

Bruxelles, 29 martie 2022
(OR. en)

**Dosar interinstituțional:
2022/0084 (COD)**

**7670/22
ADD 3**

**CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34**

PROPUNERE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	22 martie 2022
Destinatar:	DI Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2022) 119 final - Annex 3
Subiect:	ANEXĂ la Propunerea de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii

În anexă, se pune la dispoziția delegațiilor documentul COM(2022) 119 final - Annex 3.

Anexă: COM(2022) 119 final - Annex 3



COMISIA
EUROPEANĂ

Bruxelles, 22.3.2022
COM(2022) 119 final

ANNEX 3

ANEXĂ

la

**Propunerea de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL
CONSILIULUI**

privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii

{SWD(2022) 65 final} - {SWD(2022) 66 final}

ANEXA III

Măsuri pentru protecția fizică a informațiilor UE clasificate („IUEC”)

Echipamente și măsuri organizatorice pentru protecția fizică a IUEC

1. O zonă administrativă trebuie să îndeplinească următoarele cerințe:
 - (a) să aibă un perimetru delimitat în mod vizibil care să permită verificarea persoanelor și, dacă este posibil, a vehiculelor;
 - (b) să asigure faptul că ferestrele care ar putea permite accesul vizual neautorizat la IUEC în zonă sunt opace sau sunt prevăzute cu storuri, perdele sau cu alte soluții de acoperire;
 - (c) accesul neînsoțit trebuie permis numai persoanelor care sunt autorizate în mod corespunzător de către autoritatea de securitate a instituției sau a organului în cauză al Uniunii;
 - (d) toate celelalte persoane sunt însoțite în permanență sau sunt supuse unor controale echivalente.
2. În plus față de cerințele prevăzute la punctul 1, o zonă securizată trebuie să îndeplinească și următoarele cerințe:
 - (a) să aibă un perimetru delimitat și protejat în mod vizibil în care intrarea și ieșirea să fie controlate în permanență;
 - (b) să nu fie prevăzută cu linii de comunicații, telefoane sau alte dispozitive de comunicare și echipamente electrice sau electronice neautorizate;
 - (c) să fie dotată cu un sistem de control al accesului și cu un sistem de detecție a intruziunilor („SDI”) prin monitorizare în timp real, precum și cu personal de securitate pentru intervenție;
 - (d) să fie inspectată la sfârșitul programului normal de lucru și la intervale aleatorii în afara programului normal de lucru, în cazul în care nu este ocupată de personalul de serviciu 24 de ore din 24 și nu există o monitorizare SDI în timp real;
 - (e) să fie gestionată de personal de securitate instruit, supravegheat și autorizat în mod corespunzător;
 - (f) să dispună de proceduri operaționale de securitate care să includă următoarele elemente:
 - (i) nivelul IUEC care pot fi manipulate, discutate și stocate în zona respectivă;
 - (ii) măsurile de supraveghere și de protecție care trebuie asigurate;
 - (iii) persoanele autorizate să aibă acces neînsoțit în zonă în baza autorizației lor de acces la IUEC și a necesității de a cunoaște;
 - (iv) după caz, procedurile pentru însoțirea persoanelor sau pentru protecția IUEC în cazul autorizării accesului altor persoane în zona respectivă;
 - (v) orice altă măsură și procedură relevantă.
3. În cazul în care accesul într-o zonă securizată este echivalent cu accesul direct la informațiile clasificate aflate în aceasta, zona respectivă trebuie să fie stabilită ca zonă de clasă I, iar în caz contrar, zona trebuie să fie stabilită ca zonă de clasă II.

Pentru ambele clase de zonă securizată, menționate la primul paragraf și în plus față de cerințele prevăzute la punctul 2, departamentul/ofițerul de securitate al instituției sau al organului în cauză al Uniunii trebuie să indice în mod clar nivelul cel mai ridicat al clasificării de securitate a informațiilor deținute în mod obișnuit în zonă și trebuie să delimiteze în mod clar un perimetru care să permită verificarea persoanelor și, dacă este posibil, a vehiculelor.

Instituțiile și organele Uniunii trebuie să se asigure că persoanele care intră într-o zonă securizată îndeplinesc următoarele criterii:

