Parlamentul European
2019-2024

Comisia pentru libertăți civile, justiție și afaceri interne

2020/0359(COD)

15.10.2021

AVIZ

al Comisiei pentru libertăți civile, justiție și afaceri interne

destinat Comisiei pentru industrie, cercetare și energie

referitor la propunerea de Directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Raportor pentru aviz (*): Lukas Mandl(*)

Procedura comisiilor asociate – articolul 57 din Regulamentul de procedură

PA_Legam

JUSTIFICARE SUCCINTĂ

Propunerea de directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de abrogare a Directivei (UE) 2016/1148 (Directiva NIS2)[1], face parte dintr-o serie mai amplă de inițiative la nivelul Uniunii care vizează creșterea rezilienței entităților publice și private împotriva amenințărilor. Propunerea urmărește să remedieze deficiențele legislației existente și să permită entităților care intră în domeniul său de aplicare să răspundă mai bine noilor provocări identificate de Comisie în evaluarea impactului, care a inclus o consultare amplă a părților interesate. Printre aceste provocări se numără, în special, digitalizarea sporită a pieței interne și evoluția situației amenințărilor la adresa securității.

Temeiul juridic al propunerii este articolul 114 din TFUE (piața internă). Din perspectiva LIBE, este totuși important să se evidențieze faptul că măsurile impuse rețelelor și sistemelor informatice prin Directiva NIS2 nu servesc doar la asigurarea bunei funcționări a pieței interne. **Directiva ar trebui, de asemenea, să contribuie la securitatea Uniunii în ansamblu**, printre altele prin evitarea vulnerabilității divergente la riscurile de securitate cibernetică dintre statele membre.

În acest scop, este esențial să **se elimine divergențele existente între statele membre** care rezultă din interpretările diferite ale legislației de către statele membre. Din acest motiv, raportorul salută condiția uniformă stabilită de regulament pentru a stabili entitățile care intră în domeniul de aplicare al directivei. Se fac sugestii suplimentare pentru a preveni divergențele în ceea ce privește punerea în aplicare, în special pentru a obliga Comisia să emită orientări privind punerea în aplicare a *lex specialis* și criteriile aplicabile IMM-urilor (care ar trebui, de asemenea, să asigure claritatea juridică și să evite sarcinile inutile) și să solicite Grupului de cooperare să specifice factorii fără caracter tehnic care trebuie luați în considerare în evaluările riscurilor din cadrul lanțului de aprovizionare. În plus, se subliniază faptul că cooperarea dintre autoritățile competente trebuie să aibă loc atât în interiorul statelor membre, cât și între acestea, în timp real.

Proiectul de raport preia, de asemenea, o serie de **recomandări formulate de AEPD** în avizul său privind Strategia de securitate cibernetică și Directiva NIS 2.0[2]. Cel mai important, se clarifică atât în considerente, cât și în partea dispozitivă a textului că nicio prelucrare a datelor cu caracter personal în temeiul Directivei NIS2 nu aduce atingere Regulamentului (UE) 2016/679 (RGPD)[3] și Directivei 2002/58/CE[4] (Directiva asupra confidențialității și

[1] 2020/0359(COD).

[2] Avizul nr. 5/2021: https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf.

[3] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE), *JO L 119, 4.5.2016, pp. 1-88.*

[4] Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice

comunicațiilor electronice). Având în vedere domeniul de aplicare mai restrâns al termenului „securitatea rețelelor și a sistemelor informatice” (cuprinde numai protecția tehnologiei) în comparație cu „securitatea cibernetică” (cuprinde și activitățile de protejare a utilizatorilor), primul termen este utilizat numai atunci când contextul este pur tehnic. În ceea ce privește numele de domenii și datele de înregistrare, se propun clarificări cu privire la 1) temeiul juridic al publicării „informațiilor relevante” în scopul identificării și contactării, 2) categoriile de date de înregistrare a domeniului de date care fac obiectul publicării (pe baza unei recomandări a ICANN) și 3) entitățile care ar putea constitui „solicitanți legitimi de acces”. De asemenea, în textul juridic se specifică faptul că propunerea nu afectează atribuirea jurisdicției și a competențelor autorităților de supraveghere a protecției datelor în temeiul RGPD. În cele din urmă, este prevăzut un temei juridic mai cuprinzător pentru cooperarea și schimbul de informații relevante dintre autoritățile competente în temeiul propunerii și alte autorități de supraveghere relevante, în special autoritățile de supraveghere în temeiul RGPD.

Alte modificări aduse propunerii Comisiei de către raportorul LIBE se referă la următoarele:

- Pentru a asigura coerența dintre Directiva NIS2 și propunerea de directivă privind reziliența entităților critice (ICE)[5], formularea anumitor dispoziții a fost aliniată la cea a propunerii ICE. În conformitate cu o modificare similară preconizată pentru Directiva privind ICE, care ar trebui să cuprindă aceleași sectoare ca Directiva NIS2, se propune adăugarea sintagmei „producția, prelucrarea și distribuția de alimente” în domeniul de aplicare.
- În ceea ce privește datele cu caracter personal, se clarifică faptul că scanarea rețelelor și a sistemelor informatice de către CSIRT ar trebui să se facă în conformitate nu numai cu Regulamentul (UE) 2016/679 (RGPD)[6], dar și cu Directiva 2002/58/CE[7] (Directiva asupra confidențialității și comunicațiilor electronice). Transferurile internaționale de date cu caracter personal în temeiul prezentei directive ar trebui să fie în conformitate cu capitolul V din RGPD.
- Grupul de cooperare ar trebui să se reunească de două ori, și nu o dată pe an, pentru a evalua cele mai recente evoluții în materie de securitate cibernetică. EDPB ar trebui să participe la activitățile Grupului de cooperare în calitate de observator.
- ENISA ar trebui să publice un raport anual, și nu unul bienal, privind situația în materie de securitate cibernetică în Uniune. Raportul ar trebui să țină seama, de asemenea, de impactul incidentelor de securitate cibernetică asupra protecției datelor cu caracter personal în Uniune.
- Termenul-limită de declarare a incidentelor este aliniat la termenul-limită pentru

---

(Directiva asupra confidențialității și comunicațiilor electronice) (*JO L 201, 31.7.2002, p. 37*).

[5] 2020/0365(COD).

[6] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE), *JO L 119, 4.5.2016, pp. 1-88.*

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

declararea încălcărilor în temeiul RGPD, și anume 72 de ore.

- Deși declararea incidentelor de securitate cibernetică reale de către entitățile esențiale și importante ar trebui, într-adevăr, să fie obligatorie, declararea amenințărilor cibernetice ar trebui să fie voluntară pentru a limita sarcina administrativă și a evita informarea excesivă. Pentru a fi considerat semnificativ, un incident trebuie să fi cauzat daune reale și să fi afectat alte persoane fizice și juridice, în loc ca aceste daune sau efecte să fie „posibile”.
- Circumstanțele care trebuie luate în considerare atunci când se decide cu privire la o sancțiune ca urmare a unei încălcări a normelor de securitate cibernetică sunt aliniate la RGPD. Întrucât acest lucru ar contraveni practicii actuale în materie de răspundere din dreptul Uniunii, nu ar trebui să fie posibil să se impună o interdicție temporară de a exercita funcții de conducere persoanelor fizice.
- Pentru a evita prejudicierea reputației, entitățile nu ar trebui să fie obligate să facă publice aspectele legate de nerespectarea cerințelor prevăzute în prezenta directivă sau identitatea persoanelor fizice sau juridice răspunzătoare de încălcare.

AMENDAMENTE

Comisia pentru libertăți civile, justiție și afaceri interne recomandă Comisiei pentru libertăți civile, justiție și afaceri interne, care este comisie competentă, să ia în considerare următoarele amendamente:

Amendamentul 1

Propunere de directivă
Considerentul 1

Textul propus de Comisie	*Amendamentul*
(1) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului[11] vizează consolidarea capacităților în materie de securitate cibernetică în întreaga Uniune, atenuarea amenințărilor la adresa rețelelor și a sistemelor informatice utilizate pentru a furniza servicii esențiale în sectoare-cheie și asigurarea continuității acestor servicii atunci când se confruntă cu incidente de securitate cibernetică, contribuind astfel la funcționarea eficace a economiei și a societății Uniunii.	(1) Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului[11] vizează consolidarea capacităților în materie de securitate cibernetică în întreaga Uniune, atenuarea amenințărilor la adresa rețelelor și a sistemelor informatice utilizate pentru a furniza servicii esențiale în sectoare-cheie și asigurarea continuității acestor servicii atunci când se confruntă cu incidente de securitate cibernetică, contribuind astfel la ***securitatea și funcționarea eficace a*** economiei și a societății Uniunii.
[11] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un	[11] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un

nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194/1, 19.7.2016, p. 1). 1).

nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194/1, 19.7.2016, p. 1). 1).

Amendamentul 2

Propunere de directivă
Considerentul 2

Textul propus de Comisie	*Amendamentul*
(2) De la intrarea în vigoare a Directivei (UE) 2016/1148, s-au înregistrat progrese semnificative în ceea ce privește creșterea nivelului de reziliență a securității cibernetice în Uniune. Revizuirea directivei respective a arătat că aceasta a servit drept catalizator pentru abordarea instituțională și de reglementare a securității cibernetice în Uniune, deschizând calea pentru o schimbare semnificativă de mentalitate. Această directivă a asigurat finalizarea cadrelor naționale prin definirea strategiilor naționale de securitate cibernetică, prin stabilirea de capacități naționale și prin punerea în aplicare a măsurilor de reglementare care vizează infrastructurile esențiale și actorii identificați de fiecare stat membru. De asemenea, a contribuit la cooperarea la nivelul Uniunii prin instituirea Grupului de cooperare[12] și a unei rețele de echipe naționale de intervenție în caz de incidente de securitate informatică („rețeaua CSIRT”)[13]. În pofida acestor realizări, revizuirea Directivei (UE) 2016/1148 a evidențiat deficiențe inerente care o împiedică să abordeze în mod eficace provocările contemporane și emergente în materie de securitate cibernetică.	(2) De la intrarea în vigoare a Directivei (UE) 2016/1148, s-au înregistrat progrese semnificative în ceea ce privește creșterea nivelului de reziliență a securității cibernetice în Uniune. Revizuirea directivei respective a arătat că aceasta a servit drept catalizator pentru abordarea instituțională și de reglementare a securității cibernetice în Uniune, deschizând calea pentru o schimbare semnificativă de mentalitate. Această directivă a asigurat finalizarea cadrelor naționale prin definirea strategiilor naționale de securitate cibernetică, prin stabilirea de capacități naționale și prin punerea în aplicare a măsurilor de reglementare care vizează infrastructurile esențiale și actorii identificați de fiecare stat membru. De asemenea, a contribuit la cooperarea la nivelul Uniunii prin instituirea Grupului de cooperare și a unei rețele de echipe naționale de intervenție în caz de incidente de securitate informatică („rețeaua CSIRT”). În pofida acestor realizări, revizuirea Directivei (UE) 2016/1148 a evidențiat deficiențe inerente care o împiedică să abordeze în mod eficace provocările contemporane și emergente în materie de securitate cibernetică. ***În plus, extinderea activităților online în contextul pandemiei de COVID-19 a evidențiat importanța securității cibernetice, care este esențială pentru ca cetățenii UE să poată avea încredere în inovare și conectivitate, precum și în instruirea și formarea la scară largă în acest domeniu. Prin urmare, Comisia ar trebui să sprijine***

	statele membre în elaborarea programelor de instruire privind securitatea cibernetică, pentru a permite entităților importante și esențiale să recruteze experți în securitate cibernetică care să le permită să respecte obligațiile ce decurg din prezenta directivă.
[12] Articolul 11 din Directiva (UE) 2016/1148.	[12] Articolul 11 din Directiva (UE) 2016/1148.
[13] Articolul 12 din Directiva (UE) 2016/1148.	[13] Articolul 12 din Directiva (UE) 2016/1148.

Amendamentul 3

Propunere de directivă
Considerentul 3

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

interne.

cibernetică sunt acum mai importante ca niciodată ***pentru securitatea Uniunii și*** pentru buna funcționare a pieței interne***, având în vedere transformarea digitală a activităților de zi cu zi din întreaga Uniune***. ***Acest lucru necesită o cooperare mai strânsă între autoritățile din cadrul statelor membre și între acestea, precum și între autoritățile naționale și organismele responsabile ale Uniunii.***

Amendamentul 4

Propunere de directivă
Considerentul 5

Textul propus de Comisie	*Amendamentul*
(5) Toate aceste divergențe implică o fragmentare a pieței interne și pot avea un efect negativ asupra funcționării acesteia, afectând în special furnizarea transfrontalieră de servicii și nivelul de reziliență în materie de securitate cibernetică din cauza aplicării unor standarde diferite. Prezenta directivă urmărește să elimine divergențele importante dintre statele membre, în special prin stabilirea unor norme minime privind funcționarea unui cadru de reglementare coordonat, prin stabilirea unor mecanisme pentru cooperarea eficace între autoritățile responsabile din fiecare stat membru, prin actualizarea listei sectoarelor și a activităților care fac obiectul obligațiilor în materie de securitate cibernetică și prin instituirea unor căi de atac și sancțiuni eficace care sunt esențiale pentru asigurarea eficace a respectării acestor obligații. Directiva (UE) 2016/1148 trebuie, prin urmare, abrogată și înlocuită cu prezenta directivă.	(5) Toate aceste divergențe implică o fragmentare a pieței interne și pot avea un efect negativ asupra funcționării acesteia, afectând în special furnizarea transfrontalieră de servicii și nivelul de reziliență în materie de securitate cibernetică din cauza aplicării unor standarde diferite. ***În cele din urmă, aceste divergențe pot duce la o vulnerabilitate mai mare a unor state membre la amenințările la adresa securității cibernetice, cu potențiale efecte de propagare în întreaga Uniune, atât în ce privește piața sa internă, cât și securitatea sa generală.*** Prezenta directivă urmărește să elimine divergențele importante dintre statele membre, în special prin stabilirea unor norme minime privind funcționarea unui cadru de reglementare coordonat, prin stabilirea unor mecanisme pentru cooperarea eficace ***și în timp real*** între autoritățile responsabile din fiecare stat membru***, între autoritățile competente ale statelor membre***, prin actualizarea listei sectoarelor și a activităților care fac obiectul obligațiilor în materie de securitate cibernetică și prin instituirea unor căi de atac și sancțiuni eficace care sunt esențiale pentru asigurarea eficace a respectării acestor obligații. Directiva (UE) 2016/1148

trebuie, prin urmare, abrogată și înlocuită cu prezenta directivă.

