

Bruxelles, 29 martie 2022
(OR. en)

Dosar interinstituțional:
2022/0084 (COD)

7670/22
ADD 5

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
Destinatar:	DI Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2022) 119 final - Annex 5
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 5.

Anexă: COM(2022) 119 final - Annex 5



COMISIA
EUROPEANĂ

Bruxelles, 22.3.2022
COM(2022) 119 final

ANNEX 5

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 V

Protecția informațiilor UE clasificate („IUEC”) în cadrul contractelor și al acordurilor de grant clasificate

În sensul prezentei anexe, pe lângă definițiile prevăzute în anexele II și IV, „autorizare de securitate industrială” sau „ASI” înseamnă o decizie administrativă a unei autorități naționale de securitate, a unei autorități de securitate desemnate sau a oricărei alte autorități de securitate competente conform căreia, în ceea ce privește securitatea, o unitate poate oferi un nivel de protecție adecvat pentru IUEC clasificate la un anumit nivel de clasificare de securitate.

Accesul personalului contractanților și al beneficiarilor la IUEC

1. Fiecare instituție sau organ al Uniunii cu rol de autoritate contractantă sau de autoritate care acordă grantul se asigură că respectivele contracte sau acorduri de grant clasificate conțin dispoziții care să indice că membrii personalului unui contractant, subcontractant sau beneficiar care, pentru executarea contractului, a subcontractului sau a acordului de grant clasificat, necesită acces la IUEC, pot primi acces la IUEC numai în cazul în care sunt îndeplinite următoarele condiții:
 - (a) s-a stabilit că este necesar ca aceștia să cunoască informațiile respective;
 - (b) pentru informațiile clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, acestora li s-a acordat o autorizare de securitate a personalului („ASP”) la nivelul relevant de către autoritatea națională de securitate, autoritatea de securitate desemnată sau orice altă autoritate de securitate competentă;
 - (c) aceștia au fost informați cu privire la normele de securitate aplicabile pentru protecția IUEC și au confirmat că au luat cunoștință de responsabilitățile care le revin în ceea ce privește protejarea acestor informații.
2. În cazul în care un contractant sau un beneficiar dorește să angajeze un resortisant al unei țări terțe pe un post care necesită accesul la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, contractantului sau beneficiarului respectiv îi revine responsabilitatea de a iniția procedura de acordare a autorizării de securitate pentru persoana în cauză, în conformitate cu actele cu putere de lege și normele administrative naționale aplicabile în locul în care urmează să fie acordat accesul la IUEC.

Autorizarea de securitate industrială („ASI”)

3. O autorizare de securitate industrială („ASI”) se acordă de către autoritatea națională de securitate, de către autoritatea de securitate desemnată sau de către orice altă autoritate de securitate competentă a unui stat membru pentru a atesta că, în conformitate cu actele cu putere de lege și cu normele administrative naționale, o entitate poate proteja IUEC la nivelul de clasificare adecvat (CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET) în interiorul unităților sale.
4. O instituție sau un organ al Uniunii cu rol de autoritate contractantă sau de autoritate care acordă grantul trebuie să notifice, prin intermediul autorității sale de securitate, autoritatea națională de securitate, sau autoritatea de securitate desemnată sau orice altă autoritate de securitate competentă în cazul în care este necesară o ASI pentru executarea contractului sau a acordului de grant.

5. În cazul în care, în cursul procedurii de achiziții publice sau de atribuire a grantului, pentru unitățile candidaților, ale ofertanților sau ale solicitanților este necesar să se furnizeze informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, trebuie să se solicite o ASI.
6. O instituție sau un organ al Uniunii cu rol de autoritate contractantă sau de autoritate care acordă grantul trebuie să fi primit, prin intermediul autorității sale de securitate, confirmarea unei ASI pentru candidat, ofertant sau contractant sau pentru solicitantul sau beneficiarul grantului înainte de a i se acorda accesul la IUEC.
7. În cazul în care statele membre nu eliberează ASI pentru anumite unități în temeiul legislației naționale, autoritatea contractantă sau autoritatea care acordă grantul trebuie să verifice împreună cu autoritatea națională de securitate sau cu autoritatea de securitate desemnată în cauză dacă respectivele unități sunt capabile să manipuleze IUEC la nivelul necesar.
8. Cu excepția cazurilor menționate la punctul 7, instituția sau organul Uniunii, în calitate de autoritate contractantă, nu trebuie să semneze un contract clasificat sau un acord de grant clasificat înainte de a primi confirmarea, prin intermediul autorității sale de securitate, din partea autorității naționale de securitate, a autorității de securitate desemnate relevante sau a oricărei alte autorități naționale competente, că a fost emisă o ASI corespunzătoare.
9. Retragera unei ASI de către autoritatea națională de securitate, de către autoritatea de securitate desemnată relevantă sau de către orice altă autoritate de securitate competentă constituie un motiv suficient pentru ca autoritatea contractantă sau autoritatea care acordă grantul să rezilieze un contract sau un acord de grant clasificat sau să excludă un candidat, un ofertant sau un solicitant din competiție.

