Consiliul
Uniunii Europene

Bruxelles, 31 octombrie 2022
(OR. en)

14128/22

Dosar interinstituțional:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

NOTĂ PUNCT „I/A”

Sursă:	Secretariatul General al Consiliului
Destinatar:	Comitetul Reprezentanților Permanenți (partea II)/Consiliul
Nr. doc. ant.:	10097/5/22 REV 5
Nr. doc. Csie:	7474/22 + ADD 1
Subiect:	Propunere de regulament al Parlamentului European și al Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii – Abordare generală

INTRODUCERE

1. La 22 martie 2022, Comisia a adoptat propunerea de regulament privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii. Propunerea era una dintre măsurile prevăzute în Strategia de securitate cibernetică a UE pentru deceniul digital[1], care vizează consolidarea rezilienței colective a Uniunii împotriva amenințărilor cibernetice.

[1] 14133/20.

În concluziile sale din 22 martie 2021 privind această strategie[2], Consiliul a subliniat că securitatea cibernetică este „vital[ă] pentru funcționarea instituțiilor și administrației publice, atât la nivel național, cât și la nivelul UE, precum și pentru societatea noastră și pentru economie în ansamblu”.

2. Propunerea Comisiei, întemeiată pe articolul 298 din Tratatul privind funcționarea Uniunii Europene, vizează îmbunătățirea nivelului de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii prin instituirea unui cadru comun, ținând seama în mod corespunzător de autonomia fiecărei entități a Uniunii. În special, obiectivele propunerii sunt:

   – consolidarea mandatului și a finanțării CERT-UE (centru interinstituțional autonom de răspuns la incidente de securitate cibernetică pentru entitățile Uniunii);

   – instituirea unei structuri interinstituționale (Consiliul interinstituțional pentru securitate cibernetică – IICB), care să reunească reprezentanți ai tuturor entităților Uniunii pentru a asigura punerea în aplicare corespunzătoare a regulamentului;

   – introducerea obligației entităților Uniunii de a face schimb de informații (neclasificate) cu CERT-UE cu privire la incidente și de a raporta amenințări, vulnerabilități și incidente semnificative și

   – promovarea coordonării și a cooperării ca răspuns la incidente semnificative.

3. Parlamentul European a numit-o pe dna Henna Virkkunen (PPE) în calitatea de raportor al comisiei competente ITRE. Proiectul de raport a fost publicat la 7 octombrie 2022.

4. Autoritatea Europeană pentru Protecția Datelor și-a dat avizul la 17 mai 2022[3].

[2] 6722/21.
[3] 9252/22.

5. La nivelul Consiliului, examinarea propunerii în cadrul Grupului de lucru orizontal pentru chestiuni cibernetice (HWPCI) a început în timpul președinției franceze, la 29 martie 2022. Președinția franceză a pregătit primul text de compromis, discutat în cadrul HWPCI în iunie 2022, și a prezentat Consiliului un raport intermediar[4] la 21 iunie 2022.

6. În timpul președinției cehe, HWPCI a dedicat opt reuniuni[5] discuțiilor cu privire la propunere și la mai multe texte de compromis consecutive.

7. La 23 mai 2022, președinția a solicitat un aviz din partea Comitetului de securitate al Consiliului (CSC) cu privire la aspectele propunerii referitoare la securitatea informațiilor și, în special, la informațiile clasificate. CSC și-a dat avizul la 19 septembrie 2022[6]. Astfel cum a sugerat CSC, informațiile UE clasificate au fost excluse în mod explicit din domeniul de aplicare al regulamentului. Dispozițiile referitoare la derogările de la obligațiile de partajare și raportare legate de informațiile primite din afara entităților Uniunii au fost modificate în consecință.

8. La 28 octombrie 2022, HWPCI a ajuns la un acord cu privire la compromisul președinției care figurează în anexă.

---

4 9719/22.
5 6 și 20 iulie, 13, 21 și 28 septembrie, 5, 19 și 28 octombrie 2022.
6 12603/22 + COR 1.

PRINCIPALELE CHESTIUNI

9. Statele membre au salutat propunerea ca fiind oportună și complementară viitoarei Directive privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2) și au sprijinit obiectivele generale ale acesteia. Totuși, statele membre au solicitat alinieri suplimentare la NIS 2, un grad mai mare de reciprocitate în ceea ce privește schimbul de informații dintre entitățile Uniunii și statele membre și au subliniat caracterul excesiv de voluntar al unora dintre măsurile propuse. Statele membre și-au exprimat, de asemenea, preferința pentru eliminarea trimiterilor la unitatea cibernetică comună, ale cărei mandat și componență nu sunt încă definite.

10. Pe baza discuțiilor din cadrul HWPCI, următoarele puncte au fost identificate drept principalele chestiuni politice:

a) Alinierea la viitoarea Directivă NIS 2

Astfel cum au solicitat statele membre, au fost efectuate alinieri suplimentare la viitoarea Directivă NIS 2, printre care:

- o serie de definiții (articolul 3) au fost aliniate la cele din NIS 2;
- a fost introdus un nou articol 7a privind evaluările inter pares voluntare, în concordanță cu NIS 2, astfel cum a fost adaptat la nevoile entităților Uniunii;
- obligațiile de raportare de la articolul 20 au fost aliniate la cele din NIS 2.

b) Componența Consiliului interinstituțional pentru securitate cibernetică (IICB) (articolul 9)

În urma discuțiilor privind implicarea adecvată a reprezentanților statelor membre în lucrările IICB, s-a ajuns la un compromis prin intermediul unei declarații a Consiliului consemnate în procesul-verbal.

c) Autonomia instituțională

S-a ajuns la o abordare echilibrată între dorința statelor membre de a consolida mecanismele de asigurare a conformității și necesitatea de a respecta principiul autonomiei instituționale, în special în ceea ce privește auditurile și măsurile disciplinare (articolul 11).

În cele din urmă, trimiterea la un anumit procent din bugetul în domeniul tehnologiei informației dedicat securității cibernetice a fost eliminată din considerentul 8.

CONCLUZIE

11. Comitetul Reprezentanților Permanenți este invitat:

(a) să aprobe textul de compromis prevăzut în anexă, care va constitui apoi mandatul de negociere cu Parlamentul European;

(b) să invite Consiliul să aprobe textul de compromis prevăzut în anexă în cadrul reuniunii sale din 18 noiembrie 2022 și să consemneze în procesul-verbal declarația Consiliului care figurează în addendumul la prezentul document.

ANEXĂ

2022/0085 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 298,

având în vedere Tratatul de instituire a Comunității Europene a Energiei Atomice, în special articolul 106a,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) În era digitală, tehnologia informației și comunicațiilor este o piatră de temelie a unei administrații deschise, eficiente și independente a Uniunii. Evoluția tehnologiei și creșterea gradului de complexitate și de interconectare a sistemelor digitale amplifică riscurile de securitate cibernetică, făcând administrația Uniunii mai vulnerabilă la amenințările și incidentele cibernetice, care reprezintă, în cele din urmă, amenințări la adresa continuității activității administrației și a capacității acesteia de a-și securiza datele. Deși utilizarea sporită a serviciilor de tip cloud computing, utilizarea ubicuă a tehnologiei informației, nivelul ridicat de digitalizare, munca la distanță și evoluția tehnologiei și a conectivității sunt, în prezent, caracteristici esențiale ale tuturor activităților entităților administrative ale Uniunii, reziliența digitală nu este încă suficient integrată.

(2) Peisajul amenințărilor cibernetice cu care se confruntă [...] **entitățile** Uniunii este într-o continuă evoluție. Tacticile, tehnicile și procedurile utilizate de actorii care generează amenințări sunt într-o continuă evoluție, în timp ce principalele motive ale acestor atacuri se schimbă foarte puțin, de la furtul de informații confidențiale valoroase până la generarea de profit, manipularea opiniei publice sau subminarea infrastructurii digitale. Ritmul în care își desfășoară atacurile cibernetice continuă să crească, în timp ce campaniile lor sunt din ce în ce mai sofisticate și automatizate, vizând suprafețe de atac expuse care continuă să se extindă și exploatând rapid vulnerabilitățile.

(3) Mediile informatice ale [...] **entităților** Uniunii au interdependențe și fluxuri de date integrate, iar utilizatorii acestora colaborează îndeaproape. Această interconectare înseamnă că orice perturbare, chiar și atunci când este limitată inițial la o [...] **entitate** a Uniunii, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea impacturi negative de amploare și de lungă durată asupra celorlalte. În plus, mediile informatice ale anumitor [...] **entități ale Uniunii** sunt conectate cu cele ale statelor membre, ceea ce face ca un incident în cadrul unei entități a Uniunii să reprezinte un risc de securitate cibernetică a mediilor informatice ale statelor membre și viceversa. **În plus, entitățile Uniunii gestionează volume mari de informații adesea sensibile din partea statelor membre și, prin urmare, incidentele ar putea afecta în mod negativ și statele membre. Din acest motiv, securitatea cibernetică a entităților Uniunii este de o importanță deosebită și pentru statele membre. Informațiile referitoare la incidente pot, de asemenea, facilita detectarea amenințărilor sau a incidentelor cibernetice similare care afectează statele membre.**

(4) [...] **Entitățile** Uniunii sunt ținte atractive, care se confruntă cu actori care generează amenințări cu înaltă calificare și care dispun de resurse suficiente, precum și cu alte amenințări. În același timp, nivelul și maturitatea rezilienței cibernetice și capacitatea de a detecta și de a răspunde activităților cibernetice răuvoitoare variază semnificativ între aceste entități. Prin urmare, pentru buna funcționare a administrației europene este necesar ca [...] **entitățile** Uniunii să atingă un nivel comun ridicat de securitate cibernetică prin **punerea în aplicare a unor măsuri de securitate cibernetică,** [...] prin schimbul de informații și colaborarea în acest domeniu.

(5) [Propunerea de directivă] NIS 2 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune urmărește să îmbunătățească și mai mult capacitatea de reziliență în materie de securitate cibernetică și capacitatea de răspuns la incidente de securitate cibernetică ale entităților publice și private, ale autorităților și organelor naționale competente, precum și ale Uniunii în ansamblu. Prin urmare, este necesar ca [...] **entitățile** Uniunii să urmeze exemplul prin asigurarea unor norme care să fie coerente cu [propunerea de directivă] NIS 2 și să reflecte nivelul său de ambiție.

(6) Pentru a atinge un nivel comun ridicat de securitate cibernetică, este necesar ca fiecare [...] **entitate** a Uniunii să instituie un cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică, care să asigure o gestionare eficace și prudentă a tuturor riscurilor de securitate cibernetică [...]. **Cadrul ar trebui să stabilească politici de securitate cibernetică, inclusiv proceduri de evaluare a eficacității măsurilor de securitate cibernetică puse în aplicare. Cadrul ar trebui să se bazeze pe o abordare multirisc, care vizează protejarea rețelelor și a sistemelor informatice și a mediului fizic al acestor sisteme împotriva unor evenimente precum furtul, incendiile, inundațiile, penele serviciilor de telecom sau de electricitate, ori împotriva accesului fizic neautorizat și a daunelor și intruziunii la nivelul informațiilor deținute de entitatea Uniunii sau al echipamentelor acesteia de prelucrare a informațiilor, care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise, prelucrate sau accesibile prin intermediul rețelelor și al sistemelor informatice. Cadrul ar trebui să reflecte constatările analizei riscurilor, ținând seama de toate riscurile tehnice, operaționale și organizaționale relevante pentru securitatea cibernetică a entității Uniunii în cauză.**

(6a) Pentru a gestiona riscurile identificate în cadru, fiecare entitate a Uniunii ar trebui să se asigure că se iau măsuri tehnice, operaționale și organizaționale adecvate și proporționale. Acestea ar trebui să abordeze domeniile, inclusiv măsurile de securitate cibernetică prevăzute în prezentul regulament pentru a consolida securitatea cibernetică a fiecărei entități a Uniunii.