Amendamentul 5

Propunere de directivă
Considerentul 6

Textul propus de Comisie	*Amendamentul*
(6) Prezenta directivă nu aduce atingere posibilității de care dispun statele membre de a lua măsurile necesare pentru a asigura protecția intereselor sale esențiale de securitate, a apăra ordinea și siguranța publică și a permite investigarea, detectarea și urmărirea infracțiunilor, în conformitate cu legislația Uniunii. În conformitate cu articolul 346 din TFUE, niciun stat membru nu are obligația de a furniza informații a căror divulgare ar fi contrară intereselor esențiale ale siguranței sale publice. În acest context, sunt relevante normele naționale și cele ale Uniunii privind protecția informațiilor clasificate și acordurile de nedivulgare sau acordurile de nedivulgare informale, precum „Traffic Light Protocol”[14].	(6) Prezenta directivă nu aduce atingere posibilității de care dispun statele membre de a lua măsurile necesare pentru a asigura protecția intereselor sale esențiale de securitate națională, a apăra ordinea și siguranța publică și a permite prevenirea, investigarea, detectarea și urmărirea infracțiunilor, în conformitate cu legislația Uniunii. În conformitate cu articolul 346 din TFUE, niciun stat membru nu are obligația de a furniza informații a căror divulgare ar fi contrară intereselor esențiale ale siguranței sale publice. În acest context, sunt relevante normele naționale și cele ale Uniunii privind protecția informațiilor clasificate și acordurile de nedivulgare sau acordurile de nedivulgare informale, precum „Traffic Light Protocol”[14].
[14] Traffic Light Protocol (TLP) este un mijloc prin care cineva care face schimb de informații își informează publicul cu privire la eventualele limitări în răspândirea în continuare a acestor informații. Acest instrument este utilizat în aproape toate comunitățile CSIRT și în unele centre de schimb de informații și de analiză (ISAC).	[14] Traffic Light Protocol (TLP) este un mijloc prin care cineva care face schimb de informații își informează publicul cu privire la eventualele limitări în răspândirea în continuare a acestor informații. Acest instrument este utilizat în aproape toate comunitățile CSIRT și în unele centre de schimb de informații și de analiză (ISAC).

Amendamentul 6

Propunere de directivă
Considerentul 8

Textul propus de Comisie	*Amendamentul*
(8) ***În*** conformitate cu Directiva (UE) 2016/1148, statele membre au fost responsabile de stabilirea entităților care îndeplinesc criteriile pentru a fi considerate operatori de servicii esențiale („procesul de identificare”). ***Pentru a elimina divergențele*** mari ***dintre*** statele membre în această privință ***și pentru a asigura securitatea juridică în ceea ce privește cerințele de gestionare a riscurilor și obligațiile de raportare pentru toate entitățile relevante,*** ar trebui stabilit un criteriu uniform care să stabilească care sunt entitățile ce intră în domeniul de aplicare al prezentei directive. Acest criteriu ar trebui să constea în aplicarea regulii privind criteriul de dimensiune, conform căruia toate întreprinderile mijlocii și mari, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei[15], care își desfășoară activitatea în sectoarele reglementate de prezenta directivă sau furnizează tipul de servicii reglementate de aceasta intră în domeniul său de aplicare. Statele membre nu ar trebui să aibă obligația de a întocmi o listă a entităților care îndeplinesc acest criteriu general aplicabil în ceea ce privește dimensiunea.	(8) ***Responsabilitatea statelor membre în*** conformitate cu Directiva (UE) 2016/1148, ***potrivit căreia*** statele membre au fost responsabile de stabilirea entităților care îndeplinesc criteriile pentru a fi considerate operatori de servicii esențiale („procesul de identificare”) ***a dus la divergențe*** mari ***între*** statele membre în această privință***. Fără a aduce atingere excepțiilor specifice prevăzute în prezenta directivă,*** ar trebui stabilit un criteriu uniform care să stabilească care sunt entitățile ce intră în domeniul de aplicare al prezentei directive ***pentru a elimina aceste divergențe și a asigura securitatea juridică în ceea ce privește cerințele de gestionare a riscurilor și obligațiile de informare pentru toate entitățile relevante***. Acest criteriu ar trebui să constea în aplicarea regulii privind criteriul de dimensiune, conform căruia toate întreprinderile mijlocii și mari, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei[15], care își desfășoară activitatea în sectoarele reglementate de prezenta directivă sau furnizează tipul de servicii reglementate de aceasta intră în domeniul său de aplicare. Statele membre nu ar trebui să aibă obligația de a întocmi o listă a entităților care îndeplinesc acest criteriu general aplicabil în ceea ce privește dimensiunea.
[15] Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntrerinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).	[15] Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntrerinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

Amendamentul 7

Propunere de directivă
Considerentul 8 a (nou)

Textul propus de Comisie	*Amendamentul*
	(8a) Ținând seama de diferențele dintre cadrele administrațiilor publice naționale, statele membre își păstrează capacitatea de decizie în ceea ce privește desemnarea entităților care intră în domeniul de aplicare al prezentei directive.

Amendamentul 8

Propunere de directivă
Considerentul 9

Textul propus de Comisie	*Amendamentul*
(9) ***Cu toate acestea, entitățile*** mici sau microentitățile care îndeplinesc anumite criterii ce indică un rol-cheie pentru economiile sau societățile statelor membre sau pentru anumite sectoare sau tipuri de servicii ar trebui să intre, de asemenea, sub incidența prezentei directive. Statele membre ar trebui să fie responsabile de stabilirea unei liste a acestor entități și să o transmită Comisiei.	(9) ***Entitățile*** mici sau microentitățile care îndeplinesc anumite criterii care indică un rol-cheie pentru economiile sau societățile statelor membre sau pentru anumite sectoare sau tipuri de servicii ***bazate pe o evaluare a riscurilor, inclusiv entitățile definite drept entități critice sau entități echivalente cu entitățile critice în temeiul Directivei (UE) XXX/XXX a Parlamentului European și a Consiliului[1a]***, ar trebui să intre, de asemenea, sub incidența prezentei directive. Statele membre ar trebui să fie responsabile de stabilirea unei liste a acestor entități și să o transmită Comisiei. _____ ***[1a]Directiva (UE)[XXX/XXX] a Parlamentului European și a Consiliului din XXX privind reziliența entităților critice (JO ...).***

Amendamentul 9

Propunere de directivă
Considerentul 10

Textul propus de Comisie	*Amendamentul*
(10) Comisia, în cooperare cu Grupul de	(10) Comisia, în cooperare cu Grupul de

cooperare, ***poate emite*** orientări privind punerea în aplicare a criteriilor aplicabile microîntreprinderilor și ***întreprinderilor*** mici.	cooperare, ***ar trebui să emită*** orientări privind punerea în aplicare a criteriilor aplicabile microentităților și ***entităților*** mici.

Amendamentul 10

Propunere de directivă
Considerentul 12

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

Amendamentul 11

Propunere de directivă
Considerentul 14

Textul propus de Comisie	*Amendamentul*
(14) Având în vedere interconexiunile dintre securitatea cibernetică și securitatea fizică a entităților, ar trebui să se asigure o abordare coerentă între Directiva (UE) XXX/XXX a Parlamentului European și a Consiliului[17] și prezenta directivă. În acest scop, statele membre ar trebui să se asigure că, în temeiul Directivei (UE) XXX/XXX, entitățile critice și entitățile echivalente sunt considerate entități esențiale în temeiul prezentei directive. Statele membre ar trebui, de asemenea, să se asigure că strategiile lor în materie de securitate cibernetică oferă un cadru de politică pentru o coordonare consolidată între ***autoritatea competentă*** în temeiul prezentei directive și cea competentă în temeiul Directivei (UE) XXX/XXX în contextul schimbului de informații privind incidentele și amenințările cibernetice și al exercitării sarcinilor de supraveghere. Autoritățile competente în temeiul acestor două directive ar trebui să coopereze și să facă schimb de informații, în special în ceea ce privește identificarea entităților critice, amenințările cibernetice, riscurile de securitate cibernetică, incidentele care afectează entitățile critice, precum și cu privire la măsurile de securitate cibernetică adoptate de entitățile critice. La cererea autorităților competente în temeiul Directivei (UE) XXX/XXX, autorităților competente în temeiul prezentei directive ar trebui să li se permită să ***își exercite competențele de supraveghere și de asigurare a respectării legislației cu privire la o entitate esențială identificată*** ca fiind critică. Cele două tipuri de autorități ar trebui să coopereze și să facă schimb de informații în acest scop.	(14) Având în vedere interconexiunile dintre securitatea cibernetică și securitatea fizică a entităților, ar trebui să se asigure o abordare coerentă între Directiva (UE) XXX/XXX a Parlamentului European și a Consiliului17 și prezenta directivă***, oricând este posibil și adecvat***. În acest scop, statele membre ar trebui să se asigure că, în temeiul Directivei (UE) XXX/XXX, entitățile critice și entitățile echivalente sunt considerate entități esențiale în temeiul prezentei directive. Statele membre ar trebui, de asemenea, să se asigure că strategiile lor în materie de securitate cibernetică oferă un cadru de politică pentru o coordonare consolidată între ***autoritățile competente ale statelor membre și între cele din statele membre***, în temeiul prezentei directive și cea competentă în temeiul Directivei (UE) XXX/XXX în contextul schimbului de informații privind incidentele și amenințările cibernetice și al exercitării sarcinilor de supraveghere. Autoritățile ***statelor membre și cele din statele membre*** competente în temeiul acestor două directive ar trebui să coopereze și să facă schimb de informații, în special în ceea ce privește identificarea entităților critice, amenințările cibernetice, riscurile de securitate cibernetică, incidentele care afectează entitățile critice, precum și cu privire la măsurile de securitate cibernetică adoptate de ***autoritățile competente în temeiul prezentei directive relevante pentru*** entitățile critice. La cererea autorităților competente în temeiul Directivei (UE) XXX/XXX, autorităților competente în temeiul prezentei directive ar trebui să li se permită să ***evalueze securitatea cibernetică a unei entități esențiale identificate*** ca fiind critică. Cele două tipuri de autorități ar trebui să coopereze și să facă schimb de informații ***în timp real*** în acest scop.

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

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

Amendamentul 12

Propunere de directivă
Considerentul 18

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

Amendamentul 13

Propunere de directivă
Considerentul 20

Textul propus de Comisie	*Amendamentul*
(20) Aceste interdependențe din ce în ce mai mari sunt rezultatul unei rețele din ce în ce mai transfrontaliere și interdependente de furnizare de servicii care utilizează infrastructuri-cheie din întreaga Uniune în sectoare precum energia, transporturile, infrastructura digitală, apa potabilă și apele uzate, sănătatea, anumite aspecte ale administrației publice, precum și spațiul, în măsura în care furnizarea anumitor servicii în funcție de infrastructurile terestre care sunt deținute, gestionate și exploatate fie de statele membre, fie de părți private, nu acoperă, prin urmare, infrastructurile deținute, gestionate sau exploatate de Uniune sau în numele acesteia, ca parte a programelor sale spațiale. Aceste interdependențe înseamnă că orice perturbare, chiar dacă inițial este limitată la o singură entitate sau la un singur sector, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea efecte negative de amploare și de lungă durată asupra furnizării de servicii pe piața internă. ***Pandemia*** de COVID-19 a demonstrat vulnerabilitatea societăților noastre, care sunt din ce în ce mai interdependente în fața riscurilor cu probabilitate redusă de producere.	(20) Aceste interdependențe din ce în ce mai mari sunt rezultatul unei rețele din ce în ce mai transfrontaliere și interdependente de furnizare de servicii care utilizează infrastructuri-cheie din întreaga Uniune în sectoare precum energia, transporturile, infrastructura digitală, apa potabilă și apele uzate***, producția, prelucrarea și distribuția de alimente***, sănătatea, anumite aspecte ale administrației publice, precum și spațiul, în măsura în care furnizarea anumitor servicii în funcție de infrastructurile terestre care sunt deținute, gestionate și exploatate fie de statele membre, fie de părți private, nu acoperă, prin urmare, infrastructurile deținute, gestionate sau exploatate de Uniune sau în numele acesteia, ca parte a programelor sale spațiale. Aceste interdependențe înseamnă că orice perturbare, chiar dacă inițial este limitată la o singură entitate sau la un singur sector, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea efecte negative de amploare și de lungă durată asupra furnizării de servicii pe piața internă. ***Intensificarea atacurilor împotriva sistemelor informatice în timpul pandemiei*** de COVID-19 a demonstrat vulnerabilitatea societăților noastre, care sunt din ce în ce mai interdependente în fața riscurilor cu probabilitate redusă de producere. ***Prin urmare, sunt necesare investiții suplimentare în securitatea cibernetică.***

Amendamentul 14

Propunere de directivă
Considerentul 20 a (nou)

Textul propus de Comisie	*Amendamentul*
	(20a) Este esențial să se sensibilizeze opinia publică în domeniul cibernetic și

să se amplifice reziliența cibernetică în toate entitățile critice și importante, inclusiv în entitățile administrației publice.