Dispoziții privind licitațiile și punerea în aplicare a contractelor și a acordurilor de grant clasificate

10. În cazul în care unui candidat, unui ofertant sau unui solicitant îi sunt furnizate IUEC pe parcursul procedurii de achiziții publice sau de selecție, licitația sau cererea de propuneri trebuie să includă obligația candidatului, a ofertantului sau a solicitantului care nu este selectat de a restitui, într-un termen specificat, toate documentele clasificate.
11. Ca regulă generală, la încetarea contractului sau a acordului de grant clasificat sau la încheierea participării unui beneficiar de grant, contractantul sau beneficiarul grantului are obligația de a restitui autorității contractante sau autorității care acordă grantul toate IUEC aflate în posesia sa.
12. În anexa de securitate trebuie stabilite dispoziții specifice privind distrugerea IUEC pe durata executării contractului sau a acordului de grant clasificat ori la încetarea acestuia.
13. În cazul în care contractantul sau beneficiarul grantului este autorizat să rețină IUEC după încetarea unui contract sau a unui acord de grant clasificat, aceștia trebuie să respecte în continuare standardele minime cuprinse în prezentul regulament, iar confidențialitatea IUEC trebuie protejată de contractant sau de beneficiarul grantului.
14. Condițiile relevante pentru protecția IUEC pe care trebuie să le îndeplinească contractantul sau beneficiarul pentru a putea subcontracta trebuie să fie stabilite în licitație sau în cererea de propuneri, precum și în contractul sau acordul de grant clasificat.

15. Un contractant sau un beneficiar trebuie să obțină permisiunea autorității contractante sau a autorității care acordă grantul înainte de a subcontracta o parte a unui contract clasificat sau părți clasificate ale unui acord de grant.
16. Contractantul sau beneficiarul trebuie să fie responsabil pentru asigurarea faptului că toate activitățile de subcontractare sunt întreprinse în conformitate cu standardele minime prevăzute în prezentul regulament și nu trebuie să furnizeze IUEC unui subcontractant fără acordul scris prealabil al autorității contractante sau al autorității care acordă grantul.
17. În ceea ce privește IUEC create de contractant sau de beneficiar, instituția sau organul Uniunii, care este autoritatea contractantă sau autoritatea care acordă grantul, este considerat emitent și exercită drepturile care îi revin emitentului.
18. În cazul în care statele membre solicită o ASI sau o autorizare de securitate a personalului pentru contracte, acorduri de grant sau subcontracte la nivelul RESTREINT UE/EU RESTRICTED în conformitate cu actele cu putere de lege și cu normele administrative naționale, instituțiile și organele Uniunii, în calitate de autorități contractante sau de autorități care acordă granturile, nu trebuie să utilizeze cerințele naționale respective pentru a crea obligații suplimentare pentru alte state membre sau a exclude de la contracte, acorduri de grant sau subcontracte conexe ofertanții, solicitanții, contractanții, beneficiarii sau subcontractanții din state membre care nu au astfel de cerințe privind ASI sau autorizarea de securitate a personalului în legătură cu accesul la informații clasificate RESTREINT UE/EU RESTRICTED și nici să îi pună în concurență în acest sens.

Vizite în legătură cu contracte și acorduri de grant clasificate

19. În cazul în care instituțiile și organele Uniunii, contractanții, beneficiarii sau subcontractanții au nevoie de acces la informații clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET în incintele celeilalte părți în contextul punerii în aplicare a unui contract sau acord de grant clasificat, vizitele trebuie să fie organizate în colaborare cu autoritățile naționale de securitate, cu autoritățile de securitate desemnate sau cu orice altă autoritate de securitate competentă.
20. Vizitele menționate la punctul 19 fac obiectul următoarelor cerințe:
 - (a) vizita trebuie să aibă un scop oficial legat de un contract clasificat sau de un acord de grant clasificat;
 - (b) pentru a avea acces la IUEC utilizate sau generate în executarea unui contract sau a unui acord de grant clasificat, vizitatorii trebuie să dețină o autorizare de securitate a personalului la nivelul necesar și să existe necesitatea de a cunoaște;
 - (c) o cerere oficială de vizită trebuie transmisă fie autorității naționale de securitate sau autorității de securitate desemnate relevante pentru unitatea respectivă, fie autorității de securitate a instituției sau a organului în cauză al Uniunii, cu cel puțin 15 zile înainte de data vizitei.
21. În contextul unor proiecte specifice, autoritatea națională de securitate sau autoritatea de securitate desemnată relevantă și autoritatea de securitate a instituției sau a organului în cauză al Uniunii pot conveni asupra unei proceduri prin care vizitele în legătură cu un anumit contract sau grant clasificat să poată fi organizate direct de ofițerul de securitate al vizitatorului împreună cu ofițerul de securitate al unității care

urmează să fie vizitată. O astfel de procedură excepțională trebuie să fie stabilită în instrucțiunile de securitate pentru program sau proiect sau în alte acorduri specifice.