(6b) **Activele și riscurile identificate în cadru, precum și concluziile care decurg din evaluările periodice ale nivelului de maturitate ar trebui să se reflecte în planul de securitate cibernetică stabilit de fiecare entitate a Uniunii. Planul de securitate cibernetică ar trebui să includă măsurile de securitate cibernetică adoptate, cu scopul de a spori securitatea cibernetică generală a entității Uniunii în cauză.**

(6c) **Întrucât asigurarea securității cibernetice este un proces continuu, caracterul adecvat și eficacitatea tuturor măsurilor ar trebui revizuite periodic având în vedere riscurile, activele și maturitatea în schimbare ale entităților Uniunii. Cadrul ar trebui evaluat periodic și cel puțin o dată la trei ani, în timp ce planul de securitate cibernetică ar trebui revizuit cel puțin o dată la doi ani sau în urma fiecărei evaluări a nivelului de maturitate ori a fiecărei revizuiri a cadrului.**

(6d) **Entitățile Uniunii ar trebui să facă schimb de informații relevante în mod regulat, inclusiv în ceea ce privește incidentele și amenințările cibernetice relevante, asigurând totodată confidențialitatea și protecția adecvată a informațiilor furnizate de entitatea Uniunii raportoare.**

(6e) **Ar trebui pus în aplicare un mecanism care să asigure eficacitatea schimbului de informații, a coordonării și a cooperării entităților Uniunii în cazul unor incidente majore, inclusiv o identificare clară a rolurilor și a responsabilităților entităților Uniunii implicate. Punctul de contact desemnat pentru EU-CyCLONe ar trebui să țină seama de informațiile partajate atunci când face schimb de informații relevante cu EU-CyCLONe, drept contribuție la conștientizarea comună a situației.**

(7) Diferențele dintre [...] **entitățile** Uniunii necesită o anumită flexibilitate în ceea ce privește punerea în aplicare, deoarece nu există o abordare universală. Măsurile pentru un nivel comun ridicat de securitate cibernetică nu ar trebui să includă nicio obligație care să interfereze în mod direct cu exercitarea misiunilor [...] **entităților** Uniunii sau să aducă atingere autonomiei lor instituționale. Astfel, aceste [...] **entități ale Uniunii** ar trebui să își stabilească propriile cadre pentru gestionarea, guvernanța și controlul riscurilor de securitate cibernetică **și propriile planuri de securitate cibernetică** și să adopte [...] **măsuri** [...] de securitate cibernetică. **La punerea în aplicare a unor astfel de măsuri, ar trebui să se țină seama în mod corespunzător de sinergiile existente între entitățile Uniunii, în scopul gestionării adecvate a resurselor și al optimizării costurilor. De asemenea, ar trebui să se țină seama în mod corespunzător de faptul că măsurile nu afectează în mod negativ operațiunile entităților Uniunii și schimbul eficient de informații al acestora cu alte entități ale Uniunii și cu autoritățile naționale competente.**

(8) Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra [...] **entităților** Uniunii, cerințele de gestionare a riscurilor de securitate cibernetică ar trebui să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. Fiecare [...] **entitate** a Uniunii ar trebui să urmărească alocarea unui procent adecvat din bugetul său în domeniul tehnologiei informației pentru a-și îmbunătăți nivelul de securitate cibernetică [...]. **În evaluarea nivelului de maturitate ar trebui, de asemenea, să se aprecieze dacă cheltuielile entității Uniunii în materie de securitate cibernetică sunt proporționale cu riscurile cu care se confruntă.**

(9) Pentru asigurarea unui nivel comun ridicat de securitate cibernetică, aceasta trebuie să se afle sub supravegherea celui mai înalt nivel de conducere al fiecărei [...] **entități** a Uniunii. [...] **Cel mai înalt nivel de conducere ar trebui să supravegheze punerea în aplicare a prezentului regulament, inclusiv stabilirea cadrului de gestionare, guvernanță și control al riscurilor și a planurilor de securitate cibernetică, care să cuprindă măsuri de securitate cibernetică.** Abordarea culturii securității cibernetice, adică practica zilnică în domeniul securității cibernetice, este parte integrantă a unui [...] **cadru** de securitate cibernetică în toate [...] **entitățile** Uniunii.

(10) [...] [...] Măsurile **de securitate cibernetică** ar trebui să facă parte din [...] **planul** de securitate cibernetică și să fie detaliate în documentele de orientare sau în recomandările emise de CERT-UE. La definirea măsurilor și a orientărilor ar trebui să se țină seama în mod corespunzător de **evoluțiile de ultimă oră și, după caz, de standardele europene și internaționale relevante, precum și** de legislația și politicile relevante ale UE, inclusiv de evaluările riscurilor și de recomandările emise de Grupul de cooperare privind securitatea rețelelor și a informațiilor, cum ar fi evaluarea coordonată la nivelul UE a riscurilor de securitate cibernetică aferente rețelelor 5G și setul de instrumente al UE pentru securitatea cibernetică a rețelelor 5G. În plus, ar putea fi necesară certificarea produselor, a serviciilor și a proceselor TIC relevante, în cadrul sistemelor europene specifice de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881. **După caz, CERT-UE ar trebui să coopereze cu ENISA.**

(11) În mai 2011, secretarii generali ai instituțiilor și organelor Uniunii au decis să constituie o echipă de preconfigurare a unui centru de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE), supervizată de un comitet director interinstituțional. În iulie 2012, secretarii generali au confirmat modalitățile practice și au convenit să mențină CERT-UE ca entitate permanentă, pentru a contribui în continuare la îmbunătățirea nivelului general de securitate a tehnologiei informației la nivelul instituțiilor, organelor și agențiilor Uniunii, ca exemplu de cooperare interinstituțională vizibilă în domeniul securității cibernetice. În septembrie 2012, CERT-UE a fost înființat ca grup operativ al Comisiei Europene, cu un mandat interinstituțional. În decembrie 2017, instituțiile și organele Uniunii au încheiat un acord interinstituțional privind organizarea și funcționarea CERT-UE[7]. Prezentul [...] **regulament** ar trebui [...] **să ofere un set cuprinzător de norme privind organizarea, funcționarea și exploatarea CERT-UE. Dispozițiile prezentului regulament prevalează asupra dispozițiilor acordului interinstituțional privind organizarea și funcționarea CERT-UE, care a fost încheiat în decembrie 2017.**

[...]

[7] JO C 12, 13.1.2018, p. 1–11.

(13) Multe atacuri cibernetice fac parte din campanii mai ample care vizează grupuri de [...] **entități** ale Uniunii sau comunități de interes care includ [...] **entități** ale Uniunii. Pentru a permite detectarea proactivă, răspunsul la incidente sau măsurile de atenuare, [...] **entitățile** Uniunii ar trebui să informeze CERT-UE cu privire la amenințările cibernetice [...], vulnerabilitățile [...]**, incidentele evitate la limită și** incidentele propriu-zise [...] și să facă schimb de detalii tehnice adecvate care să permită detectarea sau atenuarea amenințărilor cibernetice, **a vulnerabilităților, a incidentelor evitate la limită și** a incidentelor propriu-zise similare în alte [...] **entități** ale Uniunii, precum și răspunsul la astfel de amenințări, vulnerabilități, incidente evitate la limită și incidente propriu-zise. Urmând aceeași abordare precum cea prevăzută în [propunerea de directivă] NIS 2, în cazul în care iau cunoștință de un incident semnificativ, entitățile **Uniunii** ar trebui să transmită CERT-UE o [...] **alertă timpurie** în termen de 24 de ore. Acest schimb de informații ar trebui să permită CERT-UE să disemineze informațiile către alte [...] **entități** ale Uniunii, precum și către omologii corespunzători, pentru a contribui la protejarea mediilor informatice ale Uniunii și ale omologilor Uniunii împotriva unor incidente [...] similare.

(13a) **Prezentul regulament stabilește o abordare în mai multe etape a raportării incidentelor semnificative pentru a se ajunge la un echilibru adecvat între, pe de o parte, raportarea rapidă care contribuie la atenuarea unei eventuale răspândiri a incidentelor semnificative și le permite entităților Uniunii să solicite asistență și, pe de altă parte, raportarea aprofundată, care permite extragerea unor învățăminte valoroase din incidentele individuale și îmbunătățește în timp reziliența cibernetică a entităților Uniunii la nivel individual. În această privință, prezentul regulament ar trebui să includă raportarea incidentelor care, pe baza unei evaluări inițiale efectuate de entitatea Uniunii, ar putea cauza perturbări operaționale grave ale funcționării entității Uniunii sau pierderi financiare pentru entitatea Uniunii în cauză sau ar putea afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau morale considerabile. O astfel de evaluare inițială ar trebui să ia în considerare, printre altele, rețelele și sistemele informatice afectate, în special importanța acestora pentru funcționarea entității Uniunii, gravitatea și caracteristicile tehnice ale unei amenințări cibernetice și orice vulnerabilități subiacente care sunt exploatate, precum și experiența entității Uniunii în ceea ce privește incidente similare. Indicatori precum măsura în care este afectată funcționarea entității Uniunii, durata unui incident sau numărul de persoane fizice sau juridice afectate ar putea juca un rol important în identificarea nivelului de gravitate a perturbării operaționale.**

(13b) **Întrucât infrastructura și rețelele entității Uniunii relevante și ale statului membru în care este situată entitatea Uniunii sunt interconectate, este esențial ca statul membru respectiv să fie informat fără întârzieri nejustificate cu privire la un incident semnificativ în cadrul entității Uniunii respective. În acest scop, entitatea Uniunii afectată ar trebui să-l informeze pe omologul național al CERT-UE, desemnat de statul membru în conformitate cu [propunerea de directivă] NIS 2, în același termen în care ar trebui să raporteze CERT-UE un incident semnificativ. CERT-UE ar trebui, de asemenea, să-l informeze pe acest omolog național atunci când ia cunoștință de un incident semnificativ produs în statul membru, cu excepția cazului în care a fost deja raportat de entitatea Uniunii afectată.**