Amendamentul 15

Propunere de directivă
Considerentul 21

Textul propus de Comisie	*Amendamentul*
(21) Având în vedere diferențele dintre structurile naționale de guvernanță și pentru a salvgarda acordurile sectoriale sau organismele de supraveghere și de reglementare ale Uniunii deja existente, statele membre ar trebui să fie capabile să desemneze mai multe autorități naționale competente responsabile cu îndeplinirea atribuțiilor legate de securitatea rețelelor și a sistemelor informatice ale operatorilor de servicii esențiale și ale entităților importante în temeiul prezentei directive. Statele membre ar trebui să fie capabile să atribuie acest rol unei autorități existente.	(21) Având în vedere diferențele dintre structurile naționale de guvernanță și pentru a salvgarda acordurile sectoriale sau organismele de supraveghere și de reglementare ale Uniunii deja existente, statele membre ar trebui să fie capabile să desemneze mai multe autorități naționale competente responsabile cu îndeplinirea atribuțiilor legate de securitatea rețelelor și a sistemelor informatice ale operatorilor de servicii esențiale și ale entităților importante în temeiul prezentei directive. Statele membre ar trebui să fie în măsură să atribuie acest rol unei autorități existente ***și să se asigure că aceasta dispune de resurse adecvate pentru a-și îndeplini sarcinile în mod eficace și eficient***.

Amendamentul 16

Propunere de directivă
Considerentul 22

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

informatice și cu cooperarea transfrontalieră la nivelul Uniunii.

transfrontalieră la nivelul Uniunii.

Amendamentul 17

Propunere de directivă
Considerentul 23

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

Amendamentul 18

Propunere de directivă
Considerentul 25

Textul propus de Comisie	*Amendamentul*
(25) În ceea ce privește datele cu caracter personal, CSIRT ar trebui să poată furniza, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[19], ***în ceea ce privește datele cu caracter personal***, în numele și la cererea unei entități în temeiul prezentei directive, o scanare ***proactivă a rețelei și a*** sistemelor informatice utilizate pentru	(25) În ceea ce privește datele cu caracter personal, CSIRT ar trebui să poată furniza, în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[19] ***și cu Directiva 2002/58/CE***, în numele și la cererea unei entități în temeiul prezentei directive, o scanare ***de securitate*** a sistemelor informatice ***și a plajei de rețea*** utilizate

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

pentru furnizarea serviciilor lor ***pentru a identifica, a atenua sau a preveni amenințări specifice***. Statele membre ar trebui să vizeze asigurarea unui nivel egal al capacităților tehnice pentru toate CSIRT-urile sectoriale. Statele membre pot solicita asistența Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) la dezvoltarea echipelor CSIRT naționale. ***În plus, riscurile în materie de securitate cibernetică nu ar trebui utilizate niciodată ca pretext pentru încălcarea drepturilor fundamentale.***

---

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

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

Amendamentul 19

Propunere de directivă
Considerentul 27

Textul propus de Comisie	*Amendamentul*
(27) În conformitate cu anexa la Recomandarea (UE) 2017/1584 a Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare („Blueprint”)20, un incident de mare anvergură ar trebui să însemne un incident cu un impact semnificativ asupra a cel puțin două state membre sau care provoacă o perturbare ce depășește capacitatea unui stat membru de a reacționa la acesta. În funcție de cauza și de impactul lor, incidentele de mare amploare pot escalada și se pot transforma în crize de sine stătătoare, care să împiedice buna funcționare a pieței interne. Având în vedere domeniul larg de aplicare	(27) În conformitate cu anexa la Recomandarea (UE) 2017/1584 a Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare („Blueprint”)20, un incident de mare anvergură ar trebui să însemne un incident cu un impact semnificativ asupra a cel puțin două state membre sau care provoacă o perturbare ce depășește capacitatea unui stat membru de a reacționa la acesta. În funcție de cauza și de impactul lor, incidentele de mare amploare pot escalada și se pot transforma în crize de sine stătătoare, care să împiedice buna funcționare a pieței interne ***sau să prezinte riscuri grave pentru***

și, în cele mai multe cazuri, natura transfrontalieră a unor astfel de incidente, statele membre și instituțiile, organele și agențiile relevante ale Uniunii ar trebui să coopereze la nivel tehnic, operațional și politic pentru a coordona în mod corespunzător răspunsul în întreaga Uniune.

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

securitatea publică în mai multe state membre sau în Uniune în ansamblul său. Având în vedere domeniul larg de aplicare și, în cele mai multe cazuri, natura transfrontalieră a unor astfel de incidente, statele membre și instituțiile, organele și agențiile relevante ale Uniunii ar trebui să coopereze la nivel tehnic, operațional și politic pentru a coordona în mod corespunzător răspunsul în întreaga Uniune. ***Statele membre ar trebui să monitorizeze modul în care sunt puse în aplicare normele UE, să se sprijine reciproc în cazul oricăror probleme transfrontaliere, să stabilească un dialog mai structurat cu sectorul privat și să coopereze în ceea ce privește riscurile de securitate și amenințările asociate noilor tehnologii, cum a fost cazul tehnologiei 5G.***

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

Amendamentul 20

Propunere de directivă
Considerentul 33

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

Amendamentul 21

Propunere de directivă
Considerentul 34

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

Amendamentul 22

Propunere de directivă
Considerentul 36

Textul propus de Comisie	*Amendamentul*
(36) Dacă este posibil, Uniunea ar trebui să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaționale cu țări terțe sau organizații internaționale, care să permită și să organizeze participarea acestora la anumite activități ale Grupului de cooperare și ale rețelei CSIRT. ***Astfel de acorduri*** ar trebui ***să asigure o protecție adecvată a datelor***.	(36) Dacă este posibil, Uniunea ar trebui să încheie, în conformitate cu articolul 218 din TFUE, acorduri internaționale cu țări terțe sau organizații internaționale, care să permită și să organizeze participarea acestora la anumite activități ale Grupului de cooperare și ale rețelei CSIRT. ***În măsura în care datele cu caracter personal sunt transferate unei țări terțe***

sau unei organizații internaționale, ar trebui ***să se aplice capitolul V din Regulamentul (UE) 2016/679***.

Amendamentul 23

Propunere de directivă
Considerentul 37

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

apărare comună (PSAC), ar trebui activat mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă (SEAE).

Amendamentul 24

Propunere de directivă
Considerentul 45

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

Amendamentul 25

Propunere de directivă
Considerentul 46 a (nou)

Textul propus de Comisie	*Amendamentul*
	(46a) O atenție specială ar trebui acordată faptului că serviciile, sistemele sau produsele TIC care fac obiectul unor

	cerințe specifice în țara de origine ar putea reprezenta un obstacol în calea respectării legislației UE privind confidențialitatea și protecția datelor. După caz, CEPD ar trebui consultat în cadrul unor astfel de evaluări de risc. Software-ul liber și cu sursă deschisă, precum și hardware-ul cu sursă deschisă ar putea aduce beneficii imense în ceea ce privește securitatea cibernetică, în special în materie de transparență și posibilitate de verificare a caracteristicilor. Deoarece acest lucru ar putea contribui la abordarea și atenuarea riscurilor specifice din lanțul de aprovizionare, utilizarea lor ar trebui preferată acolo unde este posibil, în concordanță cu Avizul 5/2021 al AEPD[1a].
	[1a] Avizul 5/2021 al Autorității Europene pentru Protecția Datelor privind Strategia de securitate cibernetică și Directiva NIS 2.0, 11 martie 2021.

Amendamentul 26

Propunere de directivă
Considerentul 47

Textul propus de Comisie	*Amendamentul*
(47) Evaluările riscurilor din cadrul lanțului de aprovizionare, având în vedere caracteristicile sectorului în cauză, ar trebui să țină seama atât de factori tehnici, cât și, după caz, de factori fără caracter tehnic, ***inclusiv de*** cei definiți în Recomandarea (UE) 2019/534, în evaluarea coordonată la nivelul UE a riscurilor legate de securitatea rețelelor 5G și în setul de instrumente al UE privind securitatea cibernetică 5G convenit de Grupul de cooperare. Pentru a identifica lanțurile de aprovizionare care ar trebui să facă obiectul unei evaluări coordonate a riscurilor, ar trebui să se țină seama de următoarele criterii: (i) în ce măsură entitățile esențiale și importante	(47) Evaluările riscurilor din cadrul lanțului de aprovizionare, având în vedere caracteristicile sectorului în cauză, ar trebui să țină seama atât de factori tehnici, cât și, după caz, de factori fără caracter tehnic, ***care ar trebui să fie precizați în detaliu de către Grupul de coordonare, și care îi includ pe*** cei definiți în Recomandarea (UE) 2019/534, în evaluarea coordonată la nivelul UE a riscurilor legate de securitatea rețelelor 5G și în setul de instrumente al UE privind securitatea cibernetică 5G convenit de Grupul de cooperare. Pentru a identifica lanțurile de aprovizionare care ar trebui să facă obiectul unei evaluări coordonate a riscurilor, ar trebui să se țină

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

Amendamentul 27

Propunere de directivă
Considerentul 48 a (nou)

Textul propus de Comisie	*Amendamentul*
	(48a) Întreprinderilor mici și mijlocii (IMM-urilor) le lipsesc deseori amploarea și resursele necesare pentru satisfacerea unei game largi și tot mai mari de nevoi în materie de securitate cibernetică într-o lume interconectată, caracterizată printr-o creștere a muncii de la distanță. Prin urmare, în strategiile lor naționale de securitate cibernetică statele membre ar trebui să ofere orientări și sprijin pentru IMM-uri.

Amendamentul 28

Propunere de directivă
Considerentul 50

Textul propus de Comisie	*Amendamentul*
(50) Având în vedere importanța crescândă a serviciilor de comunicații interpersonale care nu se bazează pe	(50) Având în vedere importanța crescândă a serviciilor de comunicații interpersonale care nu se bazează pe

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

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

Amendamentul 29

Propunere de directivă
Considerentul 52

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

Amendamentul 30

Propunere de directivă
Considerentul 53

Textul propus de Comisie	*Amendamentul*
(53) În special, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului ar trebui să îi informeze pe destinatarii serviciilor cu privire la amenințările cibernetice specifice și semnificative și cu privire la măsurile pe care le pot lua pentru a-și proteja securitatea comunicațiilor, de exemplu prin folosirea unor anumite tipuri de software sau de tehnologii de criptare.	(53) În special, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului ar trebui ***să pună în aplicare securitatea de la stadiul conceperii și securitatea implicită și ar trebui să aibă posibilitatea*** să îi informeze pe destinatarii serviciilor cu privire la amenințările cibernetice specifice și semnificative și cu privire la măsurile pe care le pot lua pentru a-și proteja securitatea dispozitivelor și a comunicațiilor, de exemplu prin folosirea unor anumite tipuri de software sau de tehnologii de criptare. ***Pentru a mări securitatea hardware-ului și software-ului, furnizorii ar trebui încurajați să utilizeze hardware cu sursă deschisă și liber.***

Amendamentul 31

Propunere de directivă
Considerentul 54

Textul propus de Comisie	*Amendamentul*
(54) Pentru a se garanta securitatea rețelelor și a serviciilor de comunicații electronice, ar trebui promovată utilizarea criptării, în special a criptării de la un capăt la altul și, dacă este necesar, acest tip de criptare ar trebui să fie obligatoriu pentru furnizorii de astfel de servicii și rețele, în conformitate cu principiile securității și protecției vieții private în mod implicit și începând cu momentul conceperii, în sensul articolului 18. Utilizarea criptării de la un capăt la altul ar trebui să fie reconciliată cu ***competențele*** statelor membre de a asigura protecția intereselor	(54) Pentru a garanta securitatea rețelelor și a serviciilor de comunicații electronice, ***precum și dreptul fundamental la protecția datelor și la viața privată***, ar trebui promovată utilizarea criptării, în special a criptării de la un capăt la altul și, dacă este necesar, acest tip de criptare ar trebui să fie obligatoriu pentru furnizorii de astfel de servicii și rețele, în conformitate cu principiile securității și protecției vieții private în mod implicit și începând cu momentul conceperii, în sensul articolului 18. Utilizarea criptării de la un capăt la

lor esențiale în materie de securitate și de siguranță publică și de a permite ***investigarea***, depistarea și urmărirea penală a infracțiunilor în conformitate cu dreptul Uniunii. Soluțiile pentru accesul legal la informații în comunicațiile criptate de la un capăt la altul ar trebui să mențină eficacitatea criptării în ceea ce privește protecția vieții private și securitatea comunicațiilor, ***oferind, în același timp, un răspuns eficace la criminalitate***.	altul ar trebui să fie reconciliată cu ***responsabilitatea*** statelor membre de a asigura protecția intereselor lor esențiale în materie de securitate și de siguranță publică și de a permite ***prevenirea***, depistarea și urmărirea penală a infracțiunilor în conformitate cu dreptul Uniunii ***și cu dreptul intern***. Soluțiile pentru accesul legal la informații în comunicațiile criptate de la un capăt la altul ar trebui să mențină eficacitatea criptării în ceea ce privește protecția vieții private și securitatea comunicațiilor. ***Nicio dispoziție din prezenta directivă nu ar trebui considerată drept efort de slăbire a criptării de la un capăt la altul, fie prin „crearea de uși secrete”, fie prin soluții similare, având în vedere că deficiențele legate de criptare pot fi exploatate în scopuri răuvoitoare. Orice măsură care vizează slăbirea criptării sau eludarea arhitecturii tehnologiei poate prezenta riscuri semnificative pentru capacitățile*** eficace ***de protecție pe care le implică***. ***Orice decriptare neautorizată sau orice monitorizare a comunicațiilor electronice care nu este efectuată de autorități legale ar trebui interzisă pentru a asigura eficacitatea tehnologiei și utilizarea ei mai amplă***. ***Este important ca statele membre să trateze problemele cu care se confruntă autoritățile legale și cercetătorii din domeniul vulnerabilităților. În unele state membre, entitățile și persoanele fizice care cercetează vulnerabilitățile sunt expuse răspunderii penale și civile. Prin urmare, statele membre sunt încurajate să emită orientări privind neurmărirea penală și neimpunerea răspunderii în ceea ce privește cercetarea în domeniul securității informațiilor.***

