Council of the European Union

Brussels, 29 March 2022
(OR. en)

Interinstitutional File:
2022/0084 (COD)

7670/22
ADD 5

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

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2022) 119 final - Annex 5
Subject:	ANNEX 5 to the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information security in the institutions, bodies, offices and agencies of the Union

Delegations will find attached document COM(2022) 119 final - Annex 5.

Encl.: COM(2022) 119 final - Annex 5

EUROPEAN
COMMISSION

Brussels, 22.3.2022
COM(2022) 119 final

ANNEX 5

ANNEX

to the

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on information security in the institutions, bodies, offices and agencies of the Union

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

ANNEX V

Protection of European Union classified information ('EUCI') in classified contracts and grant agreements

For the purposes of this Annex, in addition to the definitions set out in Annexes II and IV, 'Facility security clearance' or 'FSC' means an administrative determination by an National Security Authority, a Designated Security Authority or any other competent security authority that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI to a specified security classification level.

Access to EUCI by personnel of contractors and beneficiaries

1. Each Union institution or body, as contracting or granting authority, shall ensure that classified contracts or grant agreements include provisions indicating that personnel of a contractor, subcontractor or beneficiary who, for the performance of the classified contract, subcontract or grant agreement, require access to EUCI may be granted such access only if the following conditions are met:

   (a) it has been established that they have a need-to-know;

   (b) for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, they have been granted a Personnel Security Clearance ('PSC') at the relevant level by the respective National Security Authority, Designated Security Authority or any other competent security authority;

   (c) they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regard to protecting such information.

2. Where a contractor or beneficiary wishes to employ a national of a third country in a position that requires access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, it is the responsibility of the contractor or beneficiary to initiate the security clearance procedure of such a person in accordance with national laws and regulations applicable at the location where access to the EUCI is to be granted.

Facility security clearance ('FSC')

3. A Facility security clearance ('FSC') is granted by the National Security Authority or Designated Security Authority or any other competent security authority of a Member State to indicate that in accordance with national laws and regulations, an entity can protect EUCI at the appropriate classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) within its facilities.

4. A Union institution or body, as contracting or granting authority, must notify, through its Security Authority, the appropriate National Security Authority or Designated Security Authority or any other competent security authority where an FSC is required for performing the contract or grant agreement.

5. An FSC is required where information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided to the facilities of the candidates, the tenderers or applicants in the course of the procurement or grant award procedure.

6. A Union institution or body, as contracting or granting authority, must have received confirmation, through its Security Authority, of an FSC for the candidate, tenderer or

contractor, or for the grant applicant or beneficiary before granting it access to EUCI.

7. Where Member States do not issue FSCs for certain establishments under national laws, the contracting or granting authority must verify with the National Security Authority or Designated Security Authority concerned whether those establishments are capable of handling EUCI at the required level.

8. With the exception of the cases referred to in point 7, the Union institution or body, as contracting authority, must not sign a classified contract or a classified grant agreement before receiving confirmation, through its Security Authority, from the relevant National Security Authority, Designated Security Authority or any other competent national authority that an appropriate FSC has been issued.

9. Withdrawal of an FSC by the relevant National Security Authority, Designated Security Authority or any other competent security authority constitutes sufficient grounds for the contracting or granting authority to terminate a classified contract or grant agreement, or exclude a candidate, tenderer or applicant from the competition.

Provisions for tendering and implementation ofclassified contracts and grant agreements

10. Where EUCI is provided to a candidate, tenderer or applicant during the procurement or selection procedure, the call for tender or call for proposal must include an obligation for the candidate, tenderer or applicant which is not selected, to return all classified documents within a specified period of time.

11. As a general rule, the contractor or grant beneficiary is required to return any EUCI held by it to the contracting or granting authority upon termination of the classified contract or the grant agreement or upon the end of the participation of a grant beneficiary.

12. Specific provisions for the disposal of EUCI during the performance of the classified contract or grant agreement or upon its termination must be laid down in the Security Aspects Letter .