(14) Pe lângă atribuirea mai multor sarcini și a unui rol extins pentru CERT-UE, ar trebui instituit un Consiliu interinstituțional pentru securitate cibernetică (IICB), care**, pentru a facilita un nivel comun ridicat de securitate cibernetică în rândul entităților Uniunii,** ar trebui **să aibă un rol exclusiv** [...] [...] **în ceea ce privește** monitorizarea punerii în aplicare a prezentului regulament de către [...] **entitățile** Uniunii și [...] î**n ceea ce privește** supravegherea punerii în aplicare a priorităților și a obiectivelor generale de către CERT-UE și elaborarea unor orientări strategice pentru CERT-UE. IICB ar trebui**, prin urmare,** să asigure reprezentarea instituțiilor și să includă reprezentanți ai agențiilor și ai organelor prin intermediul Rețelei agențiilor UE. **Organizarea și funcționarea IICB ar trebui să fie reglementate în continuare de regulamentul său intern de procedură, care poate include precizări suplimentare privind reuniunile periodice ale IICB, inclusiv reuniunile anuale la nivel politic, în cadrul cărora reprezentanții de la cel mai înalt nivel de conducere al fiecărui membru al IICB ar permite IICB să poarte discuții strategice și să ofere orientări strategice pentru IICB. În plus, IICB poate institui un comitet executiv care să îi ofere asistență în activitatea sa și poate să îi delege unele dintre sarcinile și competențele sale, în special în ceea ce privește sarcinile care necesită** [...] **expertiza specifică a membrilor săi, de exemplu aprobarea catalogului de servicii și orice actualizări ulterioare ale acestuia, modalitățile de încheiere a acordurilor privind nivelul serviciilor, evaluările documentelor și rapoartelor transmise de entitățile Uniunii către IICB în conformitate cu prezentul regulament sau sarcinile legate de pregătirea deciziilor privind măsurile de conformitate emise de IICB și de monitorizarea punerii lor în aplicare. IICB ar trebui să stabilească regulamentul de procedură al comitetului executiv, inclusiv sarcinile și competențele acestuia.**

(15) CERT-UE ar trebui să sprijine punerea în aplicare a măsurilor pentru un nivel comun ridicat de securitate cibernetică prin propuneri de documente de orientare și recomandări adresate IICB sau prin adresarea unor apeluri la acțiune. Astfel de documente de orientare și recomandări ar trebui să fie aprobate de IICB. Atunci când este necesar, CERT-UE ar trebui să adreseze apeluri la acțiune care să descrie măsurile urgente de securitate pe care [...] **entitățile** Uniunii sunt îndemnate să le adopte într-un termen stabilit. **IICB poate solicita CERT-UE să emită, să retragă sau să modifice o propunere de document de orientare sau de recomandare sau un apel la acțiune.**

(16) IICB ar trebui să monitorizeze respectarea prezentului regulament, precum și punerea în aplicare a documentelor de orientare, a recomandărilor și a apelurilor la acțiune [...]. În ceea ce privește aspectele tehnice, IICB ar trebui să beneficieze de sprijin din partea grupurilor consultative tehnice, a căror componență este decisă de IICB și care ar trebui să lucreze în strânsă cooperare cu CERT-UE, cu [...] **entitățile** Uniunii și cu alte părți interesate, după caz. [...] **În cazul în care constată că entitățile Uniunii nu au transpus sau pus în aplicare prezentul regulament, inclusiv documentele de orientare, recomandările sau apelurile la acțiune emise în temeiul prezentului regulament, IICB poate, fără a aduce atingere procedurilor interne ale entității Uniunii relevante, să ia măsuri de asigurare a conformității. Sistemul de măsuri de asigurare a conformității ar trebui să fie utilizat pe niveluri progresive de gravitate, ceea ce înseamnă că, atunci când adoptă măsurile de asigurare a conformității, IICB ar trebui să înceapă cu o avertisment drept măsura cea mai puțin severă și, dacă este necesar, să ajungă până la cea mai severă măsură de emitere a unei alerte prin care recomandă suspendarea temporară a fluxurilor de date către entitatea Uniunii în cauză, care s-ar aplica în cazuri excepționale de nerespectare pe termen lung, deliberată și/sau gravă de către entitatea în cauză a obligației care îi revine în temeiul prezentului regulament.**

(16a) **Avertismentul reprezintă măsura de asigurare a conformității cea mai puțin severă care abordează deficiențele identificate ale entității Uniunii și cuprinde recomandări de modificare a documentelor sale privind securitatea cibernetică, într-un interval de timp specificat. Avertismentul ar trebui să fie la dispoziția tuturor entităților Uniunii, cu excepția cazului în care este restricționat în mod corespunzător în conformitate cu prezentul regulament.**

(16b) **În plus, IICB poate recomanda efectuarea unui audit al unei entități a Uniunii. Entitatea Uniunii își poate utiliza funcția de audit intern în acest scop. De asemenea, IICB ar putea solicita efectuarea unui audit de către un serviciu de audit terț, inclusiv din partea unui furnizor de servicii din sectorul privat convenit de comun acord.**

(16c) **Pe baza rezultatelor unui audit efectuat la recomandarea sau la cererea IICB, acesta poate solicita, de asemenea, entității Uniunii să asigure punerea în conformitate a gestionării, guvernanței și controlului riscurilor de securitate cibernetică cu dispozițiile prezentului regulament.**

(16d) **Întrucât statele membre partajează cu entitățile Uniunii relevante informații care pot avea un caracter sensibil, securitatea cibernetică a destinatarului acestor informații este esențială pentru statele membre. Prin urmare, în cazuri excepționale de neîndeplinire pe termen lung, deliberată, repetată și/sau gravă a obligației entității Uniunii, IICB poate emite, ca măsură de ultimă instanță, o alertă pentru toate statele membre și entitățile Uniunii, prin care recomandă suspendarea temporară a fluxurilor de date către entitatea Uniunii în cauză, care ar trebui să fie în vigoare până la remedierea situației securității cibernetice a acestei entități. Această alertă ar trebui comunicată tuturor statelor membre și entităților Uniunii prin canale de comunicare securizate adecvate.**

(16e) **Pentru a asigura punerea în aplicare corectă a prezentului regulament, în cazul în care consideră că o încălcare continuă a prezentului regulament de către o entitate a Uniunii a fost cauzată direct de acțiunile sau omisiunea unui membru al personalului său, inclusiv la cel mai înalt nivel de conducere, IICB ar trebui să solicite entității Uniunii în cauză să ia măsuri adecvate împotriva membrului respectiv al personalului, în conformitate cu Statutul funcționarilor, precum și cu alte norme echivalente aplicabile în anumite entități ale Uniunii. Aceste acțiuni pot include, de exemplu, proceduri disciplinare și, după caz, în situația specifică a agențiilor Uniunii, o cerere adresată autorității competente de a lua măsurile necesare în legătură cu posibila demitere din funcție a persoanei care ar putea fi responsabilă de încălcarea continuă a prezentului regulament.**

(17) CERT-UE ar trebui să aibă misiunea de a contribui la securitatea mediului informatic al tuturor [...] **entităților** Uniunii. **Atunci când analizează dacă să ofere consiliere tehnică sau contribuții cu privire la chestiuni de politică relevante la cererea unei entități a Uniunii, CERT-UE ar trebui să se asigure că acest lucru nu împiedică îndeplinirea celorlalte sarcini care îi revin în temeiul prezentului regulament.**

(17a) CERT-UE ar trebui să acționeze ca echivalent al coordonatorului desemnat pentru [...] **entitățile** Uniunii, în scopul divulgării coordonate a vulnerabilităților către registrul european al vulnerabilităților, astfel cum se menționează la articolul 6 din [propunerea de directivă] NIS 2 **și ar trebui să elaboreze o politică privind gestionarea vulnerabilităților, care să includă promovarea și facilitarea divulgării coordonate voluntare a vulnerabilităților.**

[...]

(19) De asemenea, CERT-UE ar trebui să își îndeplinească rolul prevăzut în [propunerea de directivă] NIS 2 privind cooperarea și schimbul de informații cu rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT). În plus, în concordanță cu Recomandarea (UE) 2017/1584 a Comisiei[8], CERT-UE ar trebui să coopereze și să se coordoneze cu părțile interesate relevante în privința răspunsului. Pentru a contribui la un nivel ridicat de securitate cibernetică în întreaga Uniune, CERT-UE ar trebui să facă schimb de informații referitoare la incidente cu omologii naționali. CERT-UE ar trebui, de asemenea, să colaboreze cu alți omologi din sectorul public și privat, inclusiv din cadrul NATO, sub rezerva aprobării prealabile de către IICB.

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

(20) În sprijinirea securității cibernetice operaționale, CERT-UE ar trebui să utilizeze expertiza de care dispune Agenția Uniunii Europene pentru Securitate Cibernetică **(ENISA)** prin intermediul unei cooperări structurate, astfel cum se prevede în Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[9]. Dacă este cazul, între cele două entități ar trebui încheiate acorduri specifice pentru a se stabili modalitățile practice de punere în aplicare a acestei cooperări și pentru a se evita suprapunerea activităților. CERT-UE ar trebui să coopereze cu [...] **ENISA** în ceea ce privește analiza amenințărilor și să transmită agenției în mod regulat raportul său privind situația amenințărilor.

[...]

(22) **Activitățile CERT-UE și gestionarea de către CERT-UE a informațiilor în temeiul prezentului regulament pot implica prelucrarea de date cu caracter personal.** Toate datele cu caracter personal prelucrate în temeiul prezentului regulament ar trebui prelucrate în conformitate cu legislația privind protecția datelor, inclusiv cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[10]. **În cazul în care, în temeiul prezentului regulament, se transmit date cu caracter personal altor destinatari stabiliți în Uniune decât entitățile Uniunii, acest lucru ar trebui să se facă în conformitate cu articolul 9 din Regulamentul (UE) 2018/1725.**

---

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

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

(23) CERT-UE și [...] **entitățile** Uniunii ar trebui să gestioneze informațiile în concordanță cu normele **aplicabile** [...] privind securitatea informațiilor[...]. [...]

(23a) În scopul schimbului de informații, se utilizează marcaje vizibile pentru a indica faptul că destinatarii informațiilor trebuie să aplice limite de partajare pe baza, în special, a unor acorduri de nedivulgare sau a unor acorduri informale de nedivulgare cum ar fi protocolul TLP („Traffic Light Protocol") sau alte indicații clare din partea sursei. Protocolul TLP trebuie înțeles drept mijloc de a furniza informații cu privire la orice limitări în ceea ce privește răspândirea ulterioară a informațiilor. Este utilizat în aproape toate echipele de intervenție în caz de incidente de securitate informatică (CSIRT) și în unele centre de analiză și schimb de informații.

(24) **Prezentul regulament și noile sarcini alocate CERT-UE nu vor avea niciun efect asupra cheltuielilor totale în temeiul cadrului financiar multianual.** Întrucât serviciile și sarcinile CERT-UE sunt în interesul tuturor [...] **entităților** Uniunii, fiecare [...] **entitate** a Uniunii cu cheltuieli în domeniul tehnologiei informației ar trebui să contribuie în mod echitabil la aceste servicii și sarcini. Contribuțiile respective nu aduc atingere autonomiei bugetare a [...] **entităților** Uniunii. **Toate entitățile Uniunii și administrațiile acestora ar trebui să asigure optimizarea resurselor lor la nivelul actual și să consolideze creșterea eficienței, inclusiv prin aprofundarea cooperării interinstituționale în domeniul securității cibernetice. Prin urmare, ar trebui privilegiată o abordare comună privind punerea în comun a cheltuielilor administrative în raport cu cheltuielile individualizate ale entităților Uniunii.**

(25) IICB, cu sprijinul CERT-UE, ar trebui să revizuiască și să evalueze punerea în aplicare a prezentului regulament și ar trebui să raporteze constatările sale Comisiei. Pe baza acestei contribuții, Comisiei ar trebui să transmită rapoarte Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor. **În plus, Curtea de Conturi Europeană este invitată să evalueze periodic funcționarea CERT-UE.**

ADOPTĂ PREZENTUL REGULAMENT:

Capitolul I
DISPOZIȚII GENERALE

Articolul 1

Obiect

(1) Prezentul regulament stabilește **măsuri care vizează atingerea unui nivel comun ridicat de securitate cibernetică în cadrul entităților Uniunii** [...]