Amendamentul 32

Propunere de directivă
Considerentul 56

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

Amendamentul 33

Propunere de directivă
Considerentul 57

Textul propus de Comisie	*Amendamentul*
(57) Atunci când există suspiciuni că un incident ar fi legat de activități infracționale grave în temeiul dreptului Uniunii sau al dreptului intern, statele membre ar trebui să încurajeze entitățile esențiale și importante, pe baza normelor aplicabile în materie de proceduri penale în conformitate cu dreptul Uniunii, să raporteze autorităților de aplicare a legii incidentele despre care există suspiciuni că ar avea un caracter infracțional grav. După	(57) Atunci când există suspiciuni că un incident ar fi legat de activități infracționale grave în temeiul dreptului Uniunii sau al dreptului intern, statele membre ar trebui să încurajeze entitățile esențiale și importante, pe baza normelor aplicabile în materie de proceduri penale în conformitate cu dreptul Uniunii, ***ar trebui*** să raporteze autorităților de aplicare a legii incidentele despre care există suspiciuni că ar avea un caracter infracțional grav. După

caz și fără a aduce atingere normelor de protecție a datelor cu caracter personal aplicabile Europol, este de dorit ca procesul de coordonare dintre autoritățile competente și autoritățile de aplicare a legii din diferite state membre să fie facilitată de ***EC3*** și de ENISA.	caz și fără a aduce atingere normelor de protecție a datelor cu caracter personal aplicabile Europol, este de dorit ca procesul de coordonare dintre autoritățile competente și autoritățile de aplicare a legii din diferite state membre să fie facilitată de ***Centrul european de combatere a criminalității informatice (EC3) al Europol*** și de ENISA.

Amendamentul 34

Propunere de directivă
Considerentul 58

Textul propus de Comisie	*Amendamentul*
(58) În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente. În acest context, autoritățile competente ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante cu autoritățile de protecție a datelor și cu autoritățile de supraveghere, în temeiul Directivei 2002/58/CE.	(58) În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente. În acest context, autoritățile competente ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante cu autoritățile de protecție a datelor și cu autoritățile de supraveghere, în temeiul ***Regulamentului (UE) 2016/679 și al*** Directivei 2002/58/CE.

Amendamentul 35

Propunere de directivă
Considerentul 59

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

protecție a datelor.

materie de protecție a datelor.

Amendamentul 36

Propunere de directivă
Considerentul 62

Textul propus de Comisie	*Amendamentul*
(62) ***Registrele*** TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii ar trebui să pună la dispoziția publicului date de înregistrare a numelor de domenii ***care nu intră în domeniul de aplicare al normelor Uniunii privind protecția datelor***, cum ar fi ***datele care se referă la persoanele*** juridice[25]. Registrele TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD ar trebui, de asemenea, să le permită solicitanților legitimi de acces, în conformitate cu ***legislația Uniunii privind protecția datelor,*** accesul legal la date specifice de înregistrare a numelor de domenii privind persoanele fizice. Statele membre ar trebui să se asigure că registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii răspund fără întârzieri nejustificate solicitărilor de divulgare a datelor de înregistrare a numelor de domenii formulate de ***solicitanții legitimi de acces***. Registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii ar trebui să stabilească politici și proceduri pentru publicarea și divulgarea datelor de înregistrare, inclusiv acorduri privind nivelul serviciilor pentru a trata cererile de acces din partea solicitanților legitimi de acces. Procedura de acces poate include, de asemenea, utilizarea unei interfețe, a unui portal sau a unui alt instrument tehnic, scopul fiind furnizarea unui sistem eficient de solicitare și accesare a datelor de înregistrare. În vederea promovării unor practici armonizate pe piața internă, Comisia poate adopta orientări cu privire la aceste	(62) ***Pentru a se conforma unei obligații legale în temeiul articolului 6 alineatul (1) litera (c) și al articolului 6 alineatul (3) din Regulamentul (UE) 2016/679, registrele*** TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii ar trebui să pună la dispoziția publicului ***anumite*** date de înregistrare a numelor de domenii ***specificate în legislația statului membru care li se aplică***, cum ar fi ***numele de domeniu și numele persoanei*** juridice. Registrele TLD și entitățile care furnizează servicii de înregistrare a numelor de domenii pentru TLD ar trebui, de asemenea, să le permită solicitanților legitimi de acces, ***îndeosebi autorităților competente în temeiul prezentei directive sau autorităților de supraveghere în temeiul regulamentului (UE) 2016/679,*** în conformitate cu ***competențele lor***, accesul legal la date specifice de înregistrare a numelor de domenii privind persoanele fizice. Statele membre ar trebui să se asigure că registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii răspund fără întârzieri nejustificate solicitărilor ***legale și justificate în mod corespunzător*** formulate de ***autoritățile publice, inclusiv de autoritățile competente în temeiul prezentei directive, de autoritățile competente în temeiul dreptului Uniunii sau al dreptului intern pentru prevenirea, investigarea sau urmărirea penală a infracțiunilor sau de autoritățile de supraveghere în temeiul regulamentului (UE) 2016/679,*** de divulgare a datelor de înregistrare a numelor de domenii.

proceduri fără a aduce atingere competențelor Comitetului european pentru protecția datelor.

Registrele TLD și entitățile care le furnizează servicii de înregistrare a numelor de domenii ar trebui să stabilească politici și proceduri pentru publicarea și divulgarea datelor de înregistrare, inclusiv acorduri privind nivelul serviciilor pentru a trata cererile de acces din partea solicitanților legitimi de acces. Procedura de acces poate include, de asemenea, utilizarea unei interfețe, a unui portal sau a unui alt instrument tehnic, scopul fiind furnizarea unui sistem eficient de solicitare și accesare a datelor de înregistrare. În vederea promovării unor practici armonizate pe piața internă, Comisia poate adopta orientări cu privire la aceste proceduri fără a aduce atingere competențelor Comitetului european pentru protecția datelor.

---

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

Amendamentul 37

Propunere de directivă
Considerentul 63

Textul propus de Comisie	*Amendamentul*
(63) ***Toate*** entitățile esențiale și importante vizate de prezenta directivă sunt considerate ca fiind sub jurisdicția statului membru în care își prestează serviciile. În cazul în care entitatea furnizează servicii în mai multe state membre, aceasta ar trebui să intre sub jurisdicția separată și concurentă a fiecăruia dintre aceste state	(63) ***În sensul prezentei directive, toate*** entitățile esențiale și importante vizate de prezenta directivă sunt considerate ca fiind sub jurisdicția statului membru în care își prestează serviciile. În cazul în care entitatea furnizează servicii în mai multe state membre, aceasta ar trebui să intre sub jurisdicția separată și concurentă a

membre. Autoritățile competente din aceste state membre ar trebui să coopereze, să își ofere asistență reciprocă și, după caz, să întreprindă acțiuni comune de supraveghere.

fiecăruia dintre aceste state membre. Autoritățile competente din aceste state membre ar trebui ***să convină asupra clasificărilor constitutive,*** să coopereze ***atunci când este posibil***, să își ofere asistență reciprocă ***în timp real*** și, după caz, să întreprindă acțiuni comune de supraveghere.

Amendamentul 38

Propunere de directivă
Considerentul 64

Textul propus de Comisie	*Amendamentul*
(64) Pentru a ține seama de caracterul transfrontalier al serviciilor și al operațiunilor furnizorilor de servicii DNS, ale registrelor de nume TLD, ale furnizorilor de rețele de distribuție de conținut, ale furnizorilor de servicii de cloud computing, ale furnizorilor de servicii de centre de date și ale furnizorilor digitali, un singur stat membru ar trebui să aibă jurisdicție asupra acestor entități. ***Competența*** ar trebui să fie atribuită statului membru în care entitatea respectivă își are sediul principal în Uniune. Criteriul stabilirii în sensul prezentei directive implică exercitarea efectivă a activității prin intermediul unor înțelegeri stabile. Forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință. Respectarea acestui criteriu nu ar trebui să depindă de localizarea fizică a rețelei și a sistemelor informatice într-un anumit loc; prezența și utilizarea unor astfel de sisteme nu constituie, în sine, un astfel de sediu principal și, prin urmare, nu sunt criterii decisive pentru stabilirea sediului principal. Sediul principal ar trebui să fie locul în care sunt luate deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică în Uniune. Aceasta va corespunde, de regulă, locului în care se	(64) Pentru a ține seama de caracterul transfrontalier al serviciilor și al operațiunilor furnizorilor de servicii DNS, ale registrelor de nume TLD, ale furnizorilor de rețele de distribuție de conținut, ale furnizorilor de servicii de cloud computing, ale furnizorilor de servicii de centre de date și ale furnizorilor digitali, un singur stat membru ar trebui să aibă jurisdicție asupra acestor entități. ***În sensul prezentei directive, competența*** ar trebui să fie atribuită statului membru în care entitatea respectivă își are sediul principal în Uniune. Criteriul stabilirii în sensul prezentei directive implică exercitarea efectivă a activității prin intermediul unor înțelegeri stabile. Forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință. Respectarea acestui criteriu nu ar trebui să depindă de localizarea fizică a rețelei și a sistemelor informatice într-un anumit loc; prezența și utilizarea unor astfel de sisteme nu constituie, în sine, un astfel de sediu principal și, prin urmare, nu sunt criterii decisive pentru stabilirea sediului principal. Sediul principal ar trebui să fie locul în care sunt luate deciziile legate de măsurile de gestionare a riscurilor în materie de securitate cibernetică în Uniune. Aceasta

află administrația centrală a întreprinderilor din Uniune. În cazul în care astfel de decizii nu sunt luate în Uniune, se consideră că sediul principal se află în statul membru în care entitatea are sediul cu cel mai mare număr de angajați din Uniune. În cazul în care serviciile sunt prestate de un grup de întreprinderi, sediul principal al întreprinderii care exercită controlul ar trebui considerat drept sediul principal al grupului de întreprinderi.

va corespunde, de regulă, locului în care se află administrația centrală a întreprinderilor din Uniune. În cazul în care astfel de decizii nu sunt luate în Uniune, se consideră că sediul principal se află în statul membru în care entitatea are sediul cu cel mai mare număr de angajați din Uniune. În cazul în care serviciile sunt prestate de un grup de întreprinderi, sediul principal al întreprinderii care exercită controlul ar trebui considerat drept sediul principal al grupului de întreprinderi.

Amendamentul 39

Propunere de directivă
Considerentul 69

Textul propus de Comisie	*Amendamentul*
(69) Prelucrarea datelor cu caracter personal, în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor de către entități, autorități publice, CERT, CSIRT și furnizorii de tehnologii și servicii de securitate ar trebui să constituie un interes legitim al operatorului de date în cauză, astfel cum se menționează ***în*** Regulamentul (UE) 2016/679. Aceasta ar trebui să includă măsuri legate de prevenirea, detectarea, analizarea și combaterea incidentelor, măsuri de sensibilizare cu privire la amenințările cibernetice specifice, schimbul de informații în contextul remedierii vulnerabilității și al divulgării coordonate, precum și schimbul voluntar de informații cu privire la incidentele respective, precum și la amenințările și vulnerabilitățile cibernetice, indicatori de compromis, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare. Astfel de măsuri pot necesita prelucrarea ***următoarelor tipuri*** de date cu caracter personal***:*** adrese IP, localizatoare uniforme de resurse (URL), nume de	(69) Prelucrarea datelor cu caracter personal, în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor de către entități, autorități publice, CERT, CSIRT și furnizorii de tehnologii și servicii de securitate ***este necesară pentru a fi în conformitate cu obligațiile lor legale în temeiul legislației naționale de transpunere a prezentei directive și, prin urmare, este cuprinsă în articolul 6 alineatul (1) litera (c) și în articolul (6) alineatul (3) din Regulamentul (UE) 2016/679. În plus, o astfel de prelucrare*** ar trebui să constituie un interes legitim al operatorului de date în cauză, astfel cum se menționează ***la articolul 6 alineatul (1) litera (f) din*** Regulamentul (UE) 2016/679. Aceasta ar trebui să includă măsuri legate de prevenirea, detectarea, analizarea și combaterea incidentelor, măsuri de sensibilizare cu privire la amenințările cibernetice specifice, schimbul de informații în contextul remedierii vulnerabilității și al divulgării coordonate, precum și schimbul voluntar de informații cu privire la incidentele respective, precum și la amenințările și vulnerabilitățile

domenii și adrese de e-mail.

cibernetice, indicatori de compromis, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare. ***În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente cibernetice și, prin urmare, autoritățile competente și autoritățile de protecție a datelor din statele membre ale UE ar trebui să coopereze și să facă schimb de informații cu privire la toate aspectele relevante pentru a combate orice încălcare a securității datelor cu caracter personal.*** Astfel de măsuri pot necesita prelucrarea ***anumitor categorii*** de date cu caracter personal***, inclusiv*** adrese IP, localizatoare uniforme de resurse (URL), nume de domenii și adrese de e-mail.

