesul Centrului de competențe, într-un mod independent și transparent, pentru a îndeplini obiectivele și a realiza misiunea acestuia, asigurându-i identitatea, autonomia și coerența.
6. ~~Comisia~~ **Consiliul de conducere** poate invita observatori, inclusiv reprezentanți ai unor organisme, officii și agenții relevante ale Uniunii, **precum și membri ai comunității**, să participe la reuniunile consiliului de conducere, dacă este cazul. [AM 124]
7. ~~Agencia Europeană pentru Securitatea Rețelelor și a Informațiilor (ENISA) este observator permanent~~ **ENISA și Consiliul consultativ pe probleme industriale și științifice sunt observatori permanenți** în consiliul de conducere, **cu rol consultativ, dar fără drepturi de vot. Consiliul de conducere acordă atenție maximă opiniilor exprimate de observatorii permanenți.** [AM 125]

Miercuri, 17 aprilie 2019

Articolul 13

Sarcinile consiliului de conducere

1. Consiliul de conducere poartă responsabilitatea generală pentru orientarea strategică și operațiunile Centrului de competențe și supraveghează punerea în aplicare a activităților acestuia.
2. Consiliul de conducere își adoptă propriul regulament de procedură. Acest regulament include proceduri specifice pentru identificarea și evitarea conflictelor de interese și pentru asigurarea confidențialității oricăror informații sensibile.
3. Consiliul de conducere ia deciziile strategice necesare, în special:
  - (a) adoptă un plan strategic multianual, care conține o declarație privind prioritățile majore și inițiativele planificate ale Centrului de competențe, inclusiv o estimare a nevoilor și a surselor de finanțare, **ținând seama de avizul ENISA; [AM 126]**
  - (b) adoptă planul de lucru al Centrului de competențe, conturile anuale, bilanțul și raportul anual de activitate, pe baza unei propuneri din partea directorului executiv, **ținând seama de avizul ENISA; [AM 127]**
  - (c) adoptă normele financiare specifice ale Centrului de competențe, în conformitate cu [articolul 70 din RF];
  - (d) adoptă o procedură de numire a directorului executiv;
  - (e) adoptă ~~criteriile și~~ procedurile de evaluare și de acreditare a entităților în calitate de membri ai Comunității ~~de competențe în materie de securitate cibernetică~~; **[AM 128]**
  - (ea) adoptă acordurile de lucru menționate la articolul 10 alineatul (2); [AM 129]**
  - (f) desemnează directorul executiv, îl revocă din funcție, îi prelungeste mandatul, îi oferă orientări și îi monitorizează activitatea și numește contabilul;
  - (g) adoptă bugetul anual al Centrului de competențe, inclusiv schema de personal aferentă, indicând numărul de posturi temporare în funcție de grupa de funcții, de grad și de numărul membrilor personalului contractual, precum și al experților naționali detașați, exprimat în echivalent normă întreagă;
  - (ga) adoptă norme de transparență pentru Centrul de competențe; [AM 130]**
  - (h) adoptă norme privind conflictele de interese;
  - (i) instituie grupuri de lucru cu membrii Comunității ~~de competențe în materie de securitate cibernetică~~, **ținând seama de opiniile observatorilor permanenți; [AM 131]**
  - (j) numește membrii Consiliului consultativ pe probleme industriale și științifice;
  - (k) instituie o funcție de audit intern în conformitate cu Regulamentul delegat (UE) nr. 1271/2013 al Comisiei <sup>(19)</sup>;
  - (l) promovează **cooperarea dintre** Centrul de competențe ~~la nivel mondial, astfel încât acesta să își sporească atractivitatea și să devină un organism de talie mondială pentru excelență în materie de securitate cibernetică și actorii globali~~; **[AM 132]**
  - (m) stabilește politica de comunicare a Centrului de competențe, la recomandarea directorului executiv;
  - (n) este responsabil cu monitorizarea acțiunilor adecvate întreprinse ca urmare a concluziilor evaluărilor retrospective;
  - (o) după caz, stabilește norme de punere în aplicare a Statutului personalului și a Regimului aplicabil celorlalți agenți în conformitate cu articolul 31 alineatul (3);
  - (p) după caz, stabilește norme privind detașarea experților naționali la centrul de competențe și recurgerea la stagiați, în conformitate cu articolul 32 alineatul (2);

<sup>(19)</sup> 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).

Miercuri, 17 aprilie 2019

- (q) adoptă de norme de securitate pentru Centrul de competențe;
- (r) adoptă o strategie de combatere a fraudei **și a corupției**, care să fie proporțională cu riscurile de fraudă **și de corupție**, ținând seama de analiza cost-beneficiu a măsurilor care ar urma să fie puse în aplicare, **și adoptă, de asemenea, măsuri cuprinzătoare de protecție pentru persoanele care raportează încălcări ale dreptului Uniunii, în conformitate cu legislația aplicabilă a Uniunii**; [AM 133]
- (s) adoptă ~~metodologia~~ **o definiție extinsă a contribuțiilor financiare din partea statelor membre și o metodologie** de calcul al ~~contribuției financiare~~ **valorii contribuțiilor voluntare** din partea statelor membre, **care pot fi considerate contribuții financiare în conformitate cu definiția respectivă, un astfel de calcul fiind efectuat la finalul fiecărui exercițiu financiar**. [AM 134]
- (t) este responsabil cu îndeplinirea oricărei sarcini care nu a fost alocată în mod specific unui anumit organism al Centrului de competențe; poate atribui astfel de sarcini oricărui organism al Centrului de competențe.

#### Articolul 14

##### Președintele și reuniunile consiliului de conducere

1. Consiliul de conducere alege un președinte și un vicepreședinte dintre membrii cu drept de vot, pentru o perioadă de doi ani, **vizând atingerea echilibrului de gen**. Mandatul președintelui și al vicepreședintelui poate fi prelungit o singură dată, în urma unei decizii a consiliului de conducere. Cu toate acestea, dacă pe durata mandatului încetează calitatea acestora de membri ai consiliului de conducere, mandatul lor expiră automat la aceeași dată. Vicepreședintele îl înlocuiește din oficiu pe președinte în cazul în care acesta din urmă nu își poate exercita prerogativele. Președintele participă la vot. [AM 135]
2. Consiliul de conducere ține ședințe ordinare de cel puțin trei ori pe an. Acesta poate organiza reuniuni extraordinare la cererea Comisiei, la cererea unei treimi din numărul total al membrilor săi, la cererea președintelui sau la cererea directorului executiv în îndeplinirea sarcinilor sale.
3. Directorul executiv ia parte la deliberări, cu excepția cazului în care consiliul de conducere decide altfel, dar nu are drept de vot. ~~Consiliul de conducere poate invita alte persoane să participe la reuniunile sale în calitate de observatori, de la caz la caz.~~ [AM 136]
4. ~~Membrii Consiliului consultativ pe probleme industriale și științifice pot lua parte la reuniunile consiliului de conducere, la invitația președintelui, fără a avea drept de vot.~~ [AM 137]
5. Sub rezerva propriului regulament de procedură, membrii consiliului de conducere și supleanții lor pot să fie asistați în cursul reuniunilor de consilieri sau de experți.
6. Centrul de competențe asigură secretariatul consiliului de conducere.