(2) În acest scop, prezentul regulament stabilește:

(c) obligații pentru [...] **fiecare entitate** a Uniunii de a institui **un** cadru [...] de gestionare, guvernanță și control al riscurilor de securitate cibernetică;

(d) obligații de gestionare a riscurilor de securitate cibernetică [...]**,** de raportare **și de schimb de informații** pentru [...] **entitățile** Uniunii;

(e) norme privind organizarea**, funcționarea** și operarea [...] **Centrului interinstituțional autonom de răspuns la incidente de securitate cibernetică** pentru [...] **entitățile** Uniunii (CERT-UE) și privind organizarea**, funcționarea** și operarea Consiliului interinstituțional pentru securitate cibernetică **(IICB)**;

(f) norme referitoare la monitorizarea punerii în aplicare a prezentului regulament.

Articolul 2

Domeniul de aplicare

(1) Prezentul regulament se aplică [...] tuturor [...] **entităților** Uniunii și [...] [...] CERT-UE și **IICB** [...].

(2) Prezentul regulament se aplică fără a aduce atingere autonomiei instituționale în temeiul tratatelor.

(3) Cu excepția articolului 12 alineatul (7), prezentul regulament nu se aplică rețelelor și sistemelor informatice care gestionează informații UE clasificate (IUEC).

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „[...] **entități** ale Uniunii” înseamnă instituțiile, organele**, oficiile** și agențiile Uniunii înființate prin Tratatul privind Uniunea Europeană, Tratatul privind funcționarea Uniunii Europene sau Tratatul de instituire a Comunității Europene a Energiei Atomice sau în temeiul acestora;

2. „rețea și sistem informatic” înseamnă rețea și sistem informatic [...] **astfel cum sunt definite la** articolul 4 punctul 1 din [propunerea de directivă] NIS 2;

3. „securitatea rețelelor și a sistemelor informatice” înseamnă securitatea rețelelor și a sistemelor informatice [...] **astfel cum este definită la** articolul 4 punctul 2 din [propunerea de directivă] NIS 2;

4. „securitate cibernetică” înseamnă securitate cibernetică **astfel cum este definită la articolul 2 punctul 1 din Regulamentul (UE) 2019/881**;

5. „cel mai înalt nivel de conducere” înseamnă un manager, un organ de conducere sau de coordonare și supraveghere de la cel mai înalt nivel administrativ **cu capacități decizionale**, ținând seama de mecanismele de guvernanță la nivel înalt din fiecare [...] **entitate** a Uniunii;

5a. „incident evitat la limită” înseamnă un incident evitat la limită astfel cum este definit la articolul 4 punctul 4a din [propunerea de directivă] NIS 2;

6. „incident” înseamnă un incident [...] **astfel cum este definit la** articolul 4 punctul 5 din [propunerea de directivă] NIS 2;

[...]

8. „[...] **incident** major” înseamnă orice incident **care cauzează un nivel de perturbare care depășește capacitatea unei entități a Uniunii și a CERT-UE de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două entități ale Uniunii**; [...]

9. „administrare a incidentelor” înseamnă administrarea incidentelor [...] **astfel cum este definită la** articolul 4 punctul 6 din [propunerea de directivă] NIS 2;

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

[...]

12. „vulnerabilitate” înseamnă vulnerabilitate în sensul articolului 4 punctul 8 din [propunerea de directivă] NIS 2;

[...]

14. „risc [...]” înseamnă **un risc în sensul articolului 4 punctul 7b din [propunerea de directivă] NIS 2** [...];

[...]

[...]

Articolul 3a

Prelucrarea datelor cu caracter personal

1) Prelucrarea datelor cu caracter personal în temeiul prezentului regulament de către CERT-UE, IICB sau entitățile Uniunii se efectuează în conformitate cu Regulamentul (UE) 2018/1725.

2) CERT-UE, IICB și entitățile Uniunii prelucrează și fac schimb de date cu caracter personal în măsura în care este necesar și exclusiv în scopul îndeplinirii obligațiilor care le revin în temeiul prezentului regulament.

Capitolul II
MĂSURI PENTRU UN NIVEL COMUN RIDICAT DE SECURITATE CIBERNETICĂ

Articolul 4

Cadrul de gestionare, guvernanță și control al riscurilor

(1) Fiecare [...] **entitate** a Uniunii își stabilește propriul cadru [...] de gestionare, guvernanță și control al riscurilor de securitate cibernetică (denumit în continuare „cadrul") pentru a sprijini misiunea entității [...]**.** [...] **Cadrul** este supravegheat de cel mai înalt nivel de conducere al entității pentru a se putea asigura o gestionare eficace și prudentă a tuturor riscurilor de securitate cibernetică. Cadrul se instituie până cel târziu la …[15 luni de la intrarea în vigoare a prezentului regulament].

(2) Cadrul acoperă întregul mediu informatic neclasificat al [...] **entității Uniunii** în cauză, inclusiv orice mediu informatic de la fața locului, **rețea tehnologică operațională,** active și servicii externalizate în medii de cloud computing sau găzduite de părți terțe, dispozitive mobile, rețele corporative, rețele organizaționale care nu sunt conectate la internet și orice dispozitive conectate la mediul informatic. Cadrul **se bazează pe o abordare multirisc și pe o evaluare a nivelului de maturitate în conformitate cu articolul 6, acoperind toate riscurile tehnice, operaționale și organizaționale relevante care ar putea avea un impact asupra securității cibernetice a entității Uniunii în cauză.** [...].

(2a) Cadrul stabilește politici de securitate cibernetică, inclusiv obiective și priorități pentru securitatea rețelelor și a sistemelor informatice, precum și politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor de securitate cibernetică puse în aplicare și pentru a defini rolurile și responsabilitățile membrilor personalului.

(2b) Cadrul este revizuit periodic și cel puțin o dată la trei ani, având în vedere riscurile în schimbare, activele și nivelul de maturitate ale entității Uniunii.

(3) Cel mai înalt nivel de conducere din fiecare [...] **entitate** a Uniunii [...] **supraveghează** respectarea de către [...] **propria** organizație a obligațiilor legate de gestionarea, guvernanța și controlul riscurilor de securitate cibernetică, fără a aduce atingere responsabilităților formale ale altor niveluri de conducere în ceea ce privește conformitatea și gestionarea riscurilor în domeniile lor respective de responsabilitate.

(3a) După caz și fără a aduce atingere responsabilității sale pentru punerea în aplicare a prezentului regulament, cel mai înalt nivel de conducere din fiecare entitate a Uniunii poate delega altor înalți funcționari din cadrul entității în cauză obligații specifice în temeiul prezentului regulament. Indiferent de posibila delegare a obligației sale specifice, cel mai înalt nivel de conducere poate fi considerat răspunzător pentru nerespectarea de către entități a obligațiilor care îi revin în temeiul prezentului regulament.

(3b) Cel mai înalt nivel de conducere din fiecare entitate a Uniunii se asigură că entitățile Uniunii aprobă planul de securitate cibernetică care include măsuri de gestionare a riscurilor de securitate cibernetică, în conformitate cu analiza lor de risc, astfel încât cadrul să fie pus în aplicare în conformitate cu prezentul regulament.

[...]

(5) Fiecare [...] **entitate** a Uniunii numește un responsabil local cu securitatea cibernetică sau o funcție echivalentă care acționează ca punct unic de contact în ceea ce privește toate aspectele securității cibernetice.

Responsabilul local cu securitatea cibernetică facilitează punerea în aplicare a prezentului regulament și raportează periodic în mod direct celui mai înalt nivel de conducere cu privire la stadiul punerii în aplicare.

Fără a aduce atingere faptului că responsabilul local cu securitatea cibernetică este punctul unic de contact în fiecare entitate a Uniunii, o entitate a Uniunii poate delega CERT-UE anumite sarcini ale responsabilului local cu securitatea cibernetică în ceea ce privește punerea în aplicare a prezentului regulament, pe baza unui acord privind nivelul serviciilor încheiat între entitatea Uniunii respectivă și CERT-UE. IICB decide dacă furnizarea acestui serviciu face parte din serviciile de referință ale CERT-UE, ținând seama de resursele umane și financiare ale entității Uniunii în cauză. Fiecare entitate a Uniunii comunică CERT-UE fără întârzieri nejustificate responsabilii locali cu securitatea cibernetică numiți și orice modificare ulterioară în acest sens. CERT-UE păstrează o listă actualizată periodic a responsabililor locali cu securitatea cibernetică numiți.

(6) Înalții funcționari în sensul articolului 29 alineatul (2) din Statutul funcționarilor[11] sau alți funcționari de nivel echivalent din fiecare entitate a Uniunii urmează periodic cursuri de formare specifice, pentru a dobândi cunoștințe și competențe suficiente care să le permită să înțeleagă și să evalueze practicile de gestionare a riscurilor de securitate cibernetică, precum și impactul acestora asupra operațiunilor organizației.

---

11 Regulamentul 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, JO L 56, 4.3.1968.

(7) Fiecare entitate a Uniunii dispune de mecanisme eficace pentru a se asigura că un procent adecvat din bugetul în domeniul tehnologiei informației este cheltuit pentru securitatea cibernetică. La definirea acestui procent se ține seama în mod corespunzător de cadru.

Articolul 5

Măsuri de gestionare a riscurilor de securitate cibernetică [...]

(1) [...] **Fiecare entitate a Uniunii, sub supravegherea** celui mai înalt nivel de conducere **al său** [...] [...]**, asigură faptul că se iau măsuri tehnice, operaționale și organizaționale adecvate și proporționale pentru a gestiona riscurile identificate în cadrul menționat la articolul 4 alineatul (1) și pentru a preveni și/sau reduce la minimum impactul incidentelor. Luând în considerare evoluțiile de ultimă oră și, după caz, standardele europene și internaționale relevante, precum și costul punerii în aplicare, măsurile respective asigură un nivel de securitate a rețelelor și a sistemelor informatice adecvat riscurilor prezentate. Atunci când se evaluează proporționalitatea măsurilor respective, se ține seama în mod corespunzător de gradul de expunere a entității la riscuri, de dimensiunea acesteia, de probabilitatea producerii unor incidente și de gravitatea acestora, inclusiv de impactul lor societal și economic.**

[...]

(3) Entitățile Uniunii abordează cel puțin următoarele domenii specifice atunci când implementează măsurile de gestionare a riscurilor de securitate cibernetică în cadrul planurilor lor de securitate cibernetică, în concordanță cu documentele de orientare și recomandările din partea IICB:

(a) politica de securitate cibernetică, în ceea ce privește specificarea instrumentelor și a măsurilor necesare pentru atingerea obiectivelor și a priorităților menționate la articolul 4 și la articolul 5 alineatul (4);

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

(c) organizarea securității cibernetice, inclusiv definirea rolurilor și a responsabilităților;

(d) gestionarea activelor, inclusiv inventarul activelor informatice și cartografierea rețelelor informatice;

(e) securitatea resurselor umane și controlul accesului;

(f) securitatea operațiunilor;

(g) securitatea comunicațiilor;

(h) achiziționarea, dezvoltarea și întreținerea de sisteme, inclusiv gestionarea și divulgarea vulnerabilităților;

(i) securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile dintre fiecare entitate a Uniunii și furnizorii săi direcți sau prestatorul său de servicii. Entitățile Uniunii iau în considerare vulnerabilitățile specifice fiecărui furnizor direct și fiecărui prestator de servicii, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale furnizorilor și prestatorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare;

(j) gestionarea incidentelor și cooperarea cu CERT-UE, cum ar fi monitorizarea și jurnalizarea evenimentelor de securitate;

(k) gestionarea continuității activității, cum ar fi gestionarea sistemelor de backup și recuperarea în caz de dezastru, precum și gestionarea crizelor și

(l) promovarea și dezvoltarea unor programe de educație, competențe, sensibilizare, exerciții și formare în materie de securitate cibernetică.