Amendamentul 40

Propunere de directivă
Considerentul 71

Textul propus de Comisie	*Amendamentul*
(71) Pentru ca asigurarea respectării să fie eficace, ar trebui stabilită o listă minimă de sancțiuni administrative pentru încălcarea obligațiilor de gestionare a riscurilor de securitate cibernetică și de raportare prevăzute în prezenta directivă, stabilind un cadru clar și coerent pentru astfel de sancțiuni în întreaga Uniune. Ar trebui să se țină seama în mod corespunzător de ***natura,*** gravitatea și durata încălcării, de daunele reale cauzate sau de pierderile suferite ori de daunele sau pierderile potențiale care ar fi putut fi declanșate, de caracterul intenționat sau din neglijență al încălcării, de acțiunile întreprinse pentru a preveni sau a atenua prejudiciul și/sau pierderile suferite, de gradul de responsabilitate sau de orice încălcare anterioară relevantă, de gradul de cooperare cu autoritatea competentă și de orice alt factor agravant sau atenuant. ***Impunerea de sancțiuni***, inclusiv ***de***	(71) Pentru ca asigurarea respectării să fie eficace, ar trebui stabilită o listă minimă de sancțiuni administrative pentru încălcarea obligațiilor de gestionare a riscurilor de securitate cibernetică și de raportare prevăzute în prezenta directivă, stabilind un cadru clar și coerent pentru astfel de sancțiuni în întreaga Uniune. Ar trebui să se țină seama în mod corespunzător de gravitatea și durata încălcării, de daunele reale cauzate sau de pierderile suferite ori de daunele sau pierderile potențiale care ar fi putut fi declanșate***, de încălcările anterioare relevante, de modul în care încălcarea a fost adusă la cunoștința autorității competente***, de caracterul intenționat sau din neglijență al încălcării, de acțiunile întreprinse pentru a preveni sau a atenua prejudiciul și/sau pierderile suferite, de gradul de responsabilitate sau de orice încălcare anterioară relevantă, de gradul de

amenzi administrative, ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene, inclusiv al unei protecții judiciare eficiente și al unui proces echitabil.

cooperare cu autoritatea competentă și de orice alt factor agravant sau atenuant. ***Sancțiunile impuse***, inclusiv ***amenzile*** administrative, ar trebui să facă obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene, inclusiv al unei protecții judiciare eficiente și al unui proces echitabil.

Amendamentul 41

Propunere de directivă
Considerentul 74

Textul propus de Comisie	*Amendamentul*
(74) Statele membre ar trebui să poată stabili norme privind sancțiunile penale pentru încălcarea normelor naționale de transpunere a prezentei directive. Cu toate acestea, impunerea de sancțiuni penale pentru încălcări ale acestor norme de drept intern și de sancțiuni administrative conexe nu ar trebui să ducă la încălcarea principiului ne bis in idem, astfel cum a fost interpretat de Curtea de Justiție.	(74) Statele membre ar trebui să poată stabili norme privind sancțiunile penale pentru încălcarea normelor naționale de transpunere a prezentei directive. ***Respectivele sancțiuni penale pot, de asemenea, permite privarea de profiturile obținute prin încălcarea prezentului regulament.*** Cu toate acestea, impunerea de sancțiuni penale pentru încălcări ale acestor norme de drept intern și de sancțiuni administrative conexe nu ar trebui să ducă la încălcarea principiului ne bis in idem, astfel cum a fost interpretat de Curtea de Justiție.

Amendamentul 42

Propunere de directivă
Considerentul 76

Textul propus de Comisie	*Amendamentul*
(76) Pentru a consolida și mai mult eficacitatea și caracterul disuasiv al sancțiunilor aplicabile în cazul încălcării obligațiilor prevăzute în temeiul prezentei directive, autoritățile competente ar trebui să fie împuternicite să aplice sancțiuni constând în suspendarea unei certificări sau	(76) Pentru a consolida și mai mult eficacitatea și caracterul disuasiv al sancțiunilor aplicabile în cazul încălcării obligațiilor prevăzute în temeiul prezentei directive, autoritățile competente ar trebui să fie împuternicite să aplice sancțiuni constând în suspendarea unei certificări sau

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

a unei autorizații privind o parte din serviciile furnizate de o entitate esențială sau toate aceste servicii. Având în vedere gravitatea și impactul lor asupra activităților entităților și, în cele din urmă, asupra consumatorilor acestora, aceste sancțiuni ar trebui aplicate numai proporțional cu gravitatea încălcării și ținând seama de circumstanțele specifice fiecărui caz, inclusiv de caracterul intenționat sau din neglijență al încălcării, de măsurile luate pentru a preveni sau a atenua prejudiciul și/sau de pierderile suferite. Astfel de sancțiuni ar trebui aplicate doar în ultimă instanță, adică numai după ce celelalte măsuri relevante de asigurare a respectării legislației prevăzute de prezenta directivă au fost epuizate și numai până în momentul în care entitățile cărora li se aplică iau măsurile necesare pentru a remedia deficiențele sau pentru a se conforma cerințelor autorității competente pentru care au fost aplicate aceste sancțiuni. Impunerea unor astfel de sancțiuni face obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu Carta drepturilor fundamentale a Uniunii Europene, inclusiv ***căi de atac efective***, respectarea garanțiilor procedurale, prezumția de nevinovăție și dreptul la apărare.

Amendamentul 43

Propunere de directivă
Considerentul 77

Textul propus de Comisie	*Amendamentul*
(77) Prezenta directivă ar trebui să stabilească norme de cooperare între autoritățile competente și autoritățile de supraveghere în ***conformitate cu Regulamentul*** (UE) 2016/679 pentru tratarea cazurilor de încălcare a normelor	(77) Prezenta directivă ar trebui să stabilească norme de cooperare între autoritățile competente ***în temeiul prezentei directive*** și autoritățile de supraveghere în ***temeiul Regulamentului*** (UE) 2016/679 pentru tratarea cazurilor de

în materie de date cu caracter personal.	încălcare a normelor în materie de date cu caracter personal.

Amendamentul 44

Propunere de directivă
Considerentul 79

Textul propus de Comisie	*Amendamentul*
(79) Ar trebui introdus un mecanism de evaluare inter pares, care să permită evaluarea de către experții desemnați de statele membre a punerii în aplicare a politicilor în materie de securitate cibernetică, inclusiv a nivelului capacităților și al resurselor de care dispun statele membre.	(79) Ar trebui introdus un mecanism de evaluare inter pares, care să permită evaluarea de către experții desemnați de statele membre a punerii în aplicare a politicilor în materie de securitate cibernetică, inclusiv a nivelului capacităților și al resurselor de care dispun statele membre. ***UE ar trebui să faciliteze un răspuns coordonat la incidentele și crizele cibernetice de mare amploare și să ofere asistență pentru a sprijini redresarea în urma unor astfel de atacuri cibernetice.***

Amendamentul 45

Propunere de directivă
Considerentul 82 a (nou)

Textul propus de Comisie	*Amendamentul*
	(82a) Prezenta directivă nu se aplică instituțiilor, oficiilor, organelor și agențiilor Uniunii. Totuși, organele Uniunii ar putea fi considerate entități esențiale sau importante în temeiul prezentei directive. Pentru a atinge un nivel uniform de protecție, prin norme coerente și omogene, Comisia ar trebui să publice o propunere legislativă cu scopul de a include instituțiile, oficiile, organele și agențiile Uniunii în cadrul de securitate cibernetică la nivelul întregii UE, până la 31 decembrie 2022.

Amendamentul 46

Propunere de directivă
Considerentul 84

Textul propus de Comisie	*Amendamentul*
(84) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă în fața unei instanțe judecătorești și dreptul de a fi ascultat. Prezenta directivă ar trebui să fie pusă în aplicare în conformitate cu drepturile și principiile menționate,	(84) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă în fața unei instanțe judecătorești și dreptul de a fi ascultat. Prezenta directivă ar trebui să fie pusă în aplicare în conformitate cu drepturile și principiile menționate ***și în deplină conformitate cu legislația existentă a Uniunii care reglementează aceste aspecte. Orice prelucrare a datelor cu caracter personal în temeiul prezentei directive face obiectul Regulamentului (UE) 2016/679 și al Directivei 2002/58/CE, în domeniul lor de aplicare respectiv, inclusiv sarcinile și prerogativele autorităților de supraveghere care au atribuția de a monitoriza respectarea acestor instrumente juridice.***

Amendamentul 47

Propunere de directivă
Articolul 2 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Prezenta directivă se aplică entităților publice și private de tipul celor menționate ca fiind entități esențiale în anexa I și entități importante în anexa II. Prezenta directivă nu se aplică entităților care se califică drept microîntreprinderi și întreprinderi mici în sensul Recomandării	1. Prezenta directivă se aplică entităților publice și private de tipul celor menționate ca fiind entități esențiale în anexa I și entități importante în anexa II. Prezenta directivă nu se aplică entităților care se califică drept microîntreprinderi și întreprinderi mici în sensul Recomandării

2003/361/CE a Comisiei[28].	2003/361/CE a Comisiei[28]. ***Articolul 3 alineatul (4) din anexa la Recomandarea 2003/361/CE a Comisiei nu se aplică.***
[28] Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).	[28] Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

Amendamentul 48

Propunere de directivă
Articolul 2 – alineatul 2 – partea introductivă

Textul propus de Comisie	*Amendamentul*
2. Cu toate acestea, indiferent de dimensiunea lor, prezenta directivă se aplică, de asemenea, entităților menționate în anexele I și II, în cazul în care:	2. Cu toate acestea, indiferent de dimensiunea lor ***și pe baza unei evaluări a riscurilor în conformitate cu articolul 18***, prezenta directivă se aplică, de asemenea, entităților menționate în anexele I și II, în cazul în care:

Amendamentul 49

Propunere de directivă
Articolul 2 – alineatul 2 – litera c

Textul propus de Comisie	*Amendamentul*
(c) entitatea este singurul furnizor al unui serviciu într-un stat membru;	(c) entitatea este singurul furnizor al unui serviciu într-un stat membru ***la nivel național sau regional***;

Amendamentul 50

Propunere de directivă
Articolul 2 – alineatul 2 – litera d

Textul propus de Comisie	*Amendamentul*
(d) o ***eventuală*** perturbare a serviciului furnizat de entitate ar putea avea un impact asupra siguranței publice, a securității	(d) o perturbare a serviciului furnizat de entitate ar putea avea un impact asupra siguranței publice, a securității publice sau

publice sau a sănătății publice;	a sănătății publice;

Amendamentul 51

Propunere de directivă
Articolul 2 – alineatul 2 – litera e

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

Amendamentul 52

Propunere de directivă
Articolul 2 – alineatul 4 a (nou)

Textul propus de Comisie	*Amendamentul*
	4a. Orice prelucrare a datelor cu caracter personal în temeiul prezentei directive respectă Regulamentul (UE) 2016/679 și Directiva 2002/58/CE și se limitează la ceea ce este strict necesar și proporțional în sensul prezentei directive.

Amendamentul 53

Propunere de directivă
Articolul 2 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Fără a aduce atingere articolului 346 din TFUE, informațiile confidențiale în conformitate cu normele Uniunii și cu cele naționale, precum cele privind secretul comercial, fac obiectul schimbului de informații cu Comisia și cu alte autorități relevante numai dacă acest lucru este necesar pentru aplicarea prezentei directive. Informațiile care fac obiectul schimbului se limitează la informații ***relevante și proporționale cu*** scopul urmărit. Schimbul de informații păstrează	5. Fără a aduce atingere articolului 346 din TFUE, informațiile confidențiale în conformitate cu normele Uniunii și cu cele naționale, precum cele privind secretul comercial, fac obiectul schimbului de informații cu Comisia și cu alte autorități relevante numai dacă acest lucru este necesar pentru aplicarea prezentei directive. Informațiile care fac obiectul schimbului se limitează la informații ***necesare pentru*** scopul urmărit. Schimbul de informații păstrează confidențialitatea

confidențialitatea informațiilor respective și protejează securitatea și interesele comerciale ale entităților esențiale sau importante.	informațiilor respective și protejează securitatea și interesele comerciale ale entităților esențiale sau importante.

Amendamentul 54

Propunere de directivă
Articolul 2 – alineatul 6 a (nou)

Textul propus de Comisie	*Amendamentul*
	6a. Până la 31 decembrie 2021, Comisia publică o propunere legislativă care să includă instituțiile, organele, oficiile și agențiile Uniunii în cadrul general de securitate cibernetică la nivelul întregii UE, în vederea realizării unui nivel uniform de protecție, prin norme coerente și omogene.