#### Articolul 15

##### Regulile de vot în cadrul consiliului de conducere

1. ~~Uniunea deține 50 % din drepturile de vot. Drepturile de vot ale Uniunii sunt indivizibile.~~
2. ~~Fiecare stat membru participant deține un vot.~~
3. ~~Consiliul de conducere adoptă deciziile sale cu o majoritate de cel puțin 75 % din totalul voturilor, inclusiv voturile membrilor care sunt absenți, reprezentând cel puțin 75 % din totalul contribuțiilor financiare către Centrul de competențe. Contribuția financiară va fi calculată pe baza cheltuielilor estimate propuse de statele membre menționate la articolul 17 alineatul (2) litera (c) și pe baza raportului privind valoarea contribuțiilor statelor membre participante menționate la articolul 22 alineatul (5).~~
4. ~~Numai reprezentanții Comisiei și reprezentanții statelor membre participante dețin drepturi de vot.~~
5. ~~Președintele participă la vot.~~ [AM 138]

Miercuri, 17 aprilie 2019

### Articolul 15a

#### Regulile de vot în cadrul consiliului de conducere

1. Deciziile supuse votului se pot referi la:
  - (a) guvernarea și organizarea Centrului de competențe și a rețelei;
  - (b) alocarea bugetului Centrului de competențe și al rețelei;
  - (c) acțiuni comune întreprinse de mai multe state membre, completate, eventual, de resurse de la bugetului Uniunii, în urma unei decizii în conformitate cu litera (b).
2. Consiliul de conducere adoptă deciziile sale cu cel puțin 75 % din totalul voturilor tuturor membrilor. Drepturile de vot ale Uniunii sunt reprezentate de Comisie și sunt indivizibile.
3. Pentru deciziile prevăzute la alineatul (1) litera (a), fiecare stat membru este reprezentat și are aceleași drepturi de vot egale. Pentru restul de voturi disponibile, până la 100 %, Uniunea ar trebui să dețină cel puțin 50 % din drepturile de vot corespunzătoare contribuției sale financiare.
4. Pentru deciziile care intră sub incidența alineatului (1) literele (b) sau (c) sau pentru orice alte decizii care nu se încadrează la nicio altă categorie de la alineatul (1), Uniunea deține cel puțin 50 % din drepturile de vot corespunzătoare contribuției sale financiare. Numai statele membre contribuitoare au drepturi de vot, iar acestea vor corespunde contribuției lor financiare.
5. Dacă președintele a fost ales dintre reprezentanții statelor membre, președintele participă la vot ca reprezentant al statului său membru. [AM 139]

### SECȚIUNEA II

#### DIRECTORUL EXECUTIV

### Articolul 16

#### Numirea, revocarea sau prelungirea mandatului directorului executiv

1. Directorul executiv este o persoană care deține o experiență specifică și o reputație deosebită în domeniile în care își desfășoară activitatea Centrul de competențe.
2. Directorul executiv este angajat ca agent temporar al Centrului de competențe în conformitate cu articolul 2 litera (a) din Regimul aplicabil celorlalți agenți.
3. Directorul executiv este numit de Consiliul de conducere dintr-o listă de candidați propuși de Comisie, **cu nominalizări care să vizeze atingerea echilibrului de gen din partea statelor membre**, în urma unei proceduri de selecție deschise și , transparente și nediscriminatorii. [AM 140]
4. În scopul încheierii contractului directorului executiv, Centrul de competențe este reprezentat de președintele consiliului de conducere.
5. Durata mandatului directorului executiv este de ~~patru~~ **cinci** ani. Până la sfârșitul perioadei respective, Comisia realizează o analiză care ia în considerare evaluarea rezultatelor obținute de directorul executiv și viitoarele sarcini și provocări cu care se va confrunta Centrul de competențe. [AM 141]
6. La propunerea Comisiei, care ia în considerare evaluarea menționată la alineatul (5), consiliul de conducere poate reînnoi mandatul directorului executiv o singură dată, cu cel mult ~~patru~~ **cinci** ani. [AM 142]
7. Un director executiv al cărui mandat a fost prelungit nu poate să participe la o nouă procedură de selecție pentru același post.
8. Directorul executiv este demis din funcție numai printr-o decizie a consiliului de conducere, care acționează la propunerea **membrilor săi sau la propunerea** Comisiei. [AM 143]

Miercuri, 17 aprilie 2019

## Articolul 17

## Sarcinile directorului executiv

1. Directorul executiv este responsabil de operațiuni și de gestionarea curentă a Centrului de competențe și este reprezentantul legal al acestuia. Directorul executiv răspunde în fața consiliului de conducere și își execută atribuțiile în deplină independență, în limita prerogativelor acordate.
2. Directorul executiv îndeplinește în special următoarele sarcini în mod independent:
  - (a) punerea în aplicare a deciziilor adoptate de consiliul de conducere;
  - (b) sprijinirea activităților consiliului de conducere, asigurarea secretariatului reuniunilor acestuia și furnizarea tuturor informațiilor necesare pentru îndeplinirea sarcinilor acestuia;
  - (c) după consultarea consiliului de conducere, **a Consiliului consultativ pe probleme industriale și științifice, a ENISA** și a Comisiei, pregătirea și înaintarea spre adoptare consiliului de conducere a proiectului de plan strategic multianual și a proiectului de plan anual de activitate ale Centrului de competențe, inclusiv obiectul cererilor de propuneri, al cererilor de exprimare a interesului și al cererilor de oferte necesare pentru punerea în aplicare a planului de lucru și a estimărilor privind cheltuielile aferente, astfel cum au fost propuse de statele membre și de Comisie; **[AM 144]**
  - (d) pregătirea și înaintarea spre adoptare consiliului de conducere a proiectului de buget anual, inclusiv a schemei de personal aferente, care indică numărul de posturi temporare în fiecare grad și grupă de funcții, precum și numărul de agenți contractuali și de experți naționali detașați, exprimat în echivalent normă întreagă;
  - (e) punerea în aplicare a planului de lucru și prezentarea de rapoarte către consiliul de conducere;
  - (f) pregătirea proiectului de raport anual de activitate al Centrului de competențe, inclusiv prezentarea de informații privind cheltuielile aferente;
  - (g) asigurarea punerii în aplicare a unor proceduri eficiente de monitorizare și de evaluare a performanțelor Centrului de competențe;
  - (h) pregătirea unui plan de acțiune pentru a da curs concluziilor evaluărilor retrospective și trimiterea către Comisie și **Parlamentul European**, la fiecare doi ani, a unui raport privind progresele înregistrate; **[AM 145]**
  - (i) pregătirea, negocierea și încheierea de acorduri cu centrele naționale de coordonare;
  - (j) este responsabil de aspectele administrative, financiare și de personal, inclusiv de execuția bugetului Centrului de competențe, ținând seama în mod corespunzător de recomandările primite din partea funcției de audit intern, în limitele delegării conferite de către consiliul de conducere;
  - (k) aprobarea și gestionarea lansării cererilor de propuneri, în conformitate cu planul de lucru, și administrarea acordurilor și a deciziilor de grant;
  - (l) **în urma consultării cu Consiliul consultativ pe probleme industriale și științifice și cu ENISA**, aprobarea listei de acțiuni selectate pentru finanțare pe baza clasamentului stabilit de un grup de experți independenți; **[AM 146]**
  - (m) aprobarea și gestionarea lansării procedurilor de ofertare, în conformitate cu planul de lucru, și administrarea contractelor;
  - (n) aprobarea ofertelor selectate pentru finanțare;
  - (o) prezentarea proiectului de conturi anuale și a proiectului de bilanț anual funcției de audit intern și, ulterior, consiliului de conducere;
  - (p) asigurarea efectuării evaluării și a gestionării riscurilor;
  - (q) semnarea acordurilor, deciziilor și contractelor individuale de grant;
  - (r) semnarea contractelor de achiziții;