(4) Entitățile Uniunii abordează cel puțin următoarele măsuri specifice de gestionare a riscurilor de securitate cibernetică atunci când implementează măsurile de gestionare a riscurilor de securitate cibernetică în cadrul planurilor lor de securitate cibernetică, în concordanță cu documentele de orientare și recomandările din partea IICB:

a) obiectivele și prioritățile privind utilizarea serviciilor de cloud computing în sensul articolului 4 punctul 19 din [propunerea de directivă] NIS 2 și modalitățile tehnice care să permită telemunca;

b) pași concreți pentru o viitoare utilizare a principiilor bazate pe modelul de încredere zero, inclusiv un model de securitate, și o strategie coordonată de gestionare a securității cibernetice și a sistemului, bazată pe recunoașterea faptului că există amenințări atât în interiorul, cât și în afara granițelor tradiționale ale rețelei;

c) adoptarea autentificării multifactor ca normă pentru toate rețelele și sistemele informatice;

d) asigurarea securității lanțului de aprovizionare cu software prin criterii de dezvoltare și evaluare securizată a software-ului;

e) consolidarea normelor privind achizițiile publice pentru a facilita un nivel comun ridicat de securitate cibernetică prin:

i) eliminarea barierelor contractuale care limitează schimbul de informații între furnizorii de servicii informatice și CERT-UE cu privire la incidente, vulnerabilități și amenințări cibernetice;

ii) obligația contractuală de a raporta incidentele, vulnerabilitățile și amenințările cibernetice, precum și de a institui măsuri adecvate de răspuns la incidente și de monitorizare a acestora;

f) utilizarea criptografiei și a criptării, în special a criptării de la un capăt la altul;

g) sisteme de comunicații securizate în cadrul organizației.

Articolul 6

Evaluările nivelului de maturitate

1. Fiecare [...] **entitate** a Uniunii**, după caz cu asistența unei părți terțe specializate,** efectuează **o** evaluare a nivelului de maturitate [...] cel puțin o dată la trei ani, încorporând toate elementele mediului său informatic, astfel cum este descris la articolul 4, ținând seama de documentele de orientare și de recomandările relevante adoptate în conformitate cu articolul 13.

2. La recomandarea CERT-UE și după consultarea Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), IICB adoptă, în termen de 4 luni de la intrarea în vigoare a prezentului regulament, orientări metodologice privind efectuarea evaluărilor nivelului de maturitate.

3. După finalizarea evaluării nivelului de maturitate [...]**, entitatea Uniunii o prezintă IICB**. **Prima evaluare a nivelului de maturitate se efectuează cel târziu la [12 luni de la intrarea în vigoare a prezentului regulament].**

Articolul 7

Planurile de securitate cibernetică

1. În urma concluziilor desprinse din evaluarea nivelului de maturitate și luând în considerare activele și riscurile identificate în temeiul articolului 4, cel mai înalt nivel de conducere din fiecare [...] **entitate** a Uniunii aprobă un plan de securitate cibernetică, fără întârzieri nejustificate, după instituirea cadrului [...], [...] **adoptarea măsurilor de gestionare a riscurilor** [...] de securitate cibernetică [...] **și efectuarea evaluării nivelului de maturitate și nu mai târziu de 21 de luni de la intrarea în vigoare a prezentului regulament**. Planul **de securitate cibernetică** vizează creșterea gradului de securitate cibernetică în ansamblu a [...] entității **Uniunii în cauză** și contribuie, astfel, la [...] îmbunătățirea unui nivel comun ridicat de securitate cibernetică în toate [...] **entitățile** Uniunii. [...] Planul **de securitate cibernetică** include cel puțin **măsurile de gestionare a riscurilor de securitate cibernetică în temeiul articolului 5** [...]. Planul **de securitate cibernetică** se revizuiește cel puțin o dată la [...] **doi** ani, **sau** în urma [...] **fiecărei** evaluări a nivelului de maturitate [...] efectuate în temeiul articolului 6 **sau a fiecărei revizuiri a cadrului în temeiul articolului 4.**

2. [...]

3. Planul de securitate cibernetică **ia în considerare** [...] orice documente de orientare și recomandări aplicabile emise **în conformitate cu articolul 13** [...].

4. **După finalizarea planului de securitate cibernetică, entitatea Uniunii îl prezintă IICB.**

Articolul 7a

Evaluarea inter pares

1. La recomandarea CERT-UE și după consultarea ENISA, IICB stabilește, cel târziu la ... [24 de luni de la intrarea în vigoare a prezentului regulament], utilizând metodologia pentru evaluări inter pares și metodologia pentru autoevaluare în conformitate cu articolul 16 din [propunerea de directivă] NIS 2 adaptate acolo unde este necesar la nevoile entităților Uniunii, metodologia și aspectele organizaționale ale unei evaluări inter pares în vederea învățării din experiența comună, a consolidării încrederii reciproce, a atingerii unui nivel comun ridicat de securitate cibernetică, precum și a consolidării capacităților și politicilor de securitate cibernetică ale entităților Uniunii necesare pentru punerea în aplicare a prezentului regulament. Participarea la evaluările inter pares este voluntară. Reprezentanți ai statelor membre pot participa la evaluarea inter pares în calitate de observatori. Evaluările inter pares sunt efectuate de experți în materie de securitate cibernetică desemnați de cel puțin două entități ale Uniunii, diferite de entitățile Uniunii care fac obiectul evaluării, și acoperă cel puțin unul dintre următoarele aspecte:

(i) nivelul punerii în aplicare a măsurilor de gestionare a riscurilor de securitate cibernetică și a obligațiilor de raportare menționate la articolele 5 și 20;

(ii) nivelul capacităților, inclusiv resursele financiare, tehnice și umane disponibile;

(iii) nivelul punerii în aplicare a cadrului privind schimbul de informații, menționat la articolul 19;

(iv) aspecte specifice de natură transsectorială.

2. Entitățile Uniunii pot identifica aspecte specifice menționate la alineatul (1) punctul (iv) care urmează să fie evaluate. Domeniul de aplicare al evaluării, incluzând aspectele identificate, este comunicat entităților Uniunii participante înainte de începerea evaluării inter pares.

3. Înainte de începerea evaluării inter pares, entitățile Uniunii pot efectua o autoevaluare a aspectelor evaluate și pot furniza această autoevaluare experților desemnați.

4. Evaluările inter pares implică vizite la fața locului fizice sau virtuale și schimburi ex situ. Având în vedere principiul bunei cooperări, entitățile Uniunii care fac obiectul evaluării inter pares furnizează experților desemnați informațiile necesare pentru evaluare, fără a aduce atingere legislației naționale sau a Uniunii privind protecția informațiilor sensibile sau clasificate. Orice informații obținute prin intermediul procesului de evaluare inter pares sunt utilizate exclusiv în acest scop. Experții care participă la evaluarea inter pares nu divulgă terților niciun fel de informații sensibile sau clasificate obținute în cursul evaluării respective.

5. Odată ce au făcut obiectul unei evaluări inter pares, aceleași aspecte evaluate în cadrul entităților Uniunii nu fac obiectul unei evaluări inter pares suplimentare în cadrul respectivelor entități ale Uniunii timp de doi ani de la finalizarea evaluării inter pares, cu excepția cazului în care entitățile Uniunii solicită acest lucru sau convin altfel în urma unei propuneri din partea IICB.

6. Entitățile Uniunii se asigură că orice risc de conflict de interese în ceea ce privește experții desemnați este dezvăluit celorlalte entități ale Uniunii și IICB înainte de începerea evaluării inter pares. Entitățile Uniunii care fac obiectul evaluării inter pares pot formula obiecții cu privire la desemnarea anumitor experți, din motive justificate în mod corespunzător, comunicate entităților Uniunii care i-au desemnat.

7. Experții care participă la evaluări inter pares elaborează rapoarte cu privire la constatările și concluziile evaluărilor. Entităților Uniunii li se permite să formuleze observații cu privire la proiectele de rapoarte ale acestora, care se anexează la rapoarte. Rapoartele includ recomandări pentru a permite îmbunătățirea aspectelor care fac obiectul evaluării inter pares. Rapoartele sunt prezentate IICB și rețelei CSIRT, dacă este cazul. Entitățile Uniunii care fac obiectul evaluării pot decide să pună la dispoziția publicului raportul lor sau o versiune ocultată a acestuia.

Articolul 8

Punerea în aplicare

1. [...]

2. Documentele de orientare și recomandările emise în conformitate cu articolul 13 sprijină punerea în aplicare a dispozițiilor prevăzute în prezentul capitol.

3. La cererea IICB, entitățile Uniunii raportează cu privire la aspecte specifice din prezentul capitol.

Capitolul III

CONSILIUL INTERINSTITUȚIONAL PENTRU SECURITATE CIBERNETICĂ

Articolul 9

Consiliul interinstituțional pentru securitate cibernetică

1. Se instituie Consiliul interinstituțional pentru securitate cibernetică (IICB).

2. IICB este responsabil cu:

   (a) monitorizarea punerii în aplicare a prezentului regulament de către [...] **entitățile Uniunii**;

   (b) supravegherea punerii în aplicare a priorităților și obiectivelor generale de către CERT-UE și elaborarea de orientări strategice pentru CERT-UE.

3. IICB este alcătuit din**:**

   a) câte un reprezentant desemnat de fiecare dintre următoarele:

      (i) Parlamentul European;

      (ii) Consiliul European;

      (iii) Consiliul Uniunii Europene;

      (iv) Comisia Europeană;

      (v) Curtea de Justiție a Uniunii Europene;

      (vi) Banca Centrală Europeană;

(vii) Curtea de Conturi Europeană;

(viii) Serviciul European de Acțiune Externă;

(ix) Comitetul Economic Și Social European;

(x) Comitetul European al Regiunilor;

(xi) Banca Europeană de Investiții;

(xii) Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică și

(xiii) Agenția Uniunii Europene pentru Securitate Cibernetică;

b) trei reprezentanți [...] **desemnați** de Rețeaua agențiilor UE (EUAN), la propunerea Comitetului său consultativ pentru tehnologia informației și comunicațiilor, pentru a reprezenta interesele agențiilor și organelor care își gestionează propriul mediu informatic. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

(3a) Membrii pot fi asistați de un supleant. Alți reprezentanți ai [...] **entităților** enumerate mai sus sau ai altor [...] **entități** ale Uniunii pot fi invitați de președinte să participe la reuniunile IICB, fără drept de vot.

4. IICB își adoptă regulamentul intern de procedură.

5. IICB desemnează un președinte din rândul membrilor săi, în conformitate cu regulamentul său intern de procedură, pentru o perioadă de [...] **doi** ani. Supleantul acestuia devine membru titular al IICB pentru aceeași durată.

6. IICB se reunește **cel puțin de trei ori pe an** la inițiativa președintelui său **și/sau** la cererea CERT-UE **și/**sau la cererea oricăruia dintre membrii săi.