13. Where the contractor or grant beneficiary is authorised to retain EUCI after termination of a classified contract or grant agreement, they must continue to comply with the minimum standards contained in this Regulation and the confidentiality of EUCI must be protected by the contractor or the grant beneficiary.

14. The conditions relevant for the protection of EUCI under which the contractor or beneficiary may subcontract must be defined in the call for tender or the call for proposals, and in the classified contract or grant agreement.

15. A contractor or beneficiary must obtain permission from the contracting or granting authority before subcontracting any parts of a classified contract or classified parts of a grant agreement.

16. The contractor or beneficiary must be responsible for ensuring that all subcontracting activities are undertaken in accordance with the minimum standards laid down in this Regulation and must not provide EUCI to a subcontractor without the prior written consent of the contracting or granting authority.

17. With regard to EUCI created by the contractor or beneficiary, the Union institution or body, which is the contracting or granting authority, is considered the originator and exercises the rights incumbent on the originator.

18. Where Member States require an FSC or a Personnel Security Clearance for contracts, grant agreements or subcontracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, the Union institutions and bodies, as contracting or granting authorities, must not use those national requirements to place additional obligations on other Member States or exclude tenderers, applicants, contractors, beneficiaries or subcontractors from Member States that have no such FSC or Personnel Security Clearance requirements for access to RESTREINT UE/EU RESTRICTED information from related contracts, grant agreements or subcontracts, or a competition for such.

Visits in connection with classified contracts and grant agreements

19. Where the Union institutions and bodies, contractors, beneficiaries or subcontractors require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET on each other's premises in the context of the implementation of a classified contract or grant agreement, visits must be arranged in liaison with the National Security Authorities, Designated Security Authorities or any other competent security authorities concerned.

20. The visits referred to in point 19 are subject to the following requirements:

(a) the visit must have an official purpose related to a classified contract or grant agreement;

(b) visitors must hold a Personnel Security Clearance at the required level and have a need-to-know in order to access EUCI used or generated in the performance a classified contract or grant agreement;

(c) a formal request to visit must be submitted either to the facility's relevant National Security Authority or Designated Security Authority or to the Security Authority of the Union institution or body concerned at least 15 days before the date of the visit.

21. In the context of specific projects, the relevant National Security Authority or Designated Security Authority and the Security Authority of the Union institution or body concerned, may agree on a procedure whereby visits in relation to a specific classified contract or grant can be arranged directly between the visitor's security officer and the security officer of the facility to be visited. Such an exceptional procedure must be set out in the Programme or Project Security Instruction or other specific arrangements.

22. Visits involving access to information classified RESTREINT UE/EU RESTRICTED must be arranged directly between the sending and receiving entity.

Electronic transmission of EUCI in connection with classified contracts and grant agreements

23. Electronic handling and transmission of EUCI must be carried out in accordance with Chapter 5, Section 5.

The CISs owned by a contractor, beneficiary or subcontractor and used to handle and store EUCI for the performance of the contract or grant agreement must be subject to accreditation by the Security Accreditation Authority ('SAA') of the country or the international organisation under whose authority the contractor, beneficiary or subcontractor functions.

Any electronic transmission of EUCI in the context of classified contracts and grant agreements must be protected by cryptographic products approved in accordance with Article 42.

24. The security accreditation of contractors' or beneficiaries' CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the security officer of a contractor or beneficiary where allowed by national laws and regulations.

Where the security accreditation task is delegated, the contractor or beneficiary must be responsible for implementing the security requirements described in the Security Aspects Letter when handling RESTREINT UE/EU RESTRICTED information in its CIS. The relevant National Security Authorities or National Security Authorities and SAAs retain responsibility for the protection of information classified RESTREINT UE/EU RESTRICTED handled or stored by the contractor or beneficiary and the right to inspect the security measures taken by the contractor or beneficiary.

In addition, the contractor or beneficiary must provide the Union institution and body, as contracting or granting authority, and where required by national laws and regulations, the competent national SAA, with a statement of compliance certifying that the contractor or beneficiary CIS and related interconnections have been accredited for handling and storing EUCI at RESTREINT UE/EU RESTRICTED level.