Miercuri, 17 aprilie 2019

- (s) elaborarea unui plan de acțiune în urma concluziilor rapoartelor de audit intern sau extern, precum și a investigațiilor desfășurate de Oficiul European de Luptă Antifraudă (OLAF) și prezentarea, de două ori pe an Comisiei și **Parlamentului European și** periodic consiliului de conducere, a unui raport privind progresele înregistrate; [AM 147]
- (t) elaborarea proiectului de reguli financiare aplicabile Centrului de competențe;
- (u) stabilirea și asigurarea funcționării unui sistem de control intern eficace și eficient și raportarea către consiliul de conducere a oricărei modificări semnificative a acestuia;
- (v) asigurarea unei comunicări eficiente cu instituțiile Uniunii și **prezentarea către Parlamentul European și Consiliu, la cerere, a unui raport**; [AM 148]
- (w) adoptarea oricărei alte măsuri necesare pentru a evalua progresul Centrului de competențe în ceea ce privește misiunea și obiectivele acestuia, astfel cum se prevede la articolele 3 și 4 din prezentul regulament;
- (x) executarea oricărei alte sarcini care îi este atribuită sau delegată de consiliul de conducere.

### SECȚIUNEA III

#### CONSILIUL CONSULTATIV PE PROBLEME INDUSTRIALE ȘI ȘTIINȚIFICE

##### Articolul 18

###### Structura Consiliului consultativ pe probleme industriale și științifice

1. Consiliul consultativ pe probleme industriale și științifice este format din cel mult ~~16~~ **25** membri. Membrii sunt numiți de consiliul de conducere dintre reprezentanții entităților din cadrul comunității ~~de competențe în materie de securitate cibernetică~~ **sau al membrilor individuali ai acesteia. Sunt eligibili numai reprezentanți ai entităților care nu sunt controlate de o țară terță sau de o entitate dintr-o țară terță, cu excepția țărilor din SEE și AELS. Numirea se face în conformitate cu o procedură deschisă, transparentă și nediscriminatorie. Componenta consiliului vizează realizarea echilibrului de gen și include o reprezentare echilibrată a grupurilor de părți interesate din industrie, comunitatea academică și societatea civilă.** [AM 149]
2. Membrii Consiliului consultativ pe probleme industriale și științifice dețin competențe specifice în ceea ce privește cercetarea în domeniul securității cibernetice, dezvoltarea industrială, ~~serviciile profesionale~~ **furnizarea, implementarea** sau desfășurarea **de servicii sau produse profesionale**. Cerințele pentru astfel de competențe specifice sunt precizate în detaliu de către consiliul de conducere. [AM 150]
3. Procedurile privind numirea membrilor săi de către consiliul de conducere și funcționarea Consiliului consultativ sunt precizate în regulamentul de procedură al Centrului de competențe și sunt făcute publice.
4. Durata mandatului membrilor Consiliului consultativ pe probleme industriale și științifice este de trei ani Acest mandat se poate reînnoi.
5. Reprezentanții Comisiei și ai ~~Agenciei Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor~~ **ENISA sunt invitați să participe** la lucrările Consiliului consultativ pe probleme industriale și științifice și ~~pot sprijini~~ **sprijină** lucrările acestuia. **Consiliul consultativ poate invita, de la caz la caz, și alți reprezentanți din partea comunității în calitate de observatori, consilieri sau experți, după caz.** [AM 151]

##### Articolul 19

###### Funcționarea Consiliului consultativ pe probleme industriale și științifice

1. Consiliul consultativ pe probleme industriale și științifice se întrunește cel puțin de ~~dois~~ **trei** ori pe an. [AM 152]

Miercuri, 17 aprilie 2019

2. Consiliul consultativ pe probleme industriale și științifice ~~poate oferi consiliere~~ **prezintă sugestii** consiliului de conducere cu privire la instituirea de grupuri de lucru cu privire la aspecte specifice relevante pentru activitatea Centrului de competențe, **ori de câte ori acestea se încadrează în sarcinile și domeniile de competențe specificate la articolul 20 și atunci când acest lucru este necesar în cadrul coordonării generale a unuia sau mai multor membri ai Consiliului consultativ pe probleme industriale și științifice.** [AM 153]
3. Consiliul consultativ pe probleme industriale și științifice își alege președintele.
4. Consiliul consultativ pe probleme industriale și științifice își adoptă regulamentul de procedură, inclusiv îi desemnează pe reprezentanții Consiliului consultativ, după caz, și stabilește durata mandatului acestora.