7. Fiecare membru al IICB dispune de un vot. Deciziile IICB sunt adoptate cu majoritate simplă, cu excepția cazurilor în care se prevede altfel în prezentul regulament. Președintele votează numai în caz de egalitate de voturi, situație în care poate exprima un vot decisiv.

8. IICB poate acționa printr-o procedură scrisă simplificată inițiată în conformitate cu regulamentul său intern de procedură. În temeiul procedurii respective, decizia relevantă se consideră aprobată în termenul stabilit de președinte, cu excepția cazului în care un membru formulează obiecții.

9. Șeful CERT-UE**, președintele Grupului de cooperare privind securitatea rețelelor și a informațiilor**, **președintele EU-CyCLONe și președintele rețelei CSIRT,** sau supleanții **acestora** [...], [...] **pot** participa la reuniunile IICB, cu excepția cazului în care IICB decide altfel**, în calitate de observatori**.

10. Secretariatul IICB este asigurat de **ENISA** [...] **și răspunde în fața președintelui IICB**.

11. Reprezentanții numiți de Rețeaua agențiilor UE (EUAN), la propunerea Comitetului consultativ pentru tehnologia informației și comunicațiilor, informează [...] **membrii EUAN** cu privire la deciziile adoptate de IICB. Orice agenție și organ al Uniunii are dreptul să abordeze cu reprezentanții sau președintele IICB orice chestiune care, în opinia sa, ar trebui adusă în atenția IICB.

12. [...]

13. IICB poate [...] **institui** un comitet executiv care să îl asiste în activitatea sa și poate să îi delege o parte din sarcinile și competențele sale**, în special cele prevăzute la articolul 10 literele (c) și (e)**. IICB stabilește regulamentul de procedură al comitetului executiv, inclusiv sarcinile și competențele acestuia, precum și mandatul membrilor săi.

14. IICB prezintă Consiliului, o dată la 12 luni, un raport care detaliază progresele înregistrate în ceea ce privește punerea în aplicare a prezentului regulament și care specifică, în special, gradul de cooperare a CERT-UE cu omologii săi naționali în fiecare dintre statele membre. Acest raport constituie o contribuție la raportul bienal privind situația în materie de securitate cibernetică în Uniune în aceeași perioadă de timp, în conformitate cu articolul 15 din [propunerea de directivă] NIS 2.

Articolul 10

Sarcinile IICB

Atunci când își exercită responsabilitățile, IICB realizează, în special, următoarele:

(a) [...] **monitorizează și supraveghează în mod eficace aplicarea** prezentului regulament [...] **si sprijină** [...] **entitățile** Uniunii **în consolidarea securității lor cibernetice**; **în acest scop, IICB poate solicita rapoarte ad-hoc din partea CERT-UE și a entităților Uniunii;**

(**aa**) **în urma unei discuții strategice, adoptă o strategie multianuală privind creșterea nivelului de securitate cibernetică în entitățile Uniunii și o evaluează periodic și cel puțin o dată la cinci ani și, dacă este necesar, o modifică;**

(b) aprobă, pe baza unei propuneri [...] **prezentate de** șeful CERT-UE, programul anual de lucru al CERT-UE și monitorizează punerea în aplicare a acestuia;

(c) aprobă, pe baza unei propuneri din partea șefului CERT-UE, catalogul de servicii al CERT-UE **și orice actualizări ulterioare ale acestuia**;

(d) aprobă, pe baza unei propuneri prezentate de șeful CERT-UE, planificarea financiară anuală a veniturilor și cheltuielilor, inclusiv în ceea ce privește personalul, pentru activitățile CERT-UE;

(e) aprobă, pe baza unei propuneri din partea șefului CERT-UE, modalitățile pentru acordurile privind nivelul serviciilor;

(f) examinează și aprobă raportul anual întocmit de șeful CERT-UE, care cuprinde activitățile CERT-UE și gestionarea fondurilor de către CERT-UE;

(g) aprobă și monitorizează indicatorii-cheie de performanță pentru CERT-UE, definiți pe baza unei propuneri din partea șefului CERT-UE;

(h) aprobă acordurile de cooperare, [...] **acordurile** privind nivelul serviciilor sau contractele dintre CERT-UE și alte entități în temeiul articolului 17;

(i) instituie [...] grupuri consultative tehnice [...] pentru a sprijini activitatea IICB, aprobă mandatul și desemnează președinții acestor grupuri;

(j) **adoptă documente de orientare și recomandări pe baza unei propuneri din partea CERT-UE în conformitate cu articolul 13 și solicită CERT-UE să emită, să retragă sau să modifice o propunere de document de orientare sau de recomandare sau un apel la acțiune;**

(k) primește și evaluează documentele și rapoartele prezentate de entitățile Uniunii în temeiul prezentului regulament;

(l) sprijină instituirea unui grup informal care să reunească responsabilii locali cu securitatea cibernetică ai tuturor entităților și, astfel, facilitează schimbul de bune practici și de informații în legătură cu punerea în aplicare a prezentului regulament;

(m) elaborează un plan de gestionare a crizelor cibernetice pentru a sprijini gestionarea coordonată a incidentelor majore la nivel operațional care afectează entitățile Uniunii și pentru a contribui la schimbul periodic de informații relevante, în special cu privire la impactul și gravitatea incidentelor majore și la posibile modalități de atenuare.

Articolul 11

Asigurarea conformității

(1) **În conformitate cu articolul 9 alineatele (2) și (10),** IICB monitorizează **în mod eficace** punerea în aplicare de către [...] **entitățile** Uniunii a prezentului regulament și a documentelor de orientare, a recomandărilor și a apelurilor la acțiune adoptate. **În acest scop, IICB poate solicita informațiile sau documentele necesare pentru a evalua aplicarea corespunzătoare a dispozițiilor regulamentului de către entitățile Uniunii. În scopul adoptării unor măsuri de asigurare a conformității în temeiul prezentului articol, entitatea Uniunii în cauză nu are drept de vot.**

(2) În cazul în care constată că [...] **entitățile** Uniunii nu au transpus sau pus în aplicare în mod eficace prezentul regulament sau documentele de orientare, recomandările și apelurile la acțiune emise în temeiul prezentului regulament, IICB poate, fără a aduce atingere procedurilor interne ale [...] **entității** Uniunii relevante **și, după ce a oferit entității sau persoanei în cauză posibilitatea de a-și prezenta punctul de vedere**:

(a) să emită un avertisment **în vederea remedierii deficiențelor identificate într-un interval de timp specificat, inclusiv recomandări de modificare a documentelor privind securitatea cibernetică adoptate de entitățile Uniunii în temeiul prezentului regulament**; dacă este necesar, având în vedere un risc semnificativ de securitate cibernetică, categoriile care pot lua cunoștință de avertisment sunt restricționate în mod corespunzător;

(aa) să emită o notificare motivată către o entitate a Uniunii, în cazul în care deficiențele identificate în avertismentul emis anterior nu au fost suficient abordate într-un interval de timp specificat, și să notifice în mod formal avizul respectiv Consiliului, Parlamentului European și Comisiei;

(b) **să emită, în special:** [...]

i. o recomandare de efectuare a unui audit al unei entități a Uniunii;

ii. o cerere privind efectuarea unui audit de către un serviciu de audit terț.

(c) să solicite entității Uniunii să pună în conformitate gestionarea, guvernanța și controlul riscurilor de securitate cibernetică cu dispozițiile prezentului regulament, după caz într-un mod specificat și într-un termen specificat;

(d) să emită o alertă pentru toate statele membre și entitățile Uniunii, prin care recomandă suspendarea temporară a fluxurilor de date către entitatea Uniunii.

(3) În cazul în care IICB a adoptat măsuri în temeiul alineatului (2) literele (a)-(d), entitatea Uniunii în cauză oferă un bilanț detaliat al măsurilor și acțiunilor întreprinse pentru a remedia presupusele deficiențe identificate de IICB. Entitatea Uniunii transmite acest bilanț într-un termen rezonabil care urmează să fie convenit cu IICB.

(4) În cazul în care consideră că există o încălcare continuă a dispozițiilor prezentului regulament de către o entitate a Uniunii, care rezultă direct din acțiunile sau omisiunile unui funcționar sau ale unui alt agent al Uniunii, inclusiv la cel mai înalt nivel de conducere, IICB solicită entității în cauză să ia măsurile corespunzătoare, inclusiv de natură disciplinară, în conformitate, în special, cu normele prevăzute în Statutul funcționarilor Uniunii Europene și Regimul aplicabil celorlalți agenți ai Uniunii Europene. În acest scop, IICB transferă informațiile necesare către entitatea în cauză.

Capitolul IV
CERT-UE

Articolul 12

Misiunea și sarcinile CERT-UE

(1) **Misiunea CERT-UE** [...] este de a contribui la securitatea mediului informatic neclasificat al tuturor [...] **entităților** Uniunii, oferindu-le consiliere cu privire la securitatea cibernetică, oferindu-le asistență pentru prevenirea, detectarea și atenuarea incidentelor și răspunsul la acestea și acționând ca centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru aceste entități.

(1a) CERT-UE colectează, gestionează, analizează și face schimb de informații cu entitățile Uniunii cu privire la amenințări, vulnerabilități și incidente legate de infrastructura TIC neclasificată. CERT-UE coordonează răspunsurile la incidente la nivel interinstituțional și la nivelul entităților Uniunii, inclusiv prin furnizarea de asistență operațională specializată sau prin coordonarea acesteia.

(2) CERT-UE îndeplinește următoarele sarcini pentru [...] **entitățile** Uniunii:

(a) le oferă sprijin pentru punerea în aplicare a prezentului regulament și contribuie la coordonarea aplicării prezentului regulament prin intermediul [...] **dispozițiilor** enumerate la articolul 13 alineatul (1) sau al rapoartelor ad-hoc solicitate de IICB;

(b) [...] **oferă servicii CSIRT standard pentru toate entitățile Uniunii printr-un** pachet de servicii de securitate cibernetică descrise în catalogul său de servicii („servicii de referință”);

(c) menține o rețea de omologi și parteneri pentru a sprijini serviciile, astfel cum se prevede la articolele 16 și 17;

(d) aduce în atenția IICB orice chestiune legată de punerea în aplicare a prezentului regulament și a documentelor de orientare, recomandărilor și apelurilor la acțiune;

(e) **pe baza informațiilor menționate la alineatul (1a),** [...] contribuie la conștientizarea situației amenințărilor la adresa securității cibernetice în UE **în strânsă cooperare cu ENISA. Aceste informații sunt comunicate IICB, precum și rețelei CSIRT și INTCEN UE;**

(f) acționează drept echivalent al coordonatorului desemnat pentru entitățile Uniunii, astfel cum se menționează la articolul 6 din [propunerea de directivă] NIS 2.

[...]

[...]

[...]

[...]

[...]

(4) **În cadrul competențelor care îi revin,** CERT-UE desfășoară o cooperare structurată cu [...] **ENISA** în ceea ce privește consolidarea capacităților, cooperarea operațională și analizele strategice pe termen lung ale amenințărilor cibernetice, în conformitate cu Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului.

(5) CERT-UE poate furniza următoarele servicii care nu sunt descrise în catalogul său de servicii („servicii contra cost”):

(a) servicii care sprijină securitatea cibernetică a mediului informatic al [...] **entităților** Uniunii, altele decât cele menționate la alineatul (2), în temeiul unor acorduri privind nivelul serviciilor și sub rezerva resurselor disponibile;

(b) servicii care sprijină operațiunile sau proiectele în materie de securitate cibernetică ale [...] **entităților** Uniunii, altele decât cele care vizează protejarea mediului lor informatic, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB;

(c) servicii care sprijină securitatea mediului informatic al altor organizații decât [...] **entitățile** Uniunii, care cooperează îndeaproape cu [...] **entitățile** Uniunii, de exemplu, cărora li s-au atribuit sarcini sau responsabilități în temeiul dreptului Uniunii, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB.

(6) CERT-UE poate organiza **sau poate participa la** exerciții de securitate cibernetică sau poate recomanda participarea la exercițiile existente, în strânsă cooperare cu [...] **ENISA**, dacă este cazul, pentru a testa nivelul de securitate cibernetică al [...] **entităților** Uniunii.

(7) CERT-UE poate oferi [...] **entităților** Uniunii asistență referitoare la incidentele din medii informatice clasificate dacă [...] **entitățile Uniunii în cauză** îi solicită acest lucru în mod expres **în conformitate cu procedurile lor respective. În acest caz, dispozițiile prevăzute la articolele 19-21 din prezentul regulament nu se aplică. Furnizarea de asistență din partea CERT-UE în temeiul prezentului alineat nu aduce atingere normelor aplicabile ale statelor membre sau ale Uniunii privind protecția informațiilor sensibile sau clasificate.**

(8) CERT-UE informează entitățile Uniunii cu privire la procedurile și procesele sale de gestionare a incidentelor.

(9) CERT-UE poate monitoriza traficul în rețea al entităților Uniunii, cu aprobarea entității Uniunii relevante.

(10) La solicitarea explicită a departamentelor tematice ale entităților Uniunii, CERT-UE poate oferi consultanță tehnică sau o contribuție cu privire la aspecte de politică relevante.

(11) În cooperare cu Autoritatea Europeană pentru Protecția Datelor, CERT-UE sprijină entitățile Uniunii în cauză atunci când abordează incidente care au ca rezultat încălcarea securității datelor cu caracter personal.

Articolul 13

Documente de orientare, recomandări și apeluri la acțiune

(1) CERT-UE sprijină punerea în aplicare a prezentului regulament prin emiterea unor:

(a) apeluri la acțiune care descriu măsurile urgente de securitate pe care [...] entitățile Uniunii sunt îndemnate să le adopte într-un termen stabilit. Fără întârzieri nejustificate după primirea apelului la acțiune, entitatea Uniunii în cauză informează CERT-UE cu privire la modul în care au fost aplicate măsurile respective;

(b) propuneri de documente de orientare, transmise IICB, care se adresează tuturor [...] **entităților** Uniunii sau doar unei părți a acestora;

(c) propuneri de recomandări, transmise IICB, care se adresează [...] **entităților** Uniunii individuale.

(2) Documentele de orientare și recomandările pot include:

(a) modalități sau îmbunătățiri ale gestionării riscurilor de securitate cibernetică și ale [...] **măsurilor de gestionare a riscurilor** de securitate cibernetică;

(b) modalități de evaluare a nivelului de maturitate și de elaborare a planurilor de securitate cibernetică și

(c) după caz, utilizarea tehnologiei și a arhitecturii comune, precum și a bunelor practici asociate în scopul realizării interoperabilității și a standardelor comune, **inclusiv o abordare coordonată privind securitatea lanțului de aprovizionare** [...]**.**

[...]

[...]

Articolul 14

Șeful CERT-UE

1. După obținerea aprobării a două treimi din membrii IICB, Comisia numește șeful CERT-UE. IICB este consultat în toate etapele procedurii care precede numirea șefului CERT-UE, în special în ceea ce privește elaborarea anunțurilor privind posturile vacante, examinarea dosarelor de candidatură și numirea comitetelor de selecție pentru acest post.

(2) Șeful CERT-UE este responsabil pentru buna funcționare a CERT-UE, în limitele competențelor sale, sub conducerea IICB. Este responsabil de punerea în aplicare a direcției strategice, a orientării, a obiectivelor și a priorităților stabilite de IICB, precum și de gestionarea CERT-UE, inclusiv a resurselor sale financiare și umane. Raportează periodic președintelui IICB.

(3) Șeful CERT-UE acordă ordonatorului de credite delegat responsabil asistență la întocmirea raportului de activitate anual, care conține informații financiare și de gestiune, inclusiv rezultatele controalelor, în conformitate cu articolul 66 alineatul (9) din Regulamentul financiar, și îi raportează periodic acestuia cu privire la punerea în aplicare a măsurilor pentru care i-au fost subdelegate competențe.

(4) Șeful CERT-UE elaborează anual o planificare financiară a veniturilor și cheltuielilor administrative pentru activitățile sale, propunerea de program de lucru anual, propunerea de catalog de servicii al CERT-UE și revizuirea acesteia, propunerea de modalități pentru acordurile privind nivelul serviciilor și propunerea de indicatori-cheie de performanță pentru CERT-UE, elemente care urmează să fie aprobate de IICB în conformitate cu articolul 10.

Atunci când revizuiește lista serviciilor din catalogul de servicii al CERT-UE, șeful CERT-UE ține seama de resursele alocate CERT-UE.

(5) Șeful CERT-UE prezintă IICB [...] rapoarte [...] **anuale** privind performanța CERT-UE, planificarea financiară, veniturile, execuția bugetară, acordurile privind nivelul serviciilor și acordurile scrise încheiate, cooperarea cu omologii și partenerii și misiunile desfășurate de personal, inclusiv rapoartele menționate la articolul 10 [...] **litera (a)**.

Articolul 15

Aspecte financiare și de personal

[...]

(1a) Deși instituit ca un furnizor de servicii interinstituțional autonom pentru toate entitățile Uniunii, CERT-UE este integrat în structura administrativă a unei direcții generale a Comisiei, pentru a beneficia de structurile de sprijin de ordin administrativ, de gestiune financiară și contabile ale Comisiei. Comisia informează IICB cu privire la amplasarea administrativă a CERT-UE și la eventuale modificări ale acesteia. Această abordare este evaluată periodic, cel târziu înainte de sfârșitul oricărui cadru financiar multianual instituit în conformitate cu articolul 312 din TFUE, pentru a permite luarea unor măsuri adecvate.

(2) În ceea ce privește aplicarea procedurilor administrative și financiare, șeful CERT-UE acționează sub autoritatea Comisiei.

(3) Sarcinile și activitățile CERT-UE, inclusiv serviciile furnizate de CERT-UE în temeiul articolului 12 alineatele (2), [...] (4) și (6) și al articolului 13 alineatul (1) [...] **entităților** Uniunii finanțate în cadrul rubricii „Administrația publică europeană” din cadrul financiar multianual, sunt finanțate printr-o linie bugetară separată a bugetului Comisiei. Posturile alocate CERT-UE sunt detaliate într-o notă de subsol la schema de personal a Comisiei.

(4) [...] **Entitățile** Uniunii, altele decât cele menționate la alineatul (3), aduc o contribuție anuală la bugetul CERT-UE pentru a acoperi serviciile furnizate de CERT-UE în temeiul alineatului menționat. Contribuțiile respective se bazează pe orientările oferite de IICB și convenite între fiecare entitate și CERT-UE în cadrul acordurilor privind nivelul serviciilor. Contribuțiile reprezintă un procent echitabil și proporțional din costurile totale ale serviciilor furnizate. Acestea sunt primite în cadrul liniei bugetare separate menționate la alineatul (3) ca venituri alocate, astfel cum se prevede la articolul 21 alineatul (3) litera (c) din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului[12].

(5) Costurile aferente sarcinilor definite la articolul 12 alineatul (5) se recuperează de la [...] **entitățile** Uniunii beneficiare ale serviciilor furnizate de CERT-UE. Veniturile sunt alocate liniilor bugetare prin care se suportă costurile.

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

Articolul 16

Cooperarea CERT-UE cu omologii din statele membre

1. **Fără întârzieri nejustificate,** CERT-UE cooperează și face schimb de informații cu omologii naționali din statele membre, **în special** [...] [...] [...] CSIRT **menționate la articolul 9 din [propunerea de directivă] NIS 2 și/sau, după caz, autoritățile naționale competente** și punctele unice de contact menționate la articolul 8 din [propunerea de directivă] NIS 2, cu privire la amenințări cibernetice, vulnerabilități și incidente, la posibile contramăsuri și la toate aspectele relevante pentru îmbunătățirea protecției mediilor informatice ale [...] **entităților** Uniunii, inclusiv prin intermediul rețelei CSIRT menționate la articolul 13 din [propunerea de directivă] NIS 2.

(1a) CERT-UE informează fără întârziere omologii naționali relevanți dintr-un stat membru menționați la alineatul (1) atunci când ia cunoștință de incidente semnificative care se produc pe teritoriul statului membru respectiv, cu excepția cazului în care CERT-UE are informații că entitatea Uniunii afectată a raportat deja un astfel de incident în conformitate cu articolul 20 alineatul (2a).

(2) **Fără întârzieri nejustificate,** CERT-UE [...] face schimb de informații referitoare la incidente cu omologii naționali din statele membre pentru a facilita detectarea amenințărilor sau a incidentelor cibernetice similare **sau pentru a contribui la analiza unui incident** fără **a fi nevoie de** acordul **entității Uniunii** [...] afectate. CERT-UE [...] **nu** face schimb de informații referitoare la incidente care dezvăluie identitatea țintei incidentului de securitate cibernetică [...] **decât în cazul în care**

(a) există acordul entității Uniunii afectate;

(b) entitatea Uniunii afectată a făcut deja public faptul că este afectată;

(c) nu există acordul entității Uniunii afectate, însă publicarea identității entității Uniunii afectate ar crește probabilitatea ca incidentele din altă parte să fie evitate sau atenuate. Astfel de decizii necesită aprobarea șefului CERT-UE. Entitatea Uniunii afectată este informată înainte de publicare.

Articolul 17

Cooperarea CERT-UE cu [...] ***alți omologi***

(1) CERT-UE poate coopera cu [...] omologi **din Uniunea Europeană alții decât cei menționați la articolul 16**, inclusiv cu omologii din cadrul sectorului, cu privire la instrumente și metode, cum ar fi tehnici, tactici, proceduri și bune practici, precum și cu privire la amenințări cibernetice și vulnerabilități. Pentru orice tip de cooperare cu astfel de [...] omologi, CERT-UE solicită aprobarea prealabilă a IICB**, de la caz la caz**. **CERT-UE informează orice omologi naționali relevanți menționați la articolul 16 alineatul (1), dintr-un stat membru în care este situat omologul, atunci când CERT-UE instituie o cooperare cu astfel de omologi.**

(2) CERT-UE poate coopera cu alți parteneri, precum entități comerciale, organizații internaționale, entități naționale din afara Uniunii Europene sau experți individuali, pentru a colecta informații cu privire la amenințările cibernetice generale și specifice, la vulnerabilități și la posibile contramăsuri. Pentru o cooperare extinsă cu astfel de parteneri, CERT-UE solicită aprobarea prealabilă a IICB**, de la caz la caz**.