Hand carriage of EUCI in connection with classified contracts and grant agreements

25. The hand carriage of classified information related to the classified contracts and grant agreements must be subject to strict security requirements.

26. RESTREINT UE/EU RESTRICTED information may be hand carried by contractor or beneficiary personnel within the European Union, provided the following requirements are met:

(a) the envelope or packaging used is opaque and bears no indication of the classification of its contents;

(b) the bearer retains possession of the classified information at all times;

(c) the envelope or packaging is not opened until it reaches its final destination.

27. As regards information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, hand carriage by contractor or beneficiary personnel within a Member State is arranged in advance between the sending and receiving entities.

The dispatching authority or facility informs the receiving authority or facility of the details of the consignment, including reference, classification, expected time of arrival and name of courier. Hand carriage is permitted, provided the following requirements are met:

(a) the classified information is carried in a double envelope or packaging;

(b) the outer envelope or packaging is secured and bears no indication of the classification of its contents, while the inner envelope bears the level of classification;

(c) the bearer retains possession of EUCI at all times;

(d) the envelope or packaging is not opened until it reaches its final destination;

(e) the envelope or packaging is carried in a lockable briefcase or similar approved container of such size and weight that it can be kept at all times by the bearer;

(f) the courier carries a courier certificate issued by their competent Security Authority authorising the courier to carry the classified consignment as identified.

28. As regards hand carriage by contractor or beneficiary personnel of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET from one Member State to another, in addition to the requirements set out in point 27 the following additional rules apply:

(a) the courier is responsible for the safe custody of the classified material carried until it is handed over to the recipient;

(b) in the event of a security breach, the sender's National Security Authority or Designated Security Authority may request the authorities in the country where the breach occurred to carry out an investigation, report their findings and take legal or other action as appropriate;

(c) the courier must have been briefed on all the security obligations to be observed during carriage and must have signed an appropriate acknowledgement;

(d) the instructions for the courier must be attached to the courier certificate;

(e) the courier must be provided with a description of the consignment and an itinerary;

(f) the courier certificate and the associated documents must be returned to the issuing National Security Authority or Designated Security Authority upon completion of the trip or trips or be kept available by the recipient of the courier certificate for monitoring purposes;

(g) where customs, immigration authorities or border police ask to examine and inspect the consignment, they must be permitted to open and observe sufficient parts of the consignment so as to establish that it contains no material other than that which is declared;

(h) customs authorities should be urged to honour the official authority of the shipping documents and of the authorisation documents carried by the courier.

Where a consignment is opened by customs, it should be done out of sight of unauthorised persons and in the presence of the courier where possible. The courier must request that the consignment be repacked and ask the authorities conducting the inspection to reseal the consignment and confirm in writing that it was opened by them.

29. Hand carriage by contractor or beneficiary personnel of information classified up to SECRET UE/EU SECRET level to a third country or an international organisation is subject to the provisions of the security of information agreement concluded between the European Union and that third country or international organisation.

Transport of EUCI by commercial couriers and as freight in connection with classified contracts and grant agreements

30. The transport of EUCI by commercial couriers must be conducted in accordance with the relevant provisions of Annex IV.

31. As regards the transport of classified material as freight, the following principles must be applied when determining security arrangements:

(a) security must be assured at all stages during transportation from the point of origin to the final destination;

(b) the degree of protection afforded to a consignment must be determined by the highest classification level of material contained within it;

(c) an FSC at the appropriate level must be obtained for companies providing transportation. In such cases, personnel handling the consignment must be security cleared;

(d) prior to any cross-border movement of material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, a transportation plan must be drawn up by the consignor and approved by the National Security Authority, Designated Security Authority or any other competent security authority concerned;

(e) trips must be point to point to the extent possible, and must be completed as quickly as the circumstances permit;

(f) wherever possible, routes must be only through Member States. Routes through third countries must only be undertaken if authorised by the National Security Authority, Designated Security Authority or any other competent security authority of the States of both the consignor and the consignee.