## Articolul 20

## Sarcinile Consiliului consultativ pe probleme industriale și științifice

Consiliul consultativ pe probleme industriale și științifice informează **periodic** Centrul de competențe cu privire la desfășurarea activităților sale și: [AM 154]

- (1) oferă directorului executiv și consiliului de conducere consiliere strategică și contribuții la **orientarea și implementarea operațiunilor Centrului de competențe în ceea ce privește sectorul industrial și cercetarea și la elaborarea planului de lucru și a planului strategic multianual în termenele stabilite de consiliul de conducere;** [AM 155]
- (1a) **consiliază consiliul de conducere în ceea ce privește instituirea grupurilor de lucru cu privire la aspecte specifice relevante pentru activitatea Centrului de competențe;** [AM 156]
- (2) organizează consultări publice deschise tuturor părților interesate din sectorul public și privat care au un interes în domeniul securității cibernetice, pentru a colecta contribuții pentru consilierea strategică menționată la alineatul (1);
- (3) promovează și colectează feedback cu privire la planul de lucru și la planul strategic multianual ale Centrului de competențe **și oferă consiliere consiliului de conducere cu privire la modul de îmbunătățire a orientării strategice și a funcționării Centrului de competențe.** [AM 157]

## CAPITOLUL III

## DISPOZIȚII FINANCIARE

## Articolul 21

## Contribuția financiară a Uniunii

1. Contribuția Uniunii la centrul de competențe pentru acoperirea costurilor administrative și a costurilor operaționale cuprinde următoarele:
- (a) ~~1 981 668 000 EUR~~ **1 780 954 875 EUR în prețurile din 2018 (1 998 696 000 EUR în prețuri curente)** din programul Europa digitală, inclusiv până la **21 385 465 EUR în prețurile din 2018 (23 746 000 EUR în prețuri curente)** pentru costuri administrative; [AM 158]
- (b) O sumă din programul Orizont Europa, inclusiv în ceea ce privește costurile administrative, care urmează să fie stabilită ținând seama de procesul de planificare strategică care va fi efectuat în conformitate cu articolul 6 alineatul (6) din Regulamentul XXX [Regulamentul privind programul Orizont Europa];
- (ba) **o sumă din Fondul european de apărare destinată acțiunilor din domeniul apărării ale Centrului de competențe, inclusiv pentru toate costurile administrative aferente, cum ar fi costurile pe care Centrul de competențe le poate suporta atunci când acționează în calitate de administrator de proiect în ceea ce privește acțiunile desfășurate în cadrul Fondului european de apărare.** [AM 159]

Miercuri, 17 aprilie 2019

2. Contribuția maximă a Uniunii se plătește din creditele din bugetul general al Uniunii alocate pentru [programul Europa digitală], din creditele alocate programului specific de punere în aplicare a programului Orizont Europa, instituit prin Decizia XXX, **din creditele pentru Fondul european de apărare și pentru alte programe și proiecte care intră în sfera de competență a Centrului de competențe sau a rețelei.** [AM 160]
3. Centrul de competențe pune în aplicare acțiunile în materie de securitate cibernetică ale [programului Europa digitală] și ale [programului Orizont Europa] în conformitate cu articolul 62 litera (c) punctul (iv) din Regulamentul (UE, Euratom) XXX<sup>(20)</sup> [Regulamentul financiar].
4. Contribuția financiară a Uniunii **din programele Europa digitală și Orizont Europa** nu acoperă sarcinile menționate la articolul 4 alineatul (8) litera (b). **Acestea pot fi acoperite de contribuții financiare din Fondul european de apărare.** [AM 161]

#### Articolul 22

##### Contribuțiile statelor membre participante

1. Statele membre participante au o contribuție totală la costurile operaționale și administrative ale Centrului de competențe cel puțin egală cu cea prevăzută la articolul 21 alineatul (1) din prezentul regulament.
2. În scopul evaluării contribuțiilor menționate la alineatul (1) și la articolul 23 alineatul (3) litera (b) punctul (ii), costurile se stabilesc în conformitate cu practicile obișnuite de contabilitate a costurilor ale statelor membre în cauză, cu standardele de contabilitate aplicabile ale statului membru și cu standardele internaționale de contabilitate și standardele internaționale de raportare financiară aplicabile. Costurile sunt certificate de un auditor extern independent desemnat de statul membru în cauză. Metoda de evaluare poate fi verificată de către Centrul de competențe, în cazul în care există dubii cu privire la certificare.
3. Dacă un stat membru participant nu își îndeplinește angajamentele privind contribuția sa financiară, directorul executiv consemnează acest lucru și stabilește un termen rezonabil pentru remedierea acestei situații. Dacă situația nu este remediată în termenul respectiv, directorul executiv convoacă o reuniune a consiliului de conducere pentru a decide dacă dreptul de vot al statului membru participant care nu și-a îndeplinit obligațiile trebuie revocat sau dacă trebuie luate alte măsuri până la îndeplinirea obligațiilor de către acesta. Drepturile de vot ale statului membru care nu și-a îndeplinit obligațiile sunt suspendate până la remedierea situației.
4. Comisia poate suprima, reduce în mod proporțional sau suspenda contribuția financiară a Uniunii către Centrul de competențe în cazul în care statele membre participante nu efectuează ~~efectuează doar parțial~~ sau efectuează ~~cu întârziere~~ **doar parțial** contribuțiile menționate la alineatul (1). **Suprimarea, reducerea sau suspendarea contribuției financiare a Uniunii de către Comisie este proporțională în ceea ce privește valoarea și durata acesteia cu reducerea, suprimarea sau suspendarea contribuțiilor statelor membre.** [AM 162]
5. Până la data de 31 ianuarie a fiecărui an, statele membre participante prezintă un raport consiliului de conducere cu privire la valoarea contribuțiilor menționate la alineatul (1), efectuate în fiecare dintre exercițiile financiare precedente.

#### Articolul 23

##### Costurile și resursele centrului de competențe

1. Centrul de competențe este finanțat în comun de Uniune și de statele membre prin contribuții financiare plătite în tranșe și contribuții aferente costurilor suportate de centrele naționale de coordonare și de beneficiari în cadrul punerii în aplicare a unor acțiuni care nu sunt rambursate de către Centrul de competențe.
2. Costurile administrative ale Centrului de competențe nu depășesc [număr] EUR și sunt acoperite prin contribuții financiare anuale, divizate în mod egal între Uniune și statele membre participante. În cazul în care o parte din contribuția la costurile administrative nu este utilizată, aceasta poate fi pusă la dispoziție pentru acoperirea costurilor operaționale ale Centrului de competențe.
3. Costurile operaționale ale Centrului de competențe sunt acoperite prin:
  - (a) contribuția financiară a Uniunii;

<sup>(20)</sup> [a se adăuga titlul complet și referința JO]

Miercuri, 17 aprilie 2019

- (b) contribuții din partea statelor membre participante sub formă de:
- (i) contribuții financiare; și
  - (ii) după caz, contribuții în natură ale statelor membre participante la costurile suportate de centrele naționale de coordonare și de beneficiari în cadrul punerii în aplicare a acțiunilor indirecte, din care se scade contribuția Centrului de competențe și orice altă contribuție a Uniunii la aceste costuri;
4. Resursele centrului de competențe incluse în bugetul acestuia constau în următoarele contribuții:
- (a) contribuții financiare ale **Uniunii și ale** statelor membre participante la costurile administrative; [AM 163]
  - (b) contribuții financiare ale **Uniunii și ale** statelor membre participante la costurile operaționale; [AM 164]
  - (c) orice venituri generate de Centrul de competențe;
  - (d) orice alte contribuții financiare, resurse și venituri.
5. Orice dobândă generată de contribuțiile plătite Centrului de competențe de către statele membre participante este considerată drept venit al acestuia.
6. Toate resursele Centrului de competențe și activitățile acestuia au ca scop îndeplinirea obiectivelor prevăzute la articolul 4.
7. Centrul de competențe este proprietarul tuturor activelor generate de el sau transferate către el în scopul îndeplinirii obiectivelor sale.
8. Cu excepția situației de lichidare a Centrului de competențe, orice excedent de venit în raport cu cheltuielile nu se plătește membrilor participanți ai Centrului de competențe.

**8a. Centrul de competențe cooperează îndeaproape cu alte instituții, agenții și organisme ale Uniunii pentru a beneficia de sinergii și, unde este posibil, pentru a reduce costurile administrative.** [AM 165]

#### Articolul 24

##### Angajamente financiare

Angajamentele financiare ale Centrului de competențe nu depășesc valoarea totală a resurselor financiare disponibile sau angajate la buget de către membrii acestuia.

#### Articolul 25

##### Exercițiul financiar

Exercițiul financiar începe la 1 ianuarie și se încheie la 31 decembrie.

#### Articolul 26

##### Întocmirea bugetului

1. În fiecare an, directorul executiv elaborează un proiect de situație a estimărilor de venituri și cheltuieli ale Centrului de competențe pentru următorul exercițiu financiar și îl înaintază consiliului de conducere, împreună cu un proiect de schemă de personal. Veniturile și cheltuielile trebuie să fie în echilibru. Cheltuielile Centrului de competențe cuprind cheltuielile cu personalul, cheltuielile administrative, cheltuielile de infrastructură și cheltuielile operaționale. Cheltuielile administrative sunt menținute la minimum.
2. În fiecare an, pe baza proiectului situației estimărilor de venituri și cheltuieli menționat la alineatul (1), consiliul de conducere adoptă situația estimărilor de venituri și cheltuieli ale Centrului de competențe pentru următorul exercițiu financiar.
3. În fiecare an, până la data de 31 ianuarie, consiliul de conducere transmite Comisiei situația estimărilor menționată la alineatul (2), care face parte din documentul unic de programare.

Miercuri, 17 aprilie 2019

4. Pe baza situației estimărilor respective, Comisia înscrie în proiectul de buget al Uniunii estimările pe care le consideră necesare pentru schema de personal și valoarea contribuției care urmează să fie suportată din bugetul general, pe care le prezintă Parlamentului European și Consiliului în conformitate cu articolele 313 și 314 din TFUE.
5. Parlamentul European și Consiliul autorizează creditele reprezentând contribuția alocată Centrului de competențe.
6. Parlamentul European și Consiliul adoptă schema de personal a Centrului de competențe.
7. Consiliul de conducere adoptă bugetul centrului odată cu planul de lucru. Bugetul centrului devine definitiv după adoptarea definitivă a bugetului general al Uniunii. După caz, consiliul de conducere ajustează bugetul Centrului de competențe și planul de lucru în conformitate cu bugetul general al Uniunii.

#### Articolul 27

##### Prezentarea conturilor Centrului de competențe și descărcarea de gestiune

Prezentarea conturilor provizorii și finale ale Centrului de competențe și descărcarea de gestiune respectă normele și calendarul Regulamentului financiar și ale normelor financiare ale acestuia, adoptate în conformitate cu articolul 29.

#### Articolul 28

##### Raportarea operațională și financiară

1. Directorul executiv prezintă anual consiliului de conducere un raport referitor la executarea sarcinilor sale în conformitate cu normele financiare ale Centrului de competențe.
2. În termen de două luni de la încheierea fiecărui exercițiu financiar, directorul executiv prezintă consiliului de conducere spre aprobare un raport anual de activitate referitor la progresul înregistrat de Centrul de competențe în anul calendaristic anterior, în special în ceea ce privește planul de lucru pentru anul respectiv. Raportul include, printre altele, informații cu privire la următoarele aspecte:
  - (a) acțiunile operaționale desfășurate și cheltuielile aferente;
  - (b) acțiunile prezentate, inclusiv o defalcare în funcție de tipul de participant, inclusiv IMM-uri, și în funcție de statul membru;
  - (c) acțiunile selectate pentru finanțare, inclusiv o defalcare în funcție de tipul de participant, inclusiv IMM-uri, și în funcție de statul membru, cu indicarea contribuției Centrului de competențe destinate participanților individuali și acțiunilor individuale;
  - (d) progresele înregistrate în privința atingerii obiectivelor prevăzute la articolul 4 și propuneri de alte acțiuni necesare în vederea îndeplinirii acestor obiective.
3. După aprobarea sa de către consiliul de conducere, raportul anual de activitate este pus la dispoziția publicului.

#### Articolul 29

##### Regulile financiare

Centrul de competențe își adoptă normele financiare specifice în conformitate cu articolul 70 din Regulamentul XXX [noul Regulament financiar].

#### Articolul 30

##### Protejarea intereselor financiare

1. În cursul punerii în aplicare a acțiunilor finanțate în temeiul prezentului regulament, Centrul de competențe ia măsurile corespunzătoare care să garanteze protejarea intereselor financiare ale Uniunii prin aplicarea de măsuri preventive împotriva fraudei, corupției și a oricăror alte activități ilegale, prin controale **periodice și** eficace și, în cazul în care se constată nereguli, prin recuperarea sumelor plătite în mod necuvenit, precum și, dacă este necesar, prin sancțiuni administrative eficace, proporționale și disuasive. [AM 166]

Miercuri, 17 aprilie 2019

2. Centrul de competențe acordă personalului Comisiei și altor persoane autorizate de Comisie, precum și Curții de Conturi, acces la sediile și spațiile sale și la toate informațiile necesare pentru efectuarea auditurilor acestora, inclusiv la informațiile în format electronic.
3. Oficiul European de Luptă Antifraudă (OLAF) poate efectua investigații, inclusiv verificări și inspecții la fața locului, în conformitate cu dispozițiile și procedurile prevăzute în Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului <sup>(21)</sup> și în Regulamentul (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului <sup>(22)</sup>, cu scopul de 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 acord de grant sau cu un contract finanțat, direct sau indirect, în conformitate cu prezentul regulament.
4. Fără a aduce atingere alineatelor (1), (2) și (3) din prezentul articol, contractele și acordurile de grant care rezultă din punerea în aplicare a prezentului regulament conțin dispoziții care împuternicesc în mod expres Comisia, Centrul de competențe, Curtea de Conturi și OLAF să efectueze astfel de audituri și investigații, în conformitate cu competențele acestora. În cazul în care punerea în aplicare a unei acțiuni este externalizată sau subdelegată, în totalitate sau parțial, sau în cazul în care se impune atribuirea unui contract de achiziții publice sau de sprijin financiar unui terț, contractul sau acordul de grant include obligația contractantului sau a beneficiarului de a impune oricărei părți terțe implicate acceptarea explicită a acestor competențe ale Comisiei, ale Centrului de competențe, ale Curții de Conturi și ale OLAF.

## CAPITOLUL IV

## PERSONALUL CENTRULUI DE COMPETENȚE

## Articolul 31

## Personalul

1. Statutul funcționarilor și Regimul aplicabil celorlalți agenți ai Uniunii Europene, astfel cum sunt stabilite în Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului <sup>(23)</sup> (denumite în continuare „Statutul funcționarilor” și „Regimul aplicabil celorlalți agenți”) și normele adoptate în comun de instituțiile Uniunii în scopul aplicării Statutului funcționarilor și a Regimului aplicabil celorlalți agenți se aplică personalului Centrului de competențe.
2. Consiliul de conducere exercită, în ceea ce privește personalul Centrului de competențe, competențele conferite autorității de numire prin Statutul funcționarilor și competențele conferite autorității abilitate să încheie contracte prin Regimul aplicabil celorlalți agenți (denumite în continuare „competențele autorității de numire”).
3. Consiliul de conducere adoptă, în conformitate cu articolul 110 din Statutul funcționarilor, o decizie, în temeiul articolului 2 alineatul (1) din Statutul funcționarilor și al articolului 6 din Regimul aplicabil celorlalți agenți, prin care competențele relevante ale autorității de numire sunt delegate directorului executiv și în care sunt definite condițiile în care această delegare de competențe poate fi suspendată. Directorul executiv este autorizat să subdelege competențele respective.
4. În cazul în care anumite circumstanțe excepționale impun acest lucru, consiliul de conducere poate, printr-o decizie, să suspende temporar delegarea competențelor autorității de numire către directorul executiv, precum și orice subdelegare efectuată de către acesta. În acest caz, consiliul de conducere exercită el însuși competențele autorității de numire sau le delegă unuia dintre membrii săi sau unui membru al personalului centrului de competențe, altul decât directorul executiv.

<sup>(21)</sup> 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).

<sup>(22)</sup> 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).

<sup>(23)</sup> Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului din 29 februarie 1968 de stabilire a Statutului funcționarilor Comunităților Europene, precum și a Regimului aplicabil celorlalți agenți ai acestor comunități și de instituire a unor măsuri speciale tranzitorii aplicabile funcționarilor Comisiei (JO L 56, 4.3.1968, p. 1).

Miercuri, 17 aprilie 2019

5. Consiliul de conducere adoptă norme de punere în aplicare referitoare la Statutul funcționarilor și la Regimul aplicabil celorlalți agenți, în conformitate cu articolul 110 din Statutul funcționarilor.
6. Resursele de personal sunt stabilite în schema de personal a Centrului de competențe, indicându-se numărul de posturi temporare pe grupe de funcții și pe grade, precum și numărul de agenți contractuali, exprimat în echivalent normă întreagă, în conformitate cu bugetul anual al acestuia.
7. **Centrul de competență urmărește să realizeze echilibrul de gen în rândul personalului său.** Personalul ~~centrului de competențe~~ este format din agenți temporari și agenți contractuali. [AM 167]
8. Toate costurile cu privire la personal sunt suportate de Centrul de competențe.

#### Articolul 32

##### Experți naționali detașați și alte categorii de personal

1. Centrul de competențe poate recurge la experți naționali detașați sau alte categorii de personal care nu sunt angajați ai Centrului de competențe.
2. Consiliul de conducere adoptă o decizie de stabilire a normelor aplicabile detașării experților naționali la Centrul de competențe, de comun acord cu Comisia.

#### Articolul 33

##### Privilegii și imunități

Centrului de competențe și personalului acestuia li se aplică Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene.

### CAPITOLUL V

#### DISPOZIȚII COMUNE

#### Articolul 34

##### Norme de securitate

1. Articolul 12 alineatul (7) din Regulamentul (UE) nr. XXX [programul Europa digitală] se aplică participării la toate acțiunile finanțate de Centrul de competențe.
2. Următoarele norme de securitate specifice se aplică acțiunilor finanțate din programul Orizont Europa:
  - (a) în sensul articolului 34 alineatul (1) [Proprietate și protecție] din Regulamentul (UE) nr. XXX [Orizont Europa], atunci când planul de lucru prevede acest lucru, acordarea de licențe neexclusive poate fi limitată la terți stabiliți sau considerați a fi stabiliți în statele membre și controlați de state membre și/sau de resortisanți ai statelor membre;
  - (b) în sensul articolului 36 alineatul (4) litera (b) [Transfer și acordarea de licențe] din Regulamentul (UE) nr. XXX [Orizont Europa], transferul sau acordarea de licență către o entitate juridică stabilită într-o țară asociată sau stabilită în Uniune, dar controlată din țări terțe este, de asemenea, un motiv pentru a se opune transferului de proprietate asupra rezultatelor sau acordării unei licențe exclusive cu privire la rezultate;
  - (c) în sensul articolului 37 alineatul (3) litera (a) [Drepturi de acces] din Regulamentul (UE) nr. XXX [Orizont Europa], atunci când planul de lucru prevede acest lucru, acordarea accesului la rezultate și la informațiile preexistente poate fi limitată doar la o entitate juridică stabilită sau considerată a fi stabilită în statele membre și controlată de statele membre și/sau de resortisanți ai statelor membre;
- (ca) **Articolul 22 [Proprietate asupra rezultatelor], articolul 23 [Proprietate asupra rezultatelor] și articolul 30 [Aplicarea normelor privind informațiile clasificate] din Regulamentul (UE) nr. XXX [Fondul european de apărare] se aplică participării la toate acțiunile din domeniul apărării ale Centrului de competențe, atunci când planul de lucru prevede acest lucru. Acordarea de licențe neexclusive poate fi limitată la părți terțe stabilite sau considerate a fi stabilite în statele membre și controlate de state membre și/sau de resortisanți ai statelor membre.** [AM 168]

Miercuri, 17 aprilie 2019

## Articolul 35

## Transparență

1. Centrul de competențe își desfășoară activitățile cu ~~un~~ **cel mai ridicat** nivel ~~ridicat~~ de transparență. [AM 169]
2. Centrul de competențe se asigură că publicului și tuturor părților interesate li se furnizează informații **cuprinzătoare**, adecvate, obiective, fiabile și ușor accesibile, în **timp util, în** special în ceea ce privește rezultatele activității sale **Centrului de competențe, rețelei, Consiliului consultativ pe probleme industriale și științifice și a Comunității**. De asemenea, acesta face publice declarațiile de interese întocmite în conformitate cu articolul ~~41~~ **42**. [AM 170]
3. Consiliul de conducere, pe baza unei propuneri primite de la directorul executiv, poate autoriza părțile interesate să participe ca observatori la unele dintre activitățile Centrului de competențe.
4. Centrul de competențe stabilește, în regulamentul său de procedură, modalitățile practice de punere în aplicare a normelor privind transparența menționate la alineatele (1) și (2). În cazul acțiunilor finanțate din programul Orizont Europa, se va ține seama în mod corespunzător de dispozițiile anexei III la Regulamentul privind programul Orizont Europa.

## Articolul 36

## Norme de securitate privind protejarea informațiilor clasificate și a informațiilor sensibile neclasificate

1. Fără a aduce atingere articolului 35, Centrul de competențe 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, integral sau parțial.
2. Membrii consiliului de conducere, directorul executiv, membrii Consiliului consultativ pe probleme industriale și științifice, experții externi care participă la grupurile de lucru ad-hoc și membrii personalului centrului respectă cerințele de confidențialitate prevăzute la articolul 339 din Tratatul privind funcționarea Uniunii Europene, chiar și după încetarea atribuțiilor lor.
3. Consiliul de conducere al Centrului de competențe adoptă normele de securitate ale Centrului de competențe, după aprobarea de către Comisie, pe baza principiilor și a normelor stabilite în normele de securitate ale Comisiei pentru protecția informațiilor UE clasificate (IUEC) și a informațiilor sensibile neclasificate, inclusiv, inter alia, dispoziții privind prelucrarea și stocarea informațiilor respective, astfel cum se prevede în Deciziile (UE, Euratom) 2015/443 <sup>(24)</sup> și 2015/444 <sup>(25)</sup> ale Comisiei.
4. Centrul de competențe poate lua toate măsurile necesare în vederea facilitării schimbului de informații relevante pentru sarcinile sale cu Comisia și statele membre și, acolo unde este cazul, cu agențiile și organismele relevante ale Uniunii. Orice acord administrativ încheiat în acest scop cu privire la partajarea IUEC sau, în absența unui astfel de acord, orice comunicare excepțională ad-hoc a IUEC trebuie să primească aprobarea prealabilă a Comisiei.

## Articolul 37

## Accesul la documente

1. Regulamentul (CE) nr. 1049/2001 se aplică documentelor deținute de Centrul de competențe.
2. Consiliul de conducere adoptă modalitățile de punere în aplicare a Regulamentului (CE) nr. 1049/2001 în termen de șase luni de la înființarea Centrului de competențe.

<sup>(24)</sup> Decizia (UE, Euratom) 2015/443 a Comisiei din 13 martie 2015 privind securitatea în cadrul Comisiei (JO L 72, 17.3.2015, p. 41).

<sup>(25)</sup> 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).

Miercuri, 17 aprilie 2019

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

#### Articolul 38

##### Monitorizare, evaluare și revizuire

1. Centrul de competențe se asigură că activitățile sale, inclusiv cele gestionate prin intermediul centrelor naționale de coordonare și al rețelei, fac obiectul monitorizării continue și sistematice și al evaluării periodice. Centrul de competențe se asigură că datele pentru monitorizarea punerii în aplicare și a rezultatelor programului sunt colectate în mod eficient, eficace și în timp util și că se impun cerințe de raportare proporționale pentru beneficiarii fondurilor Uniunii și pentru statele membre. Rezultatele evaluării se fac publice.

2. Odată ce există suficiente informații disponibile cu privire la punerea în aplicare a prezentului regulament, dar nu mai târziu de trei ani și jumătate de la începerea punerii sale în aplicare, Comisia efectuează o evaluare intermediară a centrului de competențe. Comisia întocmește un raport cu privire la această evaluare și transmite raportul respectiv Parlamentului European și Consiliului până la 31 decembrie 2024. Centrul de competențe și statele membre furnizează Comisiei informațiile necesare pentru pregătirea respectivului raport.

3. Evaluarea menționată la alineatul (2) include o evaluare a rezultatelor obținute de către Centrul de competențe, având în vedere obiectivele, mandatul și sarcinile sale, **precum și eficacitatea și eficiența**. În cazul în care consideră că existența Centrului de competențe este în continuare justificată în raport cu obiectivele, mandatul și sarcinile acestuia, Comisia poate propune ca durata mandatului Centrului de competențe, prevăzută la articolul 46, să fie prelungită. [AM 171]

4. Pe baza concluziilor evaluării intermediare menționate la alineatul (2), Comisia poate acționa în conformitate cu [articolul 22 alineatul (5)] sau poate lua orice altă măsură adecvată.

5. Monitorizarea, evaluarea, eliminarea treptată și reînnoirea contribuției din partea programului Orizont Europa vor respecta dispozițiile articolelor 8, 45 și 47 și ale anexei III din Regulamentul privind programul Orizont Europa și modalitățile de punere în aplicare convenite.

6. Monitorizarea, raportarea și evaluarea contribuției din partea programului Europa digitală vor respecta dispozițiile articolelor 24 și 25 din programul Europa digitală.

7. În cazul lichidării Centrului de competențe, Comisia efectuează o evaluare finală a Centrului de competențe în termen de șase luni de la lichidarea acestuia, dar nu mai târziu de doi ani de la declanșarea procedurii de lichidare menționate la articolul 46 din prezentul regulament. Rezultatele evaluării finale sunt prezentate Parlamentului European și Consiliului.

#### Articolul 38a

##### *Personalitatea juridică a Centrului de competențe*

1. **Centrul de competențe are personalitate juridică.**

2. **În fiecare stat membru, Centrul de competențe dispune de cea mai extinsă capacitate juridică acordată persoanelor juridice în temeiul legislației statului membru respectiv. În special, acesta poate să achiziționeze sau să înstrăineze bunuri mobile și imobile și să se constituie parte în proceduri judiciare.** [AM 172]

#### Articolul 39

##### Răspunderea Centrului de competențe

1. Răspunderea contractuală a Centrului de competențe este reglementată de dreptul aplicabil acordului, deciziei sau contractului în cauză.

Miercuri, 17 aprilie 2019

2. În cazul răspunderii extracontractuale, în conformitate cu principiile generale comune legislațiilor statelor membre, Centrul de competențe acordă despăgubiri pentru toate prejudiciile provocate de personalul său în exercițiul funcțiunii.
3. Orice plată efectuată de Centrul de competențe destinată să acopere răspunderea menționată la alineatele (1) și (2), precum și costurile și cheltuielile aferente sunt considerate cheltuieli ale Centrului de competențe și sunt suportate din resursele acestuia.
4. Centrul de competențe este singurul responsabil pentru îndeplinirea obligațiilor sale.

## Articolul 40

## Competența Curții de Justiție a Uniunii Europene și dreptul aplicabil

1. Curtea de Justiție a Uniunii Europene are competențe:
  - (1) în temeiul unei clauze compromisorii prevăzute în acordurile, deciziile sau contractele încheiate de Centrul de competențe;
  - (2) în litigiile referitoare la despăgubirile acordate pentru prejudiciile cauzate de personalul Centrului de competențe în exercițiul funcțiunii sale;
  - (3) în litigiile dintre Centrul de competențe și personalul său în limitele și condițiile prevăzute de Statutul funcționarilor.
2. Pentru orice aspect care nu este reglementat prin prezentul regulament sau prin alte acte juridice ale Uniunii, se aplică legislația statului membru în care se află sediul Centrului de competențe.

## Articolul 41

## Răspunderea membrilor și asigurarea

1. Răspunderea financiară a membrilor în ceea ce privește datoriile Centrului de competențe se limitează la contribuția lor deja plătită în contul cheltuielilor administrative.
2. Centrul de competențe subscrie la o asigurare adecvată și efectuează plățile necesare.

## Articolul 42

## Conflicte de interese

Consiliul de conducere al Centrului de competențe adoptă norme pentru prevenirea și gestionarea, **identificarea și soluționarea** conflictelor de interese în rândul membrilor, organismelor și personalului acesteia. ~~Aceste norme conțin dispozițiile menite să evite un conflict de interese în ceea ce privește reprezentanții membrilor care fac parte din consiliul de conducere, precum și din Consiliul~~ **, inclusiv în ceea ce îl privește pe directorul executiv, precum și în rândul membrilor consiliului de conducere, ai Consiliului** consultativ pe probleme industriale și științifice, ~~în conformitate cu Regulamentul XXX [noul Regulament financiar] și ai comunității.~~ [AM 173]

**Statele membre asigură prevenirea, identificarea și rezolvarea conflictelor de interese în cadrul centrelor naționale de coordonare.** [AM 174]

**Normele menționate la primul paragraf respectă Regulamentul (UE, Euratom) 2018/1046.** [AM 175]

## Articolul 43

## Protecția datelor cu caracter personal

1. Prelucrarea datelor cu caracter personal de către Centrul de competențe face obiectul Regulamentului (UE) nr. XXX/2018 al Parlamentului European și al Consiliului.
2. Consiliul de conducere adoptă măsurile de punere în aplicare menționate la articolul xx alineatul (3) din Regulamentul (UE) nr. xxx/2018. Consiliul de conducere poate adopta măsuri suplimentare necesare pentru aplicarea de către Centrul de competențe a Regulamentului (UE) nr. xxx/2018.

Miercuri, 17 aprilie 2019

Articolul 44

**Sediu și sprijin din partea statului membru gazdă [AM 176]**

***Sediul Centrului de competențe se stabilește printr-o procedură responsabilă din punct de vedere democratic, utilizând criteriile transparente și în conformitate cu dreptul Uniunii. [AM 177]***

***Statul membru gazdă pune la dispoziție cele mai bune condiții posibile pentru a asigura buna funcționare a Centrului de competențe, inclusiv un sediu unic, dar și alte condiții, cum ar fi accesibilitatea la 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 partenerii angajaților. [AM 178]***

Centrul de competențe și statul membru ~~[Belgia]~~ în care se află sediul acestuia ~~pot încheia~~ **încheie** un acord administrativ referitor la privilegii și imunități, precum și la alte tipuri de sprijin care urmează să fie oferite de statul membru respectiv Centrului de competențe. [AM 179]

CAPITOLUL VII

DISPOZIȚII FINALE

Articolul 45

Acțiuni inițiale

1. Comisiei îi revine răspunderea pentru înființarea și asigurarea exploataării Centrului de competențe în etapa inițială, până când acesta are capacitatea operațională necesară execuției propriului buget. Comisia adoptă, în conformitate cu dreptul Uniunii, toate măsurile necesare cu implicarea organismelor competente ale Centrului de competențe.
2. În sensul alineatului (1), până la preluarea de către directorul executiv a responsabilităților sale în urma numirii sale de către consiliul de conducere, în conformitate cu articolul 16, Comisia poate să desemneze un director executiv interimar și să îndeplinească sarcinile atribuite directorului executiv, care poate fi asistat de un număr limitat de funcționari ai Comisiei. Comisia poate desemna un număr limitat de funcționari proprii, cu titlu provizoriu.
3. După aprobarea prealabilă a consiliului de conducere, directorul executiv interimar poate autoriza toate plățile acoperite de creditele prevăzute în bugetul anual al Centrului de competențe și poate adopta decizii, încheia acorduri și contracte, inclusiv contracte de angajare a personalului, ca urmare a adoptării schemei de personal a Centrului de competențe.
4. Directorul executiv interimar stabilește, de comun acord cu directorul executiv al Centrului de competențe și sub rezerva aprobării de către consiliul de conducere, data la care Centrul de competențe are capacitatea de a-și executa propriul buget. De la data respectivă, Comisia se abține să angajeze credite și să efectueze plăți pentru activitățile Centrului de competențe.

**Articolul 45a**

**Exercitarea delegării**

1. **Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.**
2. **Competența de a adopta acte delegate menționată la articolul 6 alineatul (5a) și la articolul 8 alineatul (4b) se conferă Comisiei pe o perioadă nedeterminată de la ... [data intrării în vigoare a prezentului regulament].**
3. **Delegarea de competențe menționată la articolul 6 alineatul (5a) și la articolul 8 alineatul (4b) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în Jurnalul Oficial al Uniunii Europene sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.**

Miercuri, 17 aprilie 2019

4. Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legislație.
5. De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.
6. Un act delegat adoptat în temeiul articolului 6 alineatul (5a) și al articolului 8 alineatul (4b) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecțiuni în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu, sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecțiuni. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului. [AM 180]

## Articolul 46

## Durată

1. Centrul de competențe se înființează pentru perioada cuprinsă între 1 ianuarie 2021 și 31 decembrie 2029.
2. La sfârșitul acestei perioade, cu excepția cazului în care se decide altfel prin revizuirea prezentului regulament, se declanșează procedura de lichidare. Procedura de lichidare se declanșează automat în cazul în care Uniunea sau toate statele membre participante se retrag din Centrul de competențe.
3. În scopul derulării procedurilor de lichidare a Centrului de competențe, consiliul de conducere numește unul sau mai mulți lichidatori care se conformează deciziilor consiliului de conducere.
4. În momentul lichidării Centrului de competențe, activele sale sunt utilizate pentru compensarea pasivelor și a cheltuielilor legate de lichidarea sa. Orice surplus se distribuie între Uniune și statele membre participante, proporțional cu contribuția lor financiară la Centrul de competențe. Orice astfel de surplus distribuit Uniunii se restituie bugetului Uniunii.

## Articolul 47

## Intrare în vigoare

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

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

Adoptat la Bruxelles,

Pentru Parlamentul European,

Președintele

Pentru Consiliu,

Președintele