(3) CERT-UE poate, **cu condiția existenței unui acord sau contract de nedivulgare de informații cu partenerul relevant,** cu acordul **entității Uniunii** [...] afectate de un incident, să furnizeze informații referitoare la incidentul **specific** partenerilor **menționați la alineatele (1) și (2) exclusiv în scopul contribuției** [...] la analiza acestuia. **Aceste acorduri sau contracte de nedivulgare de informații sunt supuse unei verificări juridice în conformitate cu procedurile interne relevante ale Comisiei. Acordurile sau contractele de nedivulgare de informații nu necesită aprobarea prealabilă a IICB, însă trebuie să fie informat președintele IICB.**

(4) **În mod excepțional, CERT-UE poate încheia acorduri privind nivelul serviciilor cu alte entități decât entitățile Uniunii, cu aprobarea prealabilă a IICB.**

Capitolul V
OBLIGAȚII DE COOPERARE ȘI DE RAPORTARE

Articolul 18

Gestionarea informațiilor

(1) CERT-UE și [...] **entitățile** Uniunii respectă obligația de a nu divulga informații care constituie secret profesional, în conformitate cu articolul 339 din Tratatul privind funcționarea Uniunii Europene sau cu cadrele echivalente aplicabile.

(2) Dispozițiile Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului[13] se aplică în ceea ce privește cererile de acces public la documentele deținute de CERT-UE, inclusiv obligația care decurge din regulamentul menționat de a consulta alte [...] **entități** ale Uniunii **și, după caz, statele membre,** ori de câte ori o cerere se referă la documentele lor.

[...]

(4) CERT-UE și [...] **entitățile** Uniunii gestionează informațiile în concordanță cu normele **aplicabile** [...] privind securitatea informațiilor[...].

[...]

Articolul 19

[...] ***Schimbul de informații privind securitatea cibernetică***

(-1) Entitățile Uniunii pot furniza CERT-UE în mod voluntar informații privind amenințările cibernetice, incidentele propriu-zise, incidentele evitate la limită și vulnerabilitățile care le afectează. CERT-UE se asigură că sunt disponibile mijloace eficiente de comunicare, în scopul de a facilita schimbul de informații cu entitățile Uniunii. CERT-UE poate trata notificările obligatorii cu prioritate față de notificările voluntare.

[13] 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).

(1) Pentru [...] **a-și îndeplini misiunea și sarcinile astfel cum sunt definite la articolul 12**, CERT-UE [...] poate solicita [...] **entităților** Uniunii să îi furnizeze informații din inventarele lor de sisteme informatice, **inclusiv informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, indicatori de compromitere, alerte de securitate cibernetică și recomandări privind configurarea instrumentelor de securitate cibernetică pentru detectarea incidentelor cibernetice** [...]. [...] **Entitatea** Uniunii care primește o astfel de solicitare transmite informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate.

(2) [...] **Entitățile** Uniunii, la cererea CERT-UE și fără întârzieri nejustificate, îi furnizează informații digitale create prin utilizarea dispozitivelor electronice implicate în incidentele lor respective. CERT-UE poate clarifica suplimentar tipurile de informații digitale de care are nevoie pentru conștientizarea situației și pentru răspunsul la incidente.

(3) CERT-UE poate face schimb de informații referitoare la incidente **cu entitățile Uniunii** care dezvăluie identitatea [...] **entității** Uniunii afectate de incident numai cu acordul entității respective. **În cazul în care acordul este refuzat, entitatea în cauză prezintă CERT-UE motive justificate în mod corespunzător.** [...]

(4) Obligațiile privind schimbul de informații nu se aplică în cazul informațiilor UE clasificate (IUEC) și al informațiilor **a căror distribuire în afara entității Uniunii destinatare a fost exclusă de către sursa informațiilor printr-un marcaj vizibil, cu excepția cazului în care sursa informațiilor** [...] **permite în mod explicit partajarea acestor informații cu CERT-UE.** [...]

Articolul 20

Obligații <u>de raportare</u> [...]

(-1) Un incident este considerat a fi semnificativ dacă:

(a) a cauzat sau poate cauza perturbări operaționale grave în funcționarea entității Uniunii sau pierderi financiare pentru entitatea Uniunii în cauză;

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

(1) Toate [...] **entitățile** Uniunii **transmit** [...] **CERT-UE:** [...]

[...].

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

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

(c) la cererea CERT-UE, un raport intermediar privind actualizări relevante ale situației;

(d) un raport final, în termen de cel mult o lună de la transmiterea notificării unui incident semnificativ menționate la litera (b), care să includă cel puțin următoarele elemente:

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

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

(iii) măsurile de atenuare aplicate și în curs;

(iv) după caz, impactul transfrontalier al incidentului semnificativ;

(e) în cazul unor incidente semnificative în curs la momentul transmiterii raportului final menționat la litera (d), un raport privind progresele înregistrate la momentul respectiv și un raport final în termen de o lună de la gestionarea incidentului.

[...]

(g) [...]

(h) [...]

(i) [...]

(j) [...]

(2a) Toate entitățile Uniunii partajează informațiile raportate în conformitate cu alineatul (1), în același termen, cu orice omologi naționali relevanți menționați la articolul 16 alineatul (1) din statul în care sunt situate.

(3) CERT-UE transmite [...] **IICB, INTCEN UE și rețelei CSIRT, o dată la trei luni,** [...] un raport de sinteză cu date anonimizate și agregate privind amenințările cibernetice [...], vulnerabilitățile [...] **în conformitate cu articolul 19, răspunsurile entităților Uniunii la apelurile la acțiune în conformitate cu articolul 13 alineatul (1) litera (a)** și incidentele semnificative notificate în conformitate cu alineatul (1). **Raportul respectiv constituie o contribuție la raportul bienal privind situația în materie de securitate cibernetică în Uniune, în temeiul articolului 15 din [propunerea de directivă] NIS 2.**

(4) [...] **Până la [6 luni de la intrarea în vigoare a prezentului regulament],** IICB emite documente de orientare sau recomandări **care aduc precizări suplimentare referitoare la** [...] modalitățile, **formatul** și conținutul **raportării** [...]. **Documentele de orientare sau recomandările țin seama în mod corespunzător de dispozițiile care sunt puse în aplicare prin orice acte de punere în aplicare în conformitate cu articolul 20 alineatul (11) din [propunerea de directivă] NIS 2.** CERT-UE difuzează detaliile tehnice adecvate pentru a permite detectarea proactivă, răspunsul la incidente sau adoptarea unor măsuri de atenuare de către [...] **entitățile** Uniunii.

(5) Obligațiile [...] **de raportare** nu se aplică în cazul IUEC și al informațiilor **a căror distribuire în afara entității Uniunii destinatare a fost exclusă de către sursa informațiilor printr-un marcaj vizibil, cu excepția cazului în care sursa informațiilor** [...] **permite în mod explicit partajarea acestor informații cu CERT-UE.** [...]

Articolul 21

Coordonarea răspunsului la incidente și cooperarea [...]

(1) Acționând în calitate de centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente, CERT-UE facilitează schimbul de informații cu privire la amenințările cibernetice, vulnerabilități și incidente, între:

(a) [...] **entitățile** Uniunii;

(b) omologii menționați la articolele 16 și 17.

(2) CERT-UE**,** [...] **după caz în strânsă cooperare cu ENISA în conformitate cu articolul 7 alineatul (7) litera (d) din Regulamentul privind securitatea cibernetică[14],** facilitează coordonarea între [...] **entitățile** Uniunii în ceea ce privește răspunsul la incidente, inclusiv prin:

(a) contribuția la o comunicare externă coerentă;

[...]

(c) utilizarea optimă a resurselor operaționale;

(d) coordonarea cu alte mecanisme de răspuns la situații de criză la nivelul Uniunii.

(3) **În strânsă cooperare cu ENISA,** CERT-UE sprijină [...] **entitățile** Uniunii în ceea ce privește conștientizarea situației amenințărilor cibernetice, a vulnerabilităților și a incidentelor.

---

14 REGULAMENTUL (UE) 2019/881 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică).

(4) **Până la [12 luni de la data intrării în vigoare a prezentului regulament], pe baza unei propuneri din partea CERT-UE,** IICB **adoptă** [...] **documente** de orientare **sau recomandări** privind coordonarea răspunsului la incidente și cooperarea în cazul incidentelor semnificative. În cazul în care se suspectează că un incident este de natură penală, CERT-UE consiliază cu privire la modul de raportare a incidentului către autoritățile de aplicare a legii.

Articolul 22

Gestionarea incidentelor majore [...]

(-1) Pentru a sprijini gestionarea coordonată a incidentelor majore la nivel operațional care afectează entitățile Uniunii și pentru a contribui la schimbul periodic de informații relevante între entitățile Uniunii și cu statele membre, IICB elaborează un plan de gestionare a crizelor cibernetice pe baza activităților detaliate la articolul 21 alineatul (2), în strânsă cooperare cu CERT-UE și ENISA, și include cel puțin următoarele elemente:

(a) modalități de coordonare și de flux de informații între entitățile Uniunii pentru gestionarea incidentelor majore la nivel operațional;

(b) proceduri standard de operare (PSO) comune;

(c) o taxonomie comună a gravității incidentelor majore și a punctelor de declanșare a crizelor;

(d) exerciții periodice;

(e) canale de comunicare securizate care urmează să fie utilizate;

(f) un punct de contact pentru EU-CyCLONe, care face schimb de informații relevante cu EU-CyCLONe drept contribuții la conștientizarea comună a situației.

(1) CERT-UE coordonează răspunsul [...] **entităților** Uniunii la [...] **incidente** majore. CERT-UE menține un inventar al expertizei tehnice necesare pentru răspunsul la incidente în cazul unor astfel de [...] **incidente majore**.

(2) [...] **Entitățile** Uniunii contribuie la inventarul expertizei tehnice prin transmiterea unei liste, actualizate anual, de experți disponibili în cadrul organizațiilor respective, în care sunt detaliate competențele tehnice specifice ale acestora.

(3) În urma unei solicitări specifice din partea unui stat membru în care este situată entitatea Uniunii afectată și cu [...] aprobarea [...] **entități**[...]**i** [...] Uniunii **afectate**, CERT-UE poate apela, de asemenea, la experții de pe lista menționată la alineatul (2) pentru a contribui la răspunsul la un [...] **incident** major **în** [...] **entitatea Uniunii respectivă** [...]**.**

Capitolul VI
DISPOZIȚII FINALE

Articolul 23

Realocare bugetară inițială

Comisia propune realocarea personalului și a resurselor financiare de la [...] **entitățile** relevante ale Uniunii către bugetul Comisiei. Realocarea produce efecte în același timp cu primul buget adoptat după intrarea în vigoare a prezentului regulament.

Articolul 24

Revizuire

(1) IICB, cu sprijinul CERT-UE, raportează periodic Comisiei cu privire la punerea în aplicare a prezentului regulament. IICB poate, de asemenea, să facă recomandări Comisiei pentru a [...] **revizui** prezentul regulament.

(2) Comisia prezintă Parlamentului European și Consiliului un raport privind punerea în aplicare a prezentului regulament în termen de cel mult [...] **36** de luni de la intrarea în vigoare a prezentului regulament și, ulterior, o dată la trei ani.

(3) Comisia evaluează funcționarea prezentului regulament și prezintă un raport Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor nu mai [...] **târziu** de cinci ani de la data intrării în vigoare. **Raportul este însoțit, după caz, de o propunere legislativă.**

Articolul 25

Intrarea 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	*Pentru Consiliu*
Președintele	*Președintele*

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

ANEXA II

[...]

[...]

[...]

[...]

[...]

[...]

[...]