Amendamentul 55

Propunere de directivă
Articolul 4 – alineatul 1 – punctul 1 –litera b

Textul propus de Comisie	*Amendamentul*
(b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale;	(b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată de date digitale***, și care sunt integrate în sistemul informatic și utilizate pentru a furniza serviciile prevăzute***;

Amendamentul 56

Propunere de directivă
Articolul 4 – alineatul 1 – punctul 4

Textul propus de Comisie	*Amendamentul*
(4) „strategie națională de securitate cibernetică” înseamnă un cadru coerent al unui stat membru care prevede obiective și	(4) „strategie națională de securitate cibernetică” înseamnă un cadru coerent al unui stat membru care prevede obiective și

priorități strategice privind securitatea ***rețelelor și a sistemelor informatice*** în statul membru respectiv;	priorități strategice privind securitatea ***cibernetică*** în statul membru respectiv;

Amendamentul 57

Propunere de directivă
Articolul 4 – alineatul 1 – punctul 12

Textul propus de Comisie	*Amendamentul*
(12) „internet exchange point (IXP)” înseamnă o structură de rețea care permite interconectarea a mai mult de două rețele independente (sisteme autonome), în special în scopul facilitării schimbului de trafic de internet; un IXP furnizează interconectare doar pentru sisteme autonome; un IXP nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre o pereche oarecare de sisteme autonome participante și nici nu modifică sau afectează într-un alt mod acest trafic;	***eliminat***

Amendamentul 58

Propunere de directivă
Articolul 4 – alineatul 1 – punctul 22

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

Amendamentul 59

Propunere de directivă
Articolul 4 – alineatul 1 – punctul 24

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

Amendamentul 60

Propunere de directivă
Articolul 5 – alineatul 1 – litera a

Textul propus de Comisie	*Amendamentul*
(a) o definire a obiectivelor și a priorităților strategiei statelor membre privind securitatea cibernetică;	(a) o definire a obiectivelor și a priorităților strategiei statelor membre privind securitatea cibernetică***, luând în considerare nivelul general de conștientizare a securității cibernetice în rândul cetățenilor, precum și nivelul general de securitate al dispozitivelor conectate ale consumatorilor***;

Amendamentul 61

Propunere de directivă
Articolul 5 – alineatul 1 – litera f

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

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

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

Amendamentul 62

Propunere de directivă
Articolul 5 – alineatul 2 – litera b

Textul propus de Comisie	*Amendamentul*
(b) orientări privind includerea și specificarea cerințelor legate de securitatea cibernetică pentru produsele și serviciile TIC în cadrul achizițiilor publice;	(b) orientări privind includerea și specificarea cerințelor legate de securitatea cibernetică pentru produsele și serviciile TIC în cadrul achizițiilor publice***, inclusiv cerințele de criptare și promovarea utilizării produselor de securitate cibernetică cu sursă deschisă, dar fără a se limita la acestea***;

Amendamentul 63

Propunere de directivă
Articolul 5 – alineatul 2 – litera da (nouă)

Textul propus de Comisie	*Amendamentul*
	(da) o politică legată de susținerea utilizării datelor deschise și a sursei deschise în cadrul securității prin transparență;

Amendamentul 64

Propunere de directivă
Articolul 5 – alineatul 2 – litera db (nouă)

Textul propus de Comisie	*Amendamentul*
	(db) o politică de promovare a confidențialității și a securității datelor cu caracter personal ale utilizatorilor de servicii online;

Amendamentul 65

Propunere de directivă
Articolul 5 – alineatul 2 – litera e

Textul propus de Comisie	*Amendamentul*
(e) o politică de promovare și dezvoltare a inițiativelor privind competențele, sensibilizarea și cercetarea și dezvoltarea în materie de securitate cibernetică;	(e) o politică de promovare și dezvoltare a inițiativelor privind competențele, sensibilizarea și cercetarea și dezvoltarea în materie de securitate cibernetică***, inclusiv dezvoltarea unor programe de formare privind securitatea cibernetică care să furnizeze specialiști și tehnicieni entităților***;

Amendamentul 66

Propunere de directivă
Articolul 5 – alineatul 2 – litera f

Textul propus de Comisie	*Amendamentul*
(f) o politică de sprijinire a instituțiilor academice și de cercetare în ***vederea dezvoltării*** unor instrumente de securitate cibernetică și a unei infrastructuri de rețea securizate;	(f) o politică de sprijinire a instituțiilor academice și de cercetare***, care să contribuie la strategia națională*** în ***materie de securitate cibernetică, prin dezvoltarea și implementarea*** unor instrumente de securitate cibernetică și a unei infrastructuri de rețea securizate ***care să contribuie la strategia națională în materie de securitate cibernetică, inclusiv politici specifice privind aspectele legate de reprezentarea și echilibrul de gen în acest sector***;

Amendamentul 67

Propunere de directivă
Articolul 5 – alineatul 2 – litera h

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

adresa securității cibernetice.	adresa securității cibernetice ***și a capacității lor de a interveni în cazul unui incident de securitate cibernetică***.

Amendamentul 68

Propunere de directivă
Articolul 6 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. ENISA creează și menține un registru european al vulnerabilităților. În acest scop, ENISA instituie și menține sisteme, politici și proceduri de informare adecvate, în special pentru a permite entităților importante și esențiale și furnizorilor acestora de rețele și sisteme informatice să divulge și să înregistreze vulnerabilitățile prezente în produsele TIC sau serviciile TIC, precum și să ofere acces tuturor părților interesate la informațiile privind vulnerabilitățile conținute în registru. Registrul include, în special, informații care descriu vulnerabilitatea, produsul TIC sau serviciile TIC afectate și gravitatea vulnerabilității în ceea ce privește circumstanțele în care aceasta poate fi exploatată, disponibilitatea unor corecții conexe și, dacă astfel de corecții nu sunt disponibile, orientări adresate utilizatorilor de produse și servicii vulnerabile cu privire la modul în care pot fi atenuate riscurile care rezultă din vulnerabilitățile divulgate.	2. ENISA creează și menține un registru european al vulnerabilităților. În acest scop, ENISA instituie și menține sisteme, politici și proceduri de informare adecvate, în special pentru a permite entităților importante și esențiale și furnizorilor acestora de rețele și sisteme informatice să divulge și să înregistreze vulnerabilitățile prezente în produsele TIC sau serviciile TIC, precum și să ofere acces tuturor părților interesate la informațiile privind vulnerabilitățile conținute în registru. Registrul include, în special, informații care descriu vulnerabilitatea, produsul TIC sau serviciile TIC afectate și gravitatea vulnerabilității în ceea ce privește circumstanțele în care aceasta poate fi exploatată, disponibilitatea unor corecții conexe și, dacă astfel de corecții nu sunt disponibile, orientări adresate utilizatorilor de produse și servicii vulnerabile cu privire la modul în care pot fi atenuate riscurile care rezultă din vulnerabilitățile divulgate. ***Pentru a asigura securitatea și accesibilitatea informațiilor incluse în registru, ENISA aplică măsuri de securitate de ultimă generație și pune informațiile la dispoziție, în formate prelucrabile automat, prin intermediul interfețelor corespunzătoare.***

Amendamentul 69

Propunere de directivă
Articolul 7 – alineatul 3 – litera a

Textul propus de Comisie	*Amendamentul*
(a) obiectivele măsurilor și ale activităților naționale de pregătire;	(a) obiectivele măsurilor și ale activităților naționale de pregătire***, și, dacă este relevant și aplicabil, regionale și transfrontaliere***;

Amendamentul 70

Propunere de directivă
Articolul 10 – alineatul 2 – litera e

Textul propus de Comisie	*Amendamentul*
(e) furnizarea, la cererea unei entități, a unei scanări ***proactive*** a ***rețelei*** și a ***sistemelor informatice*** utilizate pentru furnizarea serviciilor lor;	(e) furnizarea, la cererea unei entități, a unei scanări ***de securitate*** a ***sistemelor informatice*** și a ***întinderii rețelei*** utilizate pentru furnizarea serviciilor lor***, cu scopul de a identifica, atenua sau preveni amenințări specifice; prelucrarea datelor cu caracter personal în contextul unei astfel de scanări se limitează la ceea ce este strict necesar și, în orice caz, la adresele IP și URL-uri;***

Amendamentul 71

Propunere de directivă
Articolul 11 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. În măsura în care este necesar pentru a îndeplini în mod eficace sarcinile și obligațiile prevăzute în prezenta directivă, statele membre asigură o cooperare adecvată între autoritățile competente și punctele unice de contact și autoritățile de aplicare a legii, autoritățile pentru protecția datelor și autoritățile responsabile cu infrastructura critică în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] și autoritățile financiare naționale	4. În măsura în care este necesar pentru a îndeplini în mod eficace sarcinile și obligațiile prevăzute în prezenta directivă, statele membre asigură o cooperare adecvată între autoritățile competente și punctele unice de contact și autoritățile de aplicare a legii, autoritățile pentru protecția datelor și autoritățile responsabile cu infrastructura critică în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] și autoritățile financiare naționale

desemnate în conformitate cu Regulamentul (UE) XXXX/XXXX al Parlamentului European și al Consiliului[39] [Regulamentul DORA] din statul membru respectiv.	desemnate în conformitate cu Regulamentul (UE) XXXX/XXXX al Parlamentului European și al Consiliului39 [Regulamentul DORA] din statul membru respectiv***, în conformitate cu competențele lor respective***.
[39] [a se introduce titlul complet și referința de publicare în JO, atunci când acestea vor fi cunoscute]	[39] [a se introduce titlul complet și referința de publicare în JO, atunci când acestea vor fi cunoscute]

Amendamentul 72

Propunere de directivă
Articolul 11 – alineatul 5

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

Amendamentul 73

Propunere de directivă
Articolul 12 – alineatul 3 – partea introductivă

Textul propus de Comisie	*Amendamentul*
3. Grupul de cooperare este format din reprezentanți ai statelor membre, ai Comisiei și ai ENISA. Serviciul European de Acțiune Externă participă la activitățile	3. Grupul de cooperare este format din reprezentanți ai statelor membre, ai Comisiei și ai ENISA. Serviciul European de Acțiune Externă***, Centrul european de***

grupului de cooperare în calitate de observator. Autoritățile europene de supraveghere (AES) în conformitate cu articolul 17 alineatul (5) litera (c) din Regulamentul (UE) XXXX/XXXX [Regulamentul DORA] pot participa la activitățile grupului de cooperare.	***combatere a criminalității informatice din cadrul Europol și Comitetul european pentru protecția datelor*** participă la activitățile grupului de cooperare în calitate de observator. Autoritățile europene de supraveghere (AES) în conformitate cu articolul 17 alineatul (5) litera (c) din Regulamentul (UE) XXXX/XXXX [Regulamentul DORA] pot participa la activitățile grupului de cooperare.

Amendamentul 74

Propunere de directivă
Articolul 12 – alineatul 3 – paragraful 1

Textul propus de Comisie	*Amendamentul*
După caz, grupul de cooperare ***poate invita*** să participe la lucrările sale ***reprezentanți ai părților interesate relevante***.	***În cazul în care acest lucru este relevant pentru îndeplinirea sarcinilor sale***, grupul de cooperare ***invită reprezentanți ai părților interesate relevante*** să participe la lucrările sale***, iar Parlamentul European este invitat să participe în calitate de observator***.

Amendamentul 75

Propunere de directivă
Articolul 12 – alineatul 8

Textul propus de Comisie	*Amendamentul*
8. Grupul de cooperare se reunește periodic și cel puțin ***o dată*** pe an cu Grupul privind reziliența entităților critice instituit în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] pentru a ***promova*** cooperarea strategică și schimbul de informații.	8. Grupul de cooperare se reunește periodic și cel puțin ***de două ori*** pe an cu Grupul privind reziliența entităților critice instituit în temeiul Directivei (UE) XXXX/XXXX [Directiva privind reziliența entităților critice] pentru a ***facilita*** cooperarea strategică și schimbul de informații ***în timp real***.

Amendamentul 76

Propunere de directivă
Articolul 13 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Rețeaua CSIRT este formată din reprezentanți ai echipelor CSIRT ale statelor membre și ai CERT-UE. Comisia participă la rețeaua CSIRT în calitate de observator. ENISA asigură secretariatul și sprijină activ cooperarea între echipele CSIRT.	2. Rețeaua CSIRT este formată din reprezentanți ai echipelor CSIRT ale statelor membre și ai CERT-UE. Comisia ***și Centrul european de combatere a criminalității informatice din cadrul Europol*** participă la rețeaua CSIRT în calitate de observator. ENISA asigură secretariatul și sprijină activ cooperarea între echipele CSIRT.

Amendamentul 77

Propunere de directivă
Articolul 14 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. UE - CyCLONe este formată din reprezentanți ai autorităților de gestionare a crizelor din statele membre desemnați în conformitate cu articolul 7, reprezentanți ai Comisiei și ai ENISA. ENISA asigură secretariatul rețelei și sprijină schimbul securizat de informații.	2. UE - CyCLONe este formată din reprezentanți ai autorităților de gestionare a crizelor din statele membre desemnați în conformitate cu articolul 7, reprezentanți ai Comisiei și ai ENISA. ***Centrul european de combatere a criminalității informatice din cadrul Europol participă la activitățile UE-CyCLONe în calitate de observator.*** ENISA asigură secretariatul rețelei și sprijină schimbul securizat de informații.

Amendamentul 78

Propunere de directivă
Articolul 14 – alineatul 6

Textul propus de Comisie	*Amendamentul*
6. UE-CyCLONe cooperează cu rețeaua CSIRT pe baza modalităților procedurale convenite.	6. UE-CyCLONe cooperează cu rețeaua CSIRT pe baza modalităților procedurale convenite ***și cu asigurarea respectării legii în cadrul Protocolului UE privind răspunsul în caz de urgență al autorităților de aplicare a legii***.

Amendamentul 79

Propunere de directivă
Articolul 15 – alineatul 1 – partea introductivă

Textul propus de Comisie	*Amendamentul*
1. ENISA elaborează, în cooperare cu Comisia, un raport ***bienal*** privind situația în materie de securitate cibernetică în Uniune. Raportul include, în special, o evaluare a următoarelor elemente:	1. ENISA elaborează, în cooperare cu Comisia, un raport ***anual*** privind situația în materie de securitate cibernetică în Uniune. Raportul ***este furnizat într-un format citibil automat și*** include, în special, o evaluare a următoarelor elemente:

Amendamentul 80

Propunere de directivă
Articolul 15 – alineatul 1 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(ca) impactul incidentelor de securitate cibernetică asupra protecției datelor cu caracter personal în Uniune.

Amendamentul 81

Propunere de directivă
Articolul 15 – alineatul 1 – litera cb (nouă)

Textul propus de Comisie	*Amendamentul*
	(cb) o prezentare de ansamblu a nivelului general de conștientizare în domeniul cibernetic și de utilizare a securității cibernetice în rândul cetățenilor, precum și a nivelului general de securitate a dispozitivelor conectate orientate către consumatori, introduse pe piața Uniunii.