22. Vizitele care implică accesul la informații clasificate RESTREINT UE/EU RESTRICTED trebuie să fie organizate direct între entitatea expeditoare și entitatea destinatară.

Transmiterea electronică de IUEC în legătură cu contractele și acordurile de grant clasificate

23. Manipularea și transmiterea electronică a IUEC trebuie efectuate în conformitate cu capitolul 5 secțiunea 5.

SIC deținute de un contractant, beneficiar sau subcontractant și utilizate pentru manipularea și stocarea IUEC în vederea executării contractului sau a acordului de grant trebuie să facă obiectul acreditării de către autoritatea de acreditare în materie de securitate („AAS”) a țării terțe sau a organizației internaționale sub a cărei autoritate funcționează contractantul, beneficiarul sau subcontractantul.

Orice transmitere electronică de IUEC în contextul contractelor și al acordurilor de grant clasificate trebuie să fie protejată prin produse criptografice aprobate în conformitate cu articolul 42.

24. Acreditarea în materie de securitate a sistemelor informatice și de comunicații ale contractanților sau al beneficiarilor care manipulează IUEC de nivelul RESTREINT UE/EU RESTRICTED și orice interconexiune în acest sens pot fi delegate ofițerului de securitate al contractantului sau al beneficiarului în cazul în care actele cu putere de lege și normele administrative naționale permit acest lucru.

În cazul în care sarcina de acreditare în materie de securitate este delegată, contractantul sau beneficiarul trebuie să fie responsabil de punerea în aplicare a cerințelor de securitate descrise în anexa de securitate atunci când manipulează informații RESTREINT UE/EU RESTRICTED în cadrul sistemului său informatic și de comunicații. Autoritățile naționale de securitate sau autoritățile de securitate desemnate relevante și AAS păstrează responsabilitatea pentru protecția informațiilor clasificate RESTREINT UE/EU RESTRICTED manipulate sau stocate de contractant sau de beneficiar, precum și dreptul de a inspecta măsurile de securitate luate de acesta.

În plus, contractantul sau beneficiarul trebuie să ofere instituției sau organului Uniunii, în calitate de autoritate contractantă sau autoritate care acordă grantul, și, atunci când acest lucru este impus prin actele cu putere de lege și normele administrative naționale, AAS naționale competente, o declarație de conformitate care să certifice faptul că sistemul informatic și de comunicații al contractantului sau al beneficiarului și interconexiunile aferente au fost acreditate pentru manipularea și stocarea IUEC la nivelul RESTREINT UE/EU RESTRICTED.

Transportul personal al IUEC în legătură cu contractele și acordurile de grant clasificate

25. Transportul personal al informațiilor clasificate legate de contractele și acordurile de grant clasificate trebuie să facă obiectul unor cerințe stricte de securitate.
26. Informațiile RESTREINT UE/EU RESTRICTED pot fi transportate personal de membrii personalului contractantului sau al beneficiarului în cadrul Uniunii, cu condiția să fie îndeplinite următoarele cerințe:

- (a) plicul sau ambalajul folosit să fie opac și să nu poarte nicio indicație privind clasificarea conținutului său;
 - (b) purtătorul să rămână în permanență în posesia informațiilor clasificate;
 - (c) plicul sau ambalajul să nu fie deschis înainte de a ajunge la destinația finală.
27. În ceea ce privește informațiile clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, transportul personal de către membrii personalului contractantului sau al beneficiarului pe teritoriul unui stat membru este organizat în prealabil de către entitățile expeditoare împreună cu entitățile destinate.
- Autoritatea sau unitatea expeditoare informează autoritatea sau unitatea destinată cu privire la detaliile pachetului transportat, inclusiv referința, clasificarea, ora estimată a sosirii și numele curierului. Transportul personal de acest tip este permis cu condiția îndeplinirii următoarelor cerințe:
- (a) informațiile clasificate să fie transportate într-un plic sau ambalaj dublu;
 - (b) plicul sau ambalajul exterior să fie securizat și să nu poarte nicio indicație a clasificării conținutului său, iar plicul interior să poarte indicația nivelului de clasificare;
 - (c) purtătorul să rămână în permanență în posesia IUEC;
 - (d) plicul sau ambalajul să nu fie deschis înainte de a ajunge la destinația finală;
 - (e) plicul sau ambalajul să fie transportat într-o servietă cu încuietoare sau într-un recipient similar aprobat, având o dimensiune și o greutate care îi permit purtătorului să îl păstreze în permanență asupra sa;
 - (f) curierul să dețină un certificat de curier eliberat de autoritatea sa de securitate competentă, prin care este autorizat să transporte pachetul clasificat astfel cum este identificat.
28. În ceea ce privește transportul personal de către membrii personalului contractantului sau al beneficiarului al informațiilor clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET dintr-un stat membru în altul, în plus față de cerințele prevăzute la punctul 27, se aplică și următoarele norme suplimentare:
- (a) curierul este responsabil de păstrarea în siguranță a materialului clasificat transportat, până la momentul în care acesta este înmănat destinatarului;
 - (b) în eventualitatea unei încălcări a securității, autoritatea națională de securitate sau autoritatea de securitate desemnată a expeditorului poate solicita ca autoritățile din țara în care a avut loc încălcarea să desfășoare o investigație, să raporteze constatările în urma acesteia și să ia măsurile legale sau alte măsuri, după caz;
 - (c) curierul trebuie să fie informat în prealabil cu privire la toate obligațiile de securitate care trebuie respectate în timpul transportului și trebuie să semneze un document corespunzător de luare la cunoștință;
 - (d) instrucțiunile destinate curierului trebuie să fie atașate la certificatul de curier;
 - (e) curierului trebuie să i se furnizeze o descriere a pachetului transportat și itinerarul;

- (f) certificatul de curier și documentele asociate trebuie restituite autorității naționale de securitate sau autorității de securitate desemnate emitente la încheierea călătoriei sau a călătoriilor sau trebuie să fie puse la dispoziție de către destinatarul certificatului de curier în scopul monitorizării;
- (g) în cazul în care autoritățile vamale, autoritățile de imigrație sau poliția de frontieră solicită examinarea și inspectarea pachetului transportat, acestora trebuie să li se permită să deschidă și să observe părți suficiente din acesta, astfel încât să stabilească faptul că nu conține alte materiale decât cele declarate;
- (h) autoritățile vamale ar trebui îndemnate să respecte autoritatea oficială a documentelor de transport și a documentelor de autorizare transportate de curier.

În cazul în care un pachet transportat este deschis de autoritățile vamale, acest lucru ar trebui realizat la distanță de persoane neautorizate și, pe cât posibil, în prezența curierului. Curierul trebuie să solicite ca pachetul transportat să fie reambalat și să le ceară autorităților care efectuează inspecția să resigileze pachetul transportat și să confirme în scris că acesta a fost deschis de ele.

29. Transportul personal de către membrii personalului contractantului sau al beneficiarului de informații clasificate până la nivelul SECRET UE/EU SECRET către o țară terță sau o organizație internațională face obiectul dispozițiilor acordului privind securitatea informațiilor încheiat între Uniunea Europeană și țara terță sau organizația internațională respectivă.

Transportul de IUEC de către serviciile de curierat comercial și ca marfă în legătură cu contracte și acorduri de grant clasificate

30. Transportul de IUEC de către serviciile de curierat comercial trebuie să se desfășoare în conformitate cu dispozițiile relevante din anexa IV.
31. În ceea ce privește transportul ca marfă al materialelor clasificate, la stabilirea măsurilor de securitate se aplică următoarele principii:
- (a) trebuie garantată securitatea în toate etapele transportului, de la punctul de plecare și până la destinația finală;
 - (b) nivelul de protecție acordat unui pachet transportat trebuie stabilit în funcție de materialul cu cel mai înalt nivel de clasificare conținut de acesta;
 - (c) societățile de transport trebuie să obțină o ASI de nivel corespunzător. În astfel de cazuri, personalul care manipulează pachetul transportat trebuie să primească o autorizare de securitate;
 - (d) înaintea oricărei deplasări transfrontaliere de materiale clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau SECRET UE/EU SECRET, expeditorul trebuie să întocmească un plan de transport aprobat de autoritatea națională de securitate, de autoritatea de securitate desemnată sau de orice altă autoritate de securitate competentă implicată;
 - (e) deplasările trebuie să se realizeze, în măsura posibilului, pe rute directe și trebuie încheiate pe atât de rapid pe cât o permit circumstanțele;
 - (f) atunci când este posibil, ar trebui să se aleagă numai rute care trec prin state membre. Rutele care trec prin țări terțe trebuie efectuate numai dacă sunt autorizate de autoritatea națională de securitate, de autoritatea de securitate desemnată sau de orice altă autoritate de securitate competentă atât din statul expeditorului, cât și din cel al destinatarului.