- (a) solicită o autorizație specifică pentru a intra în zonă;
 - (b) sunt însoțite în permanență;
 - (c) dețin o autorizare de securitate corespunzătoare, cu excepția cazului în care se iau măsuri pentru a se asigura că nu este posibil accesul la IUEC.
4. O zonă securizată protejată împotriva interceptării pasive și active trebuie desemnată ca zonă securizată din punct de vedere tehnic. Următoarele cerințe se aplică în plus față de cele pentru zonele securizate:
- (a) aceasta trebuie să fie dotată cu un SDI, să fie încuiată atunci când nu este ocupată și să fie păzită atunci când este ocupată. Toate cheile trebuie să fie gestionate în conformitate cu articolul 29 alineatul (3);
 - (b) trebuie să fie inspectată periodic, din punct de vedere fizic sau tehnic sau din ambele puncte de vedere de către autoritatea de securitate a instituției sau a organului în cauză al Uniunii. Astfel de inspecții trebuie efectuate și în urma accesului neautorizat sau a suspiciunii de acces neautorizat;
 - (c) trebuie să aibă o protecție acustică și TEMPEST corespunzătoare.
5. Toate persoanele care intră în zonele securizate din punct de vedere tehnic trebuie să respecte cerințele prevăzute la punctul 3.
6. Pot fi instituite temporar zone securizate și zone securizate din punct de vedere tehnic într-o zonă administrativă, în scopul unei reuniuni clasificate sau în orice alt scop similar.
7. Camerele tezaur trebuie construite în cadrul zonelor securizate. O cameră tezaur este o încăpăre cu construcție fizică consolidată pentru care pereții, podelele, tavanele, ferestrele și ușile cu încuietori sunt aprobate de autoritatea de securitate a instituției sau a organului în cauză al Uniunii. Aceste încăperi trebuie să ofere o protecție echivalentă cu cea a unui container de securitate aprobat pentru stocarea IUEC cu același nivel de clasificare.

Măsuri de protecție fizică pentru manipularea și stocarea IUEC

8. IUEC clasificate RESTREINT UE/EU RESTRICTED trebuie manipulate și stocate în oricare dintre următoarele zone:
- (a) într-o zonă securizată;
 - (b) într-o zonă administrativă, cu condiția ca IUEC să fie protejate împotriva accesului persoanelor neautorizate;
 - (c) în afara unei zone securizate sau a unei zone administrative, cu condiția ca deținătorul să se fi angajat să respecte măsurile compensatorii decise de autoritatea de securitate a fiecărei instituții și a fiecărui organ al Uniunii.

9. IUEC clasificate RESTREINT UE/EU RESTRICTED trebuie stocate în mobilier de birou încuiat dintr-o zonă administrativă sau o zonă securizată. Acestea pot fi stocate temporar în afara unei zone administrative sau a unei zone securizate, cu condiția ca deținătorul să se fi angajat să stocheze documentele în cauză în mobilier de birou încuiat corespunzător atunci când acestea nu sunt citite sau discutate.
10. Instituțiile și organele Uniunii pot manipula și stoca informații RESTREINT UE/EU RESTRICTED în afara amplasamentelor lor, cu condiția ca informațiile relevante să fie protejate în mod corespunzător. În acest scop, instituțiile și organele Uniunii trebuie să respecte măsurile prevăzute la punctul 8 litera (c).
11. Informațiile CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET trebuie manipulate și stocate în una dintre următoarele zone:
 - (a) într-o zonă securizată;
 - (b) într-o zonă administrativă, cu condiția ca IUEC să fie protejate împotriva accesului persoanelor neautorizate;
 - (c) în afara unei zone securizate sau a unei zone administrative în cazul în care volumul și timpul sunt limitate și cu condiția ca deținătorul să se fi angajat să respecte măsurile compensatorii decise de autoritatea de securitate a instituției sau a organului în cauză al Uniunii. În plus, deținătorul IUEC trebuie să ia următoarele măsuri:
 - (i) să notifice responsabilului cu registrul relevant cu privire la faptul că documente clasificate sunt manipulate în afara zonelor protejate;
 - (ii) să păstreze documentul sub controlul său în permanență.
12. Informațiile CONFIDENTIEL UE/EU CONFIDENTIAL și SECRET UE/EU SECRET trebuie stocate într-o zonă securizată acreditată la acest nivel de către autoritatea competentă de acreditare în materie de securitate a instituției sau a organului în cauză al Uniunii, fie în interiorul unui container de securitate, fie în interiorul unei camere tezaur.
13. Documentele clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau la un nivel superior pot fi copiate numai de către responsabilul cu registrul relevant.
14. Informațiile TRES SECRET UE/EU TOP SECRET trebuie manipulate și stocate într-o zonă securizată acreditată la acest nivel. În acest scop, instituțiile și organele Uniunii pot încheia acordurile necesare pentru a utiliza o zonă securizată găzduită și acreditată la nivelul corespunzător de către autoritatea de acreditare în materie de securitate a unei alte instituții sau a unui alt organ al Uniunii.
15. Informațiile TRES SECRET UE/EU TOP SECRET trebuie stocate într-o zonă securizată, acreditată la acest nivel de către autoritatea de acreditare în materie de securitate a respectivei instituții sau organ competent al Uniunii, în una dintre următoarele condiții:
 - (a) într-un container de securitate aprobat de autoritatea de securitate a fiecărei instituții și organ al Uniunii, cu unul dintre următoarele controale suplimentare:
 - (i) protecție continuă sau verificări efectuate de personalul de securitate sau de serviciu deținător de autorizare de securitate;
 - (ii) un SDI aprobat și personal de securitate de intervenție;
 - (b) într-o cameră tezaur dotată cu SDI și personal de securitate de intervenție.