Amendamentul 82

Propunere de directivă
Articolul 17 – alineatul 2

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

Amendamentul 83

Propunere de directivă
Articolul 18 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Statele membre se asigură că entitățile esențiale și importante iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice ***pe care entitățile respective le utilizează pentru a furniza*** servicii. Ținând seama de cele mai avansate cunoștințe în domeniu, măsurile respective asigură un nivel de securitate a rețelelor și a sistemelor informatice adecvat riscului prezentat.	1. Statele membre se asigură că entitățile esențiale și importante iau măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității ***cibernetice a*** rețelelor și a sistemelor informatice ***utilizate pentru furnizarea serviciilor lor și în vederea garantării continuității acestor*** servicii ***și a reducerii riscurilor la adresa drepturilor persoanelor, în contextul prelucrării datelor cu caracter personal ale acestora***. Ținând seama de cele mai avansate cunoștințe în domeniu, măsurile respective asigură un nivel de securitate ***cibernetică*** a rețelelor și a sistemelor informatice adecvat riscului prezentat.

Amendamentul 84

Propunere de directivă
Articolul 18 – alineatul 2 – litera g

Textul propus de Comisie	*Amendamentul*

(g) utilizarea criptografiei și a criptării.	(g) utilizarea criptografiei și a criptării ***solide***.

Amendamentul 85

Propunere de directivă
Articolul 18 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Statele membre se asigură că, atunci când au în vedere luarea măsurilor adecvate menționate la alineatul (2) litera (d), entitățile iau în considerare vulnerabilitățile specifice fiecărui prestator și furnizor de servicii, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale prestatorilor și furnizorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare.	3. Statele membre se asigură că, atunci când au în vedere luarea măsurilor adecvate ***și proporționale*** menționate la alineatul (2) litera (d), entitățile iau în considerare vulnerabilitățile specifice fiecărui prestator și furnizor de servicii, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale prestatorilor și furnizorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare. ***Autoritățile competente oferă entităților orientări cu privire la aplicarea practică și proporțională.***

Amendamentul 86

Propunere de directivă
Articolul 18 – alineatul 6 a (nou)

Textul propus de Comisie	*Amendamentul*
	6a. Statele membre acordă utilizatorului unei rețele și al unui sistem informatic furnizat de o entitate esențială sau importantă dreptul de a obține de la entitatea respectivă informații despre măsurile tehnice și organizatorice existente pentru a gestiona riscurile la adresa securității rețelei și a sistemelor informatice. Statele membre definesc limitările acestui drept.

Amendamentul 87

Propunere de directivă
Articolul 19 – alineatul 1

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

Amendamentul 88

Propunere de directivă
Articolul 20 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Statele membre se asigură că entitățile esențiale și importante notifică, fără întârzieri nejustificate, autorităților competente sau CSIRT, în conformitate cu alineatele (3) și (4), orice incident care are un impact semnificativ asupra prestării serviciilor lor**.** Dacă este ***cazul,*** entitățile respective notifică, fără întârzieri nejustificate, destinatarilor serviciilor lor incidentele care ar putea afecta în mod negativ prestarea serviciului respectiv. Statele membre se asigură că entitățile respective raportează, printre altele, orice informație care să le permită autorităților competente sau CSIRT să stabilească dacă incidentul are un impact transfrontalier.	1. Statele membre se asigură că entitățile esențiale și importante notifică, fără întârzieri nejustificate ***și, în orice caz, în 24 de ore***, autorităților competente sau CSIRT, în conformitate cu alineatele (3) și (4), orice incident care are un impact semnificativ asupra prestării serviciilor lor***, precum și autorităților competente de aplicare a legii*** dacă ***se suspectează sau se știe că natura incidentului*** este ***rău-intenționată.*** Entitățile respective notifică, fără întârzieri nejustificate, ***și, în orice caz, în 24 de ore,*** destinatarilor serviciilor lor incidentele care ar putea afecta în mod negativ prestarea serviciului respectiv ***și furnizează informații care să le permită să atenueze efectele negative ale atacurilor cibernetice. În mod excepțional, în cazul în care divulgarea publică ar putea declanșa alte atacuri cibernetice, entitățile respective pot întârzia notificarea***. Statele membre se asigură că entitățile respective raportează, printre altele, orice informație care să le permită autorităților competente sau CSIRT să stabilească dacă incidentul are un impact transfrontalier.

Amendamentul 89

Propunere de directivă
Articolul 20 – alineatul 2 – partea introductivă

Textul propus de Comisie	*Amendamentul*
2. Statele membre se asigură că entitățile esențiale și importante ***notifică, fără întârzieri nejustificate,*** autorităților competente sau CSIRT orice amenințare cibernetică semnificativă pe care entitățile respective o identifică și care ar fi putut duce la un incident semnificativ.	2. Statele membre se asigură că entitățile esențiale și importante ***sunt în măsură să notifice*** autorităților competente sau CSIRT orice amenințare cibernetică semnificativă pe care entitățile respective o identifică și care ar fi putut duce la un incident semnificativ.

Amendamentul 90

Propunere de directivă
Articolul 20 – alineatul 2 – paragraful 1

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

Amendamentul 91

Propunere de directivă
Articolul 20 – alineatul 4 – litera c – partea introductivă

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

Amendamentul 92

Propunere de directivă
Articolul 20 – alineatul 4 – litera c – punctul ii

Textul propus de Comisie	*Amendamentul*
(ii) tipul de amenințare sau de cauză principală care probabil că a declanșat incidentul;	(ii) tipul de amenințare ***cibernetică*** sau de cauză principală care probabil că a declanșat incidentul;

Amendamentul 93

Propunere de directivă
Articolul 20 – alineatul 4 – litera c – punctul iii

Textul propus de Comisie	*Amendamentul*
(iii) măsurile de atenuare aplicate și în curs.	(iii) măsurile de atenuare ***sau corective*** aplicate și în curs.

Amendamentul 94

Propunere de directivă
Articolul 20 – alineatul 6

Textul propus de Comisie	*Amendamentul*
6. După caz, mai ales dacă incidentul menționat la alineatul (1) implică două sau mai multe state membre, autoritatea competentă sau CSIRT informează celelalte state membre afectate și ENISA cu privire la incident. Astfel, autoritățile competente, echipele CSIRT și punctele unice de contact, în conformitate cu dreptul Uniunii sau cu legislația națională conformă cu dreptul Uniunii, protejează interesele de securitate și comerciale ale entității, precum și confidențialitatea informațiilor furnizate.	6. După caz, mai ales dacă incidentul menționat la alineatul (1) implică două sau mai multe state membre, autoritatea competentă sau CSIRT informează celelalte state membre afectate și ENISA cu privire la incident. ***În cazul în care incidentul afectează două sau mai multe state membre și este presupus a fi de natură infracțională, autoritatea competentă sau CSIRT informează EUROPOL.*** Astfel, autoritățile competente, echipele CSIRT și punctele unice de contact, în conformitate cu dreptul Uniunii sau cu legislația națională conformă cu dreptul Uniunii, protejează interesele de securitate și comerciale ale entității, precum și confidențialitatea

informațiilor furnizate.

Amendamentul 95

Propunere de directivă
Articolul 22 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. ENISA, în colaborare cu statele membre, elaborează avize și orientări în ceea ce privește domeniile tehnice care ar trebui să fie examinate în legătură cu alineatul (1), precum și în ceea ce privește standardele deja existente, inclusiv standardele naționale ale statelor membre, care ar permite reglementarea acestor domenii.	2. ENISA, ***după consultarea CEPD și*** în colaborare cu statele membre, elaborează avize și orientări în ceea ce privește domeniile tehnice care ar trebui să fie examinate în legătură cu alineatul (1), precum și în ceea ce privește standardele deja existente, inclusiv standardele naționale ale statelor membre, care ar permite reglementarea acestor domenii.

Amendamentul 96

Propunere de directivă
Articolul 23 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Pentru a contribui la securitatea, stabilitatea și reziliența DNS, statele membre se asigură că ***registrele*** TLD ***și entitățile care prestează servicii de înregistrare*** a ***numelor de domenii pentru TLD*** colectează și mențin date exacte și complete privind înregistrarea numelor de domenii într-o bază de date dedicată, ***cu diligența necesară, sub rezerva legislației*** Uniunii în materie de protecție a datelor ***î*** cu caracter personal.	1. Pentru a contribui la securitatea, stabilitatea și reziliența DNS, statele membre se asigură că TLD ***dispun de politici și proceduri pentru*** a ***garanta că se*** colectează și ***se*** mențin date exacte și complete privind înregistrarea numelor de domenii într-o bază de date dedicată, ***în conformitate cu legislația*** Uniunii în materie de protecție a datelor cu caracter personal. ***Statele membre se asigură că aceste politici și proceduri sunt puse la dispoziția publicului.***

Amendamentul 97

Propunere de directivă
Articolul 23 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Statele membre se asigură că bazele de date cu datele de înregistrare a numelor de domenii menționate la alineatul (1) conțin ***informații relevante*** pentru identificarea și contactarea titularilor numelor de domenii și a punctelor de contact care administrează numele de domenii în cadrul TLD-urilor.	2. Statele membre se asigură că bazele de date cu datele de înregistrare a numelor de domenii menționate la alineatul (1) conțin ***informațiile necesare*** pentru identificarea și contactarea titularilor numelor de domenii***, adică numele lor, adresa lor fizică și adresa de e-mail, precum și numărul lor de telefon,*** și a punctelor de contact care administrează numele de domenii în cadrul TLD-urilor.

Amendamentul 98

Propunere de directivă
Articolul 23 – alineatul 3

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

Justificare

Acest alineat a fost integrat în articolul 23 alineatul (1).

Amendamentul 99

Propunere de directivă
Articolul 23 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD publică, fără întârzieri	4. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD publică, ***în***

nejustificate după înregistrarea unui nume de domeniu, date de înregistrare a ***domeniului care nu sunt date cu caracter personal***.	***conformitate cu articolul 6 alineatul (1) litera (c) și cu articolul 6 alineatul (3) din Regulamentul (UE) 2016/679 și*** fără întârzieri nejustificate după înregistrarea unui nume de domeniu, ***anumite*** date de înregistrare a ***numelor de domeniu, cum ar fi numele domeniului și numele persoanei juridice***.

Amendamentul 100

Propunere de directivă
Articolul 23 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD oferă acces la datele de înregistrare a numelor de domenii specifice în baza unor cereri legale și justificate în mod corespunzător ale ***solicitanților*** de ***acces legitimi***, în conformitate cu legislația Uniunii în materie de protecție a datelor. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD răspund fără întârzieri nejustificate la toate cererile de acces. Statele membre se asigură că politicile și procedurile de divulgare a unor astfel de date sunt puse la dispoziția publicului.	5. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD oferă acces la datele de înregistrare a numelor de domenii specifice în baza unor cereri legale și justificate în mod corespunzător ale ***autorităților publice, inclusiv ale autorităților competente, în temeiul prezentei directive sau al dreptului național, pentru prevenirea, anchetarea sau urmărirea infracțiunilor, sau ale autorităților*** de ***supraveghere în temeiul Regulamentului (UE) 2016/679***, în conformitate cu legislația Uniunii în materie de protecție a datelor. Statele membre se asigură că registrele TLD și entitățile care prestează servicii de înregistrare a numelor de domenii pentru TLD răspund fără întârzieri nejustificate la toate cererile de acces ***legale și notificate în mod corespunzător***. Statele membre se asigură că politicile și procedurile de divulgare a unor astfel de date sunt puse la dispoziția publicului.

Amendamentul 101

Propunere de directivă
Articolul 24 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. În cazul în care o entitate menționată la alineatul (1) nu este stabilită în Uniune, dar oferă servicii în Uniune, aceasta desemnează un reprezentant în Uniune. Reprezentantul se stabilește în unul dintre statele membre în care se oferă serviciile. O astfel de entitate se consideră sub jurisdicția statului membru în care este stabilit reprezentantul. În absența unui reprezentant desemnat în Uniune în temeiul prezentului articol, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității pentru nerespectarea obligațiilor care îi revin în temeiul prezentei directive.	3. În cazul în care o entitate menționată la alineatul (1) nu este stabilită în Uniune, dar oferă servicii în Uniune, aceasta desemnează un reprezentant în Uniune. Reprezentantul se stabilește în unul dintre statele membre în care se oferă serviciile. ***Fără a aduce atingere competențelor autorităților de supraveghere în temeiul Regulamentului (UE) 2016/679,*** o astfel de entitate se consideră sub jurisdicția statului membru în care este stabilit reprezentantul. În absența unui reprezentant desemnat în Uniune în temeiul prezentului articol, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității pentru nerespectarea obligațiilor care îi revin în temeiul prezentei directive.

Amendamentul 102

Propunere de directivă
Articolul 25 – alineatul 1 – partea introductivă

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

Amendamentul 103

Propunere de directivă
Articolul 26 – alineatul 1 – partea introductivă

Textul propus de Comisie	*Amendamentul*
1. Fără a aduce atingere Regulamentului (UE) 2016/679, statele membre se asigură că entitățile esențiale și	1. Fără a aduce atingere Regulamentului (UE) 2016/679 ***sau Directivei 2002/58/CE***, statele membre se

importante pot face schimb reciproc de informații relevante în materie de securitate cibernetică, inclusiv de informații referitoare la amenințări cibernetice, vulnerabilități, indicatori de compromis, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, în cazul în care un astfel de schimb de informații:	asigură că entitățile esențiale și importante pot face schimb reciproc de informații relevante în materie de securitate cibernetică, inclusiv de informații referitoare la amenințări cibernetice, vulnerabilități, indicatori de compromis, tactici, tehnici și proceduri, alerte de securitate cibernetică și instrumente de configurare, ***precum și locul în care se află atacatorul sau identitatea sa*** în cazul în care un astfel de schimb de informații:

Amendamentul 104

Propunere de directivă
Articolul 28 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Autoritățile competente lucrează în strânsă cooperare cu autoritățile de ***protecție a datelor*** în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal.	2. Autoritățile competente lucrează în strânsă cooperare cu autoritățile de ***supraveghere*** în cazul incidentelor care au ca rezultat încălcarea securității ***datelor cu caracter personal, fără a aduce atingere competențelor, sarcinilor și atribuțiilor autorităților de supraveghere în temeiul Regulamentului (UE) 2016/679. În acest scop, autoritățile competente și autoritățile de supraveghere fac schimb de informații relevante pentru domeniul lor de competență. În plus, la cererea autorităților de supraveghere competente, autoritățile competente le furnizează acestora toate informațiile obținute în contextul oricăror audituri și investigații care se referă la prelucrarea datelor cu caracter personal.***

Amendamentul 105

Propunere de directivă
Articolul 29 – alineatul 4 – litera h

Textul propus de Comisie	*Amendamentul*
(h) de a dispune ca entitățile respective să facă publice într-un mod	***eliminat***

specific aspectele legate de nerespectarea obligațiilor prevăzute în prezenta directivă;

Amendamentul 106

Propunere de directivă
Articolul 29 – alineatul 5 – litera b

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

Amendamentul 107

Propunere de directivă
Articolul 29 – alineatul 5 – paragraful 1

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

Amendamentul 108

Propunere de directivă
Articolul 29 – alineatul 7 – litera c

Textul propus de Comisie	*Amendamentul*
(c) daunele ***reale cauzate*** sau ***pierderile suferite ori daunele*** sau pierderile ***potențiale care ar fi putut fi cauzate***, în măsura în care acestea pot fi determinate. La evaluarea acestui aspect, se ține seama, printre altele, de pierderile financiare sau economice reale sau potențiale, de efectele asupra altor servicii și de numărul de utilizatori afectați sau potențial afectați;	(c) daunele ***materiale*** sau ***morale reale cauzate*** sau pierderile ***suferite***, în măsura în care acestea pot fi determinate. La evaluarea acestui aspect, se ține seama, printre altele, de pierderile financiare sau economice reale sau potențiale, de efectele asupra altor servicii și de numărul de utilizatori afectați sau potențial afectați;

Amendamentul 109

Propunere de directivă
Articolul 29 – alineatul 7 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(ca) orice încălcare anterioară relevantă comisă de entitatea în cauză;

Amendamentul 110

Propunere de directivă
Articolul 29 – alineatul 7 – litera cb (nouă)

Textul propus de Comisie	*Amendamentul*
	(cb) modul în care încălcarea a fost adusă la cunoștința autorității competente, în special dacă și în ce măsură entitatea a notificat încălcarea;

Amendamentul 111

Propunere de directivă
Articolul 29 – alineatul 7 – litera g

Textul propus de Comisie	*Amendamentul*
(g) nivelul de cooperare ***al persoanei (persoanelor) fizice sau juridice considerate responsabile cu autoritățile***	(g) nivelul de cooperare ***cu autoritățile competente pentru a remedia încălcarea și a atenua posibilele efecte negative ale***

competente.	***încălcărilor;***

Amendamentul 112

Propunere de directivă
Articolul 29 – alineatul 7 – litera ga (nouă)

Textul propus de Comisie	*Amendamentul*
	(ga) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

Amendamentul 113

Propunere de directivă
Articolul 29 – alineatul 9

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

Amendamentul 114

Propunere de directivă
Articolul 30 – alineatul 4 – litera g

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

Amendamentul 115

Propunere de directivă
Articolul 30 – alineatul 4 – litera h

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

Amendamentul 116

Propunere de directivă
Articolul 31 – alineatul 2

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

Amendamentul 117

Propunere de directivă
Articolul 31 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. ***Atunci când se ia decizia*** de a impune o amendă administrativă și se decide cuantumul acesteia în fiecare caz în parte, se acordă atenția cuvenită, cel puțin, elementelor prevăzute la articolul 29 alineatul (7).	3. ***Decizia*** de a impune o amendă administrativă ***depinde de circumstanțele fiecărui caz în parte*** și ***atunci când*** se decide cuantumul acesteia în fiecare caz în parte, se acordă atenția cuvenită, cel puțin, elementelor prevăzute la articolul 29 alineatul (7).

Amendamentul 118

Propunere de directivă
Articolul 32 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. În cazul în care autoritățile competente au indicii că încălcarea de către o entitate esențială sau importantă a obligațiilor prevăzute la articolele 18 și 20 atrage după sine o încălcare a securității datelor cu caracter personal, astfel cum este definită la articolul 4 alineatul (12) din Regulamentul (UE) nr. 2016/679, care este notificată în temeiul articolului 33 din regulamentul respectiv, acestea informează ***într-un*** termen ***rezonabil*** autoritățile de supraveghere competente în temeiul articolelor 55 și 56 din regulamentul respectiv.	1. În cazul în care autoritățile competente au indicii că încălcarea de către o entitate esențială sau importantă a obligațiilor prevăzute la articolele 18 și 20 atrage după sine o încălcare a securității datelor cu caracter personal, astfel cum este definită la articolul 4 alineatul (12) din Regulamentul (UE) nr. 2016/679, care este notificată în temeiul articolului 33 din regulamentul respectiv, acestea informează ***fără întârzieri nejustificate și, în orice caz, în*** termen ***de 24 de ore*** autoritățile de supraveghere competente în temeiul articolelor 55 și 56 din regulamentul respectiv.

Amendamentul 119

Propunere de directivă
Articolul 32 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. În cazul în care autoritatea de supraveghere competentă în temeiul Regulamentului (UE) 2016/679 este	3. În cazul în care autoritatea de supraveghere competentă în temeiul Regulamentului (UE) 2016/679 este

stabilită într-un alt stat membru decât autoritatea competentă, aceasta din urmă ***poate informa*** autoritatea de supraveghere stabilită în același stat membru.	stabilită într-un alt stat membru decât autoritatea competentă, aceasta din urmă ***informează*** autoritatea de supraveghere stabilită în același stat membru.

Amendamentul 120

Propunere de directivă
Articolul 34 a (nou)

Textul propus de Comisie	*Amendamentul*
	Articolul 34a
	Răspundere pentru nerespectarea obligațiilor
	Fără a aduce atingere oricărei căi de atac administrative sau fără caracter judiciar disponibile, beneficiarii serviciilor furnizate de entități esențiale și importante care au suferit daune ca urmare a nerespectării de către furnizori a prezentei directive au dreptul la o cale de atac judiciară efectivă.

Amendamentul 121

Propunere de directivă
Articolul 35 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Comisia revizuiește ***periodic*** funcționarea prezentei directive și prezintă un raport Parlamentului European și Consiliului. Raportul evaluează în special relevanța sectoarelor, a subsectoarelor, a dimensiunii și a tipului de entități menționate în anexele I și II pentru funcționarea economiei și a societății în ceea ce privește securitatea cibernetică. În acest scop și în vederea intensificării cooperării strategice și operaționale, Comisia ține cont de rapoartele grupului de cooperare și ale rețelei CSIRT privind experiența obținută la nivel strategic și operațional. Primul raport se transmite până la… [***54*** de luni de la data intrării în vigoare a prezentei	Comisia revizuiește funcționarea prezentei directive ***o dată la trei ani*** și prezintă un raport Parlamentului European și Consiliului. Raportul evaluează în special ***măsura în care directiva a contribuit la atingerea celui mai înalt nivel de securitate și integritate a rețelelor și informațiilor, oferind în același timp o protecție optimă a vieții private și a datelor cu caracter personal, precum și*** relevanța sectoarelor, a subsectoarelor, a dimensiunii și a tipului de entități menționate în anexele I și II pentru funcționarea economiei și a societății în ceea ce privește securitatea cibernetică. În acest scop și în vederea intensificării cooperării strategice și operaționale,

directive].	Comisia ține cont de rapoartele grupului de cooperare și ale rețelei CSIRT privind experiența obținută la nivel strategic și operațional. Primul raport se transmite până la… [***36*** de luni de la data intrării în vigoare a prezentei directive].

Amendamentul 122

Propunere de directivă
Anexa I – Punctul 5 (Sectorul sănătății) – liniuța 6 (nouă)

Textul propus de Comisie

Sectorul	Subsectorul	Tipul de entitate
5. Sectorul sănătății		– Furnizorii de servicii medicale menționați la articolul 3 litera (g) din Directiva 2011/24/UE (90) – Laboratoarele de referință ale UE menționate la articolul 15 din Regulamentul XXXX/XXXX privind amenințările transfrontaliere grave pentru sănătate[91] – Entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor menționate la articolul 1 punctul 2 din Directiva 2001/83/CE (92) – Entitățile care fabrică produse farmaceutice de bază și preparate farmaceutice menționate în secțiunea C diviziunea 21 din NACE Rev. 2 – Entitățile care fabrică dispozitive medicale considerate esențiale în contextul unei urgențe de sănătate publică („lista dispozitivelor esențiale pentru urgența de sănătate publică”) menționate la articolul 20 din Regulamentul XXXX[93]

[91] [Regulamentul Parlamentului European și al Consiliului privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 1082/2013/UE, trimiterea urmând să fie actualizată după adoptarea propunerii COM(2020)727 final].

[92] Directiva 2001/83/CE a Parlamentului European și a Consiliului din 6 noiembrie 2001 de instituire a unui cod comunitar cu privire la medicamentele de uz uman (JO L 311, 28.11.2001, p. 67).

[93] [Regulamentul Parlamentului European și al Consiliului privind consolidarea rolului Agenției Europene pentru Medicamente în ceea ce privește pregătirea pentru situații de criză în domeniul medicamentelor și al dispozitivelor medicale și gestionarea acestora, trimiterea urmând să fie actualizată după adoptarea propunerii COM(2020)725 final].

Amendamentul

Sectorul	Subsectorul	Tipul de entitate
5. Sectorul sănătății		– Furnizorii de servicii medicale menționați la articolul 3 litera (g) din Directiva 2011/24/UE (90) – Laboratoarele de referință ale UE menționate la articolul 15 din Regulamentul XXXX/XXXX privind amenințările transfrontaliere grave pentru sănătate[91] – Entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor menționate la articolul 1 punctul 2 din Directiva 2001/83/CE (92) – Entitățile care fabrică produse farmaceutice de bază și preparate farmaceutice menționate în secțiunea C diviziunea 21 din NACE Rev. 2 – Entitățile care fabrică dispozitive medicale considerate esențiale în contextul unei urgențe de sănătate publică („lista dispozitivelor esențiale pentru urgența de sănătate publică”) menționate la articolul 20 din Regulamentul XXXX[93] ***– Entitățile titulare ale unei autorizații de distribuție menționate la articolul 79 din Directiva 2001/83/CE***

[91] [Regulamentul Parlamentului European și al Consiliului privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 1082/2013/UE, trimiterea urmând să fie actualizată după adoptarea propunerii COM(2020)727 final].

[92] Directiva 2001/83/CE a Parlamentului European și a Consiliului din 6 noiembrie 2001 de instituire a unui cod comunitar cu privire la medicamentele de uz uman (JO L 311, 28.11.2001, p. 67).

[93] [Regulamentul Parlamentului European și al Consiliului privind consolidarea rolului Agenției Europene pentru Medicamente în ceea ce privește pregătirea pentru situații de criză în domeniul medicamentelor și al dispozitivelor medicale și gestionarea acestora, trimiterea urmând să fie actualizată după adoptarea propunerii COM(2020)725 final].

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

Titlu	Măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, abrogarea Directivei (UE) 2016/1148
Referințe	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Comisie competentă Data anunțului în plen	ITRE 21.1.2021
Aviz emis de către Data anunțului în plen	LIBE 21.1.2021
Comisii asociate - data anunțului în plen	20.5.2021
Raportor/Raportoare pentru aviz Data numirii	Lukas Mandl 12.4.2021
Examinare în comisie	16.6.2021 3.9.2021 11.10.2021
Data adoptării	12.10.2021
Rezultatul votului final	+: 44 –: 14 0: 4
Membri titulari prezenți la votul final	Magdalena Adamowicz, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Maria Grapini, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Javier Zarzalejos
Membri supleanți prezenți la votul final	Olivier Chastel, Tanja Fajon, Jan-Christoph Oetjen, Philippe Olivier, Anne-Sophie Pelletier, Thijs Reuten, Rob Rooken, Maria Walsh

VOT FINAL PRIN APEL NOMINAL
ÎN COMISIA SESIZATĂ PENTRU AVIZ

44	+
ID	Nicolas Bay, Nicolaus Fest, Peter Kofod, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche
NI	Laura Ferrara
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Elissavet Vozemberg-Vrionidi, Maria Walsh, Javier Zarzalejos
Renew	Olivier Chastel, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Jan-Christoph Oetjen, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Marina Kaljurand, Juan Fernando López Aguilar, Javier Moreno Sánchez, Thijs Reuten, Birgit Sippel, Bettina Vollath
Verts/ALE	Damien Carême

14	-
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Rob Rooken, Jadwiga Wiśniewska
ID	Marcel de Graaff
NI	Martin Sonneborn, Milan Uhrík
Verts/ALE	Patrick Breyer, Saskia Bricmont, Terry Reintke, Diana Riba i Giner, Tineke Strik

4	0
The Left	Pernando Barrena Arza, Clare Daly, Cornelia Ernst, Anne-Sophie Pelletier

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri