

**COMMISSION DECISION (EU, Euratom) 2021/259****of 10 February 2021****laying down implementing rules on industrial security with regard to classified grants**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

Having regard to Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 <sup>(1)</sup>,

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission <sup>(2)</sup>,

Having regard to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information <sup>(3)</sup>,

Having regard to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission <sup>(4)</sup>,

After consulting the Commission Security Expert Group, in accordance with Article 41(5) of Decision (EU, Euratom) 2015/444,

Whereas:

- (1) Articles 41, 42, 47 and 48 of Decision (EU, Euratom) 2015/444 provide that more detailed provisions to supplement and support Chapter 6 of that Decision are to be laid down in implementing rules on industrial security, governing issues such as the award of classified grant agreements, facility security clearances, personnel security clearances, visits and transmission and carriage of European Union classified information ('EUCI').
- (2) Decision (EU, Euratom) 2015/444 states that classified grant agreements are to be implemented in close cooperation with the national security authority, the designated security authority or any other competent authority of the Member States concerned. The Member States have agreed to ensure that any entity under their jurisdiction which may receive or generate classified information originating in the Commission is appropriately security cleared and is capable of providing suitable protection equivalent to that afforded by the security rules of the Council of the European Union for protecting EU classified information bearing a corresponding classification marking, as provided for in the Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union (2011/C 202/05) <sup>(5)</sup>.

<sup>(1)</sup> OJ L 193, 30.7.2018, p. 1.

<sup>(2)</sup> OJ L 72, 17.3.2015, p. 41.

<sup>(3)</sup> OJ L 72, 17.3.2015, p. 53.

<sup>(4)</sup> OJ L 6, 11.1.2017, p. 40.

<sup>(5)</sup> OJ C 202, 8.7.2011, p. 13.

- (3) The Council, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy have agreed to ensure maximum consistency in the application of security rules regarding their protection of EU CI, while taking into account their specific institutional and organisational needs, in accordance with the declarations attached to the minutes of the Council session at which Council Decision 2013/488/EU <sup>(6)</sup> on the security rules for protecting EU classified information was adopted.
- (4) The Commission's implementing rules on industrial security with regard to classified grants should therefore also ensure maximum consistency and take into account the Guidelines on Industrial Security approved by the Council Security Committee on 13 December 2016.
- (5) On 4 May 2016 the Commission adopted a decision <sup>(7)</sup> empowering the Member of the Commission responsible for security matters to adopt, on behalf of the Commission and under its responsibility, the implementing rules provided for in Article 60 of Decision (EU, Euratom) 2015/444,

HAS ADOPTED THIS DECISION:

## CHAPTER 1

### GENERAL PROVISIONS

#### *Article 1*

#### **Subject matter and scope**

1. This Decision sets out implementing rules on industrial security with regard to classified grants within the meaning of Decision (EU, Euratom) 2015/444, and in particular Chapter 6 of that Decision.
2. This Decision lays down specific requirements to ensure the protection of EU classified information (EU CI) in the publication of calls, and when awarding grants and implementing the classified grant agreements concluded by the European Commission.
3. This Decision applies to grants involving information classified at the following levels:
  - (a) RESTREINT UE/EU RESTRICTED;
  - (b) CONFIDENTIEL UE/EU CONFIDENTIAL;
  - (c) SECRET UE/EU SECRET.
4. This Decision applies without prejudice to specific rules laid down in other legal acts, such as those concerning the European Defence Industrial Development Programme.

#### *Article 2*

#### **Responsibilities within the Commission**

1. As part of the responsibilities of the authorising officer of the granting authority referred to in Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council, he or she shall ensure that the classified grant complies with Decision (EU, Euratom) 2015/444 and its implementing rules.

<sup>(6)</sup> Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

<sup>(7)</sup> Commission Decision of 4.5.2016 on an empowerment relating to security (C(2016) 2797 final).

2. To that end, the authorising officer concerned shall, at all stages, seek the advice of the Commission security authority on issues regarding the security elements of a classified grant agreement, programme or project, and shall inform the local security officer about the signed classified grant agreements. The decision on the classification level of specific subjects shall rest with the granting authority and shall be taken with due regard to the security classification guide.
3. Where the programme or project security instructions referred to in Article 5(3) are applied, the granting authority and the Commission security authority shall discharge the responsibilities assigned to them in those instructions.
4. In respecting the requirements of these implementing rules, the Commission security authority shall cooperate closely with the national security authorities ('NSAs') and the designated security authorities ('DSAs') of the Member States concerned, in particular as regards facility security clearances ('FSCs') and personnel security clearances ('PSCs'), visit procedures and transportation plans.
5. Where grants are managed by EU executive agencies or other funding bodies and the specific rules laid down in other legal acts referred to in Article 1(4) do not apply:
  - (a) the delegating Commission department shall exercise the rights pertaining to the originator of EUCI generated in the context of the grants if the delegation arrangements so provide;
  - (b) the delegating Commission department shall be responsible for determining the security classification;
  - (c) requests for security clearance information and the notifications to NSAs and/or DSAs shall be sent through the Commission security authority.

## CHAPTER 2

### HANDLING OF CALLS FOR CLASSIFIED GRANTS

#### *Article 3*

##### **Basic principles**

1. Classified parts of the grants shall be implemented only by beneficiaries registered in a Member State, or by beneficiaries registered in a third country or established by an international organisation where that third country or international organisation has concluded a security of information agreement with the Union or entered into an administrative arrangement with the Commission <sup>(8)</sup>.
2. Before launching a call for a classified grant, the granting authority shall determine the security classification of any information that could be provided to applicants. The granting authority shall also determine the maximum security classification of any information used or generated in the performance of the grant agreement or programme or project, or at least the anticipated volume and type of information to be produced or handled, and the need for a classified communication and information system (CIS).
3. The granting authority shall ensure that calls for classified grants provide information about the special security obligations related to classified information. The call documentation shall include clarifications about the timeline for beneficiaries to obtain the FSCs, where they are required. Annexes I and II contain sample templates for information regarding the call conditions.

<sup>(8)</sup> The list of agreements concluded by the EU and of administrative arrangements entered into by the European Commission, under which EU classified information may be exchanged with third countries and international organisations, can be found on the Commission website.

4. The granting authority shall ensure that information classified RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET is disclosed to applicants only after they have signed a non-disclosure agreement, obliging applicants to handle and protect EUCI in accordance with Decision (EU, Euratom) 2015/444, its implementing rules and the applicable national rules.

5. Where RESTREINT UE/EU RESTRICTED information is provided to applicants, the minimum requirements mentioned in Article 5(7) of this Decision shall be included in the call or in the non-disclosure arrangements concluded at proposal stage.

6. All applicants and beneficiaries which are required to handle or store information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either at the proposal stage or during the performance of the classified grant agreement itself, shall hold an FSC at the required level, except for cases mentioned in paragraph 9. The following identifies the three scenarios that may arise during the proposal stage for a classified grant involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level:

(a) no access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level during the proposal stage:

Where the call concerns a grant that will involve EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level, but does not require the applicant to handle such information at the proposal stage, an applicant which does not hold an FSC at the required level shall not be excluded from the application process on the grounds that it does not hold an FSC;

(b) access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the granting authority during the proposal stage:

Access shall be granted to applicant personnel who hold a PSC at the required level and who have a need-to-know;

(c) handling or storage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level on the premises of the applicant during the proposal stage:

Where the call requires applicants to handle or store EUCI on their premises, the applicant shall hold an FSC at the required level. In such circumstances, the granting authority shall obtain, through the Commission security authority, an assurance from the relevant NSA or DSA that the applicant has been granted an appropriate FSC before any EUCI material is provided to the applicant. Access shall be granted to applicant personnel who hold a PSC at the required level and who have a need-to-know.

7. In principle, an FSC or PSC shall not be required for access to RESTREINT UE/EU RESTRICTED information, either at the proposal stage or for the performance of the grant agreement. Where Member States require an FSC or PSC for grant agreements or subcontracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, as listed in Annex IV, those national requirements shall not place any additional obligations on other Member States or exclude applicants, beneficiaries or subcontractors from Member States that have no such FSC or PSC requirements for access to RESTREINT UE/EU RESTRICTED information from related grant agreements or subcontracts, or a competition for such. Those grant agreements shall be performed in Member States in accordance with their national laws and regulations.

8. Where an FSC is required in the handling of a call and for the implementation of a classified grant agreement, the granting authority shall submit, through the Commission security authority, a request to the beneficiary's NSA or DSA using a facility security clearance information sheet ('FSCIS') or any established equivalent electronic form. Annex III, Appendix D, contains an example of an FSCIS<sup>(9)</sup>. Response to an FSCIS is provided, to the extent possible, within ten working days of the date of the request.

9. Where Member States' government establishments or establishments under the control of their government participate in classified grants that require FSCs, and where FSCs are not issued for those establishments under national laws, the granting authority shall verify with the NSA or DSA concerned, through the Commission security authority, whether those government establishments are capable of handling EUCI at the required level.

<sup>(9)</sup> Other forms used may differ from the example provided in these implementing rules in their design.

10. Where a PSC is required for the performance of a classified grant agreement and where, according to national rules, an FSC is necessary before a PSC is granted, the granting authority shall check with the beneficiary's NSA or DSA, through the Commission security authority, using an FSCIS, that the beneficiary holds an FSC or that the FSC process is underway. In this case, the Commission shall not issue requests for PSCs using personnel security clearance information sheet ('PSCIS').

#### Article 4

### Subcontracting in classified grants

1. The conditions under which beneficiaries may subcontract action tasks involving EUCI shall be defined in the call and in the grant agreement. These conditions shall include the requirement that all FSCISs shall be submitted through the Commission security authority. Subcontracting shall be subject to prior written consent from the granting authority. Where applicable, subcontracting shall comply with the basic act establishing the programme.
2. Classified parts of the grants shall be subcontracted only to entities registered in a Member State, or to entities registered in a third country or established by an international organisation where that third country or international organisation has concluded a security of information agreement with the Union or entered into an administrative arrangement with the Commission <sup>(10)</sup>.

#### CHAPTER 3

### HANDLING OF CLASSIFIED GRANTS

#### Article 5

### Basic principles

1. When awarding a classified grant, the granting authority, together with the Commission security authority, shall ensure that the beneficiaries' obligations regarding the protection of EUCI used or generated in the performance of the grant agreement are an integral part of the grant agreement. Grant-specific security requirements shall take the form of a security aspects letter ('SAL'). A sample template for a SAL is set out in Annex III.
2. Before signing a classified grant, the granting authority shall approve a security classification guide ('SCG') for the tasks to be performed and information generated in the implementation of the grant, or at programme or project level, where applicable. The SCG shall be part of the SAL.
3. Programme- or project-specific security requirements shall take the form of a programme (or project) security instruction ('PSI'). The PSI may be drafted using the provisions of the SAL template as set out in Annex III. The PSI shall be developed by the Commission department managing the programme or project, in close cooperation with the Commission security authority, and submitted for advice to the Commission Security Expert Group. Where a grant agreement is part of a programme or project with its own PSI, the SAL of the grant agreement shall have a simplified form and shall include reference to the security provisions set out in the PSI of the programme or project.
4. Except for cases mentioned in Article 3(9), the classified grant agreement shall not be signed until the applicant's NSA or DSA has confirmed the applicant's FSC, or, where the classified grant agreement is awarded to a consortium, until the NSA or DSA of at least one applicant, within the consortium, or more if necessary, has confirmed that applicant's FSC.
5. In principle, and save provided otherwise in other relevant rules, the granting authority shall be considered the originator of EUCI generated in the performance of the grant agreement.

<sup>(10)</sup> The list of agreements concluded by the EU and of administrative arrangements entered into by the European Commission, under which EU classified information may be exchanged with third countries and international organisations, can be found on the Commission website.

6. The granting authority, through the Commission security authority, shall notify the NSAs and/or DSAs of all beneficiaries and subcontractors about the signature of classified grant agreements or subcontracts and any extensions or early terminations of such grant agreements or subcontracts. A list of country requirements is provided in Annex IV.

7. Grant agreements involving information classified RESTREINT UE/EU RESTRICTED shall include a security clause making the provisions set out in Annex III, Appendix E binding upon beneficiaries. Those grant agreements shall include an SAL setting out, as a minimum, the requirements for handling RESTREINT UE/EU RESTRICTED information including information assurance aspects and specific requirements to be fulfilled by the beneficiaries regarding the accreditation of their CIS handling RESTREINT UE/EU RESTRICTED information.

8. Where this is required by Member States' national laws and regulations, NSAs or DSAs ensure that beneficiaries or subcontractors under their jurisdiction comply with the applicable security provisions for the protection of RESTREINT UE/EU RESTRICTED information and conduct verification visits to beneficiaries' or subcontractors' facilities located in their territory. Where the NSA or DSA is not under such an obligation, the granting authority shall ensure that the beneficiaries implement the required security provisions set out in Annex III, Appendix E.

#### *Article 6*

##### **Access to EUCI by staff of beneficiaries and subcontractors**

1. The granting authority shall ensure that classified grant agreements include provisions stating that staff of beneficiaries or subcontractors who, for the performance of the classified grant agreement or subcontract, require access to EUCI, may be granted that access only if:

- (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 security cleared at the relevant level by the respective NSA or DSA 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 applicable, access to EUCI shall also be in compliance with the basic act establishing the programme and take account of any additional markings defined in the SCG.

3. If a beneficiary or subcontractor wishes to employ a national of a non-EU country in a position that requires access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, it is the responsibility of the beneficiary or subcontractor 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.

#### *Article 7*

##### **Access to EUCI by experts participating in checks, reviews or audits**

1. Where external persons ('experts') are involved in checks, reviews or audits conducted by the granting authority or in performance reviews of the beneficiaries that require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, they shall be provided with a contract only if they have been security cleared at the relevant level by the respective NSA or DSA or any other competent security authority. The granting authority, through the Commission security authority, shall check and, where necessary, ask the NSA or DSA to initiate the vetting process for experts at least six months prior to the start of their respective contracts.

2. Before signing their contracts, the experts shall be briefed on the applicable security rules for protecting EUCI, and shall have acknowledged their responsibilities with regard to protecting such information.

## CHAPTER 4

## VISITS IN CONNECTION WITH CLASSIFIED GRANT AGREEMENTS

*Article 8***Basic principles**

1. Where the granting authority, experts, 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 grant agreement, visits shall be arranged in liaison with the NSAs or DSAs or any other competent security authorities concerned.
2. The visits referred to in paragraph 1 shall be subject to the following requirements:
  - (a) the visit shall have an official purpose related to the classified grant;
  - (b) any visitor shall hold a PSC at the required level and shall have a need-to-know in order to access EUCI used or generated in the performance of the classified grant.

*Article 9***Requests for visits**

1. Visits by beneficiaries or subcontractors to other beneficiaries' or subcontractors' facilities, or to granting authority premises, that involve access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged in accordance with the following procedure:
  - (a) the security officer of the facility sending the visitor shall complete all relevant parts of the request for visit (RFV) form and submit the request to the facility's NSA or DSA. A template for the RFV form is set out in Annex III, Appendix C;
  - (b) the sending facility's NSA or DSA needs to confirm the visitor's PSC before submitting the RFV to the host facility's NSA or DSA (or the Commission security authority if the visit is to the premises of a granting authority);
  - (c) the security officer of the sending facility shall then obtain from its NSA or DSA the reply of the host facility's NSA or DSA (or the Commission security authority) either authorising or denying the RFV;
  - (d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.
2. Visits by granting authority officials or experts or auditors to beneficiaries' or subcontractors' facilities that involve access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged in accordance with the following procedure:
  - (a) the visitor shall complete all relevant parts of the RFV form and submit it to the Commission security authority;
  - (b) the Commission security authority shall confirm the PSC of the visitor before submitting the RFV to the host facility's NSA or DSA;
  - (c) the Commission security authority shall obtain a reply from the host facility's NSA or DSA either authorising or denying the RFV;
  - (d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.
3. An RFV may cover either a single visit or recurring visits. In the case of recurring visits, the RFV may be valid for up to one year from the start date requested.
4. The validity of any RFV shall not exceed the validity of the visitor's PSC.
5. As a general rule, an RFV should be submitted to the host facility's competent security authority at least 15 working days before the date of the visit.

*Article 10***Visit procedures**

1. Before allowing visitors to have access to EUCI, the security office of the host facility shall comply with all the visit-related security procedures and rules laid down by its NSA or DSA.
2. Visitors shall prove their identity upon arrival at the host facility by presenting a valid ID card or passport. That identification information shall correspond to the information supplied in the RFV.
3. The host facility shall ensure that records are kept of all visitors, including their names, the organisation they represent, the date of expiry of the PSC, the date of the visit and the names of the persons visited. Such records shall be retained for a period of at least five years, or longer if required by the national rules and regulations of the country where the host facility is located.

*Article 11***Visits arranged directly**

1. In the context of specific projects, the relevant NSAs or DSAs and the Commission security authority may agree on a procedure whereby visits for a specific classified grant can be arranged directly between the visitor's security officer and the security officer of the facility to be visited. A template of the form to be used for this purpose is set out in Annex III, Appendix C. Such an exceptional procedure shall be set out in the PSI or other specific arrangements. In such cases, the procedures set out in Article 9 and Article 10(1) shall not apply.
2. Visits involving access to information classified RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending and receiving entity, without the need to follow the procedures set out in Article 9 and Article 10(1).

## CHAPTER 5

**TRANSMISSION AND CARRIAGE OF EUCI IN PERFORMANCE OF CLASSIFIED GRANT AGREEMENTS***Article 12***Basic principles**

The granting authority shall ensure that all decisions related to EUCI transfer and carriage are in accordance with Decision (EU, Euratom) 2015/444 and its implementing rules, and with the terms of the classified grant agreement, including the consent of the originator.

*Article 13***Electronic handling**

1. Electronic handling and transmission of EUCI shall be carried out in accordance with Chapters 5 and 6 of Decision (EU, Euratom) 2015/444 and its implementing rules.

The communication and information systems owned by a beneficiary and used to handle EUCI for the performance of the grant agreement ('beneficiary CIS') shall be subject to accreditation by the security accreditation authority responsible ('SAA'). Any electronic transmission of EUCI shall be protected by cryptographic products approved in accordance with Article 36(4) of Decision (EU, Euratom) 2015/444. TEMPEST security measures shall be implemented in accordance with Article 36(6) of that Decision.

2. The security accreditation of the beneficiary CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and of any interconnection thereof may be delegated to the security officer of a beneficiary if this is permitted by national laws and regulations. Where that task is delegated, the beneficiary shall be responsible for implementing the minimum security requirements described in the SAL when handling RESTREINT UE/EU RESTRICTED information on its CIS. However, the relevant NSAs or DSAs, and SAAs retain responsibility for the protection of RESTREINT UE/EU RESTRICTED information handled by the beneficiary and the right to inspect the security measures taken by the beneficiary. In addition, the beneficiary shall provide the granting authority and, where required by national laws and regulations, the competent national SAA, with a statement of compliance certifying that the beneficiary CIS and related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level <sup>(11)</sup>.

#### Article 14

### Transport by commercial couriers

The transport of EUCI by commercial couriers shall abide by the relevant provisions of Commission Decision (EU, Euratom) 2019/1962 <sup>(12)</sup> on implementing rules for handling RESTREINT UE/EU RESTRICTED information and Commission Decision (EU, Euratom) 2019/1961 <sup>(13)</sup> on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information.

#### Article 15

### Hand carriage

1. The carriage of classified information by hand shall be subject to strict security requirements.
2. RESTREINT UE/EU RESTRICTED information may be hand carried by beneficiary personnel within the 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 classified information does not leave the possession of the bearer;
  - (c) the envelope or packaging is not opened *en route*.
3. For information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET, hand carriage by 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. Such 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) EUCI does not leave the possession of the bearer;
  - (d) the envelope or packaging is not opened *en route*;
  - (e) the envelope or packaging is carried in a lockable briefcase or similar approved container of such size and weight that it can be retained at all times in the personal possession of the bearer and not be consigned to a baggage hold;
  - (f) the courier carries a courier certificate issued by his or her competent security authority authorising the courier to carry the classified consignment as identified.

<sup>(11)</sup> The minimum requirements for communication and information systems handling EUCI at RESTREINT UE/EU RESTRICTED level are laid down in Annex III, Appendix E.

<sup>(12)</sup> Commission Decision (EU, Euratom) 2019/1962 of 17 October 2019 on implementing rules for handling RESTREINT UE/EU RESTRICTED information (OJ L 311, 2.12.2019, p. 21).

<sup>(13)</sup> Commission Decision (EU, Euratom) 2019/1961 of 17 October 2019 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information (OJ L 311, 2.12.2019, p. 1).

4. For hand carriage by beneficiary personnel of information classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET from one Member State to another, the following additional rules shall apply:

- (a) the courier shall be 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 NSA or DSA may request that the authorities in the country where the breach occurred carry out an investigation, report their findings and take legal or other action as appropriate;
- (c) the courier shall have been briefed on all the security obligations to be observed during carriage and shall have signed an appropriate acknowledgement;
- (d) the instructions for the courier shall be attached to the courier certificate;
- (e) the courier shall have been provided with a description of the consignment and an itinerary;
- (f) the documents shall be returned to the issuing NSA or DSA upon completion of the journey(s) or be kept available by the recipient for monitoring purposes;
- (g) if customs, immigration authorities or border police ask to examine and inspect the consignment, they shall 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.

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

5. Hand carriage by beneficiary personnel of information classified RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET to a third country or an international organisation shall be subject to the provisions of the security of information agreement or the administrative arrangement concluded between, respectively, the Union or the Commission and that third country or international organisation.

## CHAPTER 6

### BUSINESS CONTINUITY PLANNING

#### *Article 16*

#### **Contingency plans and recovery measures**

The granting authority shall ensure that the classified grant agreement requires the beneficiaries to set out business contingency plans ('BCP') for protecting EUCI handled in the context of the classified grant in emergency situations, and to put in place preventive and recovery measures in the context of business continuity planning to minimise the impact of incidents in relation to the handling and storage of EUCI. The beneficiaries shall confirm to the granting authority that their BCPs are in place.

#### *Article 17*

#### **Entry into force**

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 10 February 2021.

*For the Commission,  
On behalf of the President,  
Johannes HAHN  
Member of the Commission*

---

## ANNEX I

## STANDARD INFORMATION IN THE CALL

(to be adapted to the call used)

## Security

Projects involving EU classified information must undergo security scrutiny to authorise funding and may be made subject to specific security rules (detailed in a security aspects letter (SAL) which is annexed to the Grant Agreement).

These rules (governed by Commission Decision (EU, Euratom) 2015/444 <sup>(1)</sup> and/or national rules) provide for instance that:

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can **NOT** be funded;
- classified information must be marked in accordance with the applicable security instructions in the SAL;
- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/EU RESTRICTED if required by national rules) may be:
  - created or accessed only on premises with facility security clearing from the competent national security authority (NSA), in accordance with the national rules;
  - handled only in a secured area accredited by the competent NSA;
  - accessed and handled only by persons with a valid personnel security clearance (PSC) and a need-to-know;
- at the end of the grant, the classified information must either be returned or continued to be protected in accordance with the applicable rules;
- action tasks involving EU classified information (EUCI) may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission);
- disclosure of EUCI to third parties is subject to prior written approval from the granting authority.

Please note that, depending on the type of activity, facility security clearing may have to be provided before grant signature. The granting authority will assess the need for clearings in each case and will establish their delivery date during grant preparation. Please note that in **no circumstances** can we sign any grant agreement until at least one of the beneficiaries in a consortium has facility security clearing.

Further security recommendations may be added to the Grant Agreement in the form of security deliverables (e.g. *create security advisory group, limit level of detail, use fake scenario, exclude use of classified information, etc.*).

Beneficiaries must ensure that their projects are not subject to national/third-country security requirements that could affect implementation or put into question the award of the grant (e.g. *technology restrictions, national security classification, etc.*). The granting authority must be notified immediately of any potential security issues.

[*additional OPTION for FPAs: For framework partnerships, both the framework partnership applications and the grant applications may have to undergo security scrutiny.*]

---

<sup>(1)</sup> See Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

## ANNEX II

**STANDARD GRANT AGREEMENT CLAUSES**

*(to be adapted to the grant agreement used)*

**13.2 Security – Classified information**

The parties must handle classified information (EU or national) in accordance with the applicable EU or national law on classified information (in particular, Commission Decision (EU, Euratom) 2015/444 <sup>(1)</sup> and its implementing rules).

Specific security rules (if any) are set out in Annex 5.

## ANNEX 5

## Security – EU classified information

*[OPTION for actions with EU classified information (standard): If EU classified information is used or generated by the action, it must be treated in accordance with the security classification guide (SCG) and security aspect letter (SAL) set out in Annex 1 and Decision (EU, Euratom) 2015/444 and its implementing rules – until it is declassified.]*

Deliverables which contain EU classified information must be submitted according to special procedures agreed with the granting authority.

Action tasks involving EU classified information may be subcontracted only with prior explicit written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission).

EU classified information may not be disclosed to any third party (including participants involved in the action implementation) without prior explicit written approval from the granting authority.]

---

---

<sup>(1)</sup> Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

*ANNEX III***[Annex IV (to the .....)]****SECURITY ASPECTS LETTER (SAL) <sup>(1)</sup>****[Model]**

---

<sup>(1)</sup> This model of SAL applies where the Commission is considered the originator of classified information created and handled for the performance of the grant agreement. Where the originator of classified information created and handled for the performance of the grant agreement is not the Commission, and where a specific security framework is set up by the Member States participating in the grant, other models of SAL may apply.

## Appendix A

**SECURITY REQUIREMENTS**

The granting authority must include the following security requirements in the security aspects letter (SAL). Some clauses may not be applicable to the grant agreement. These are shown in square brackets.

The list of clauses is not exhaustive. Further clauses may be added depending on the nature of the classified grant.

**GENERAL CONDITIONS** [N.B.: applicable to all classified grant agreements]

1. This security aspects letter (SAL) is an integral part of the classified grant agreement [or subcontract] and describes grant agreement-specific security requirements. Failure to meet these requirements may constitute sufficient grounds to terminate the grant agreement.
2. Grant beneficiaries are subject to all obligations set out in Commission Decision (EU, Euratom) 2015/444 <sup>(2)</sup> (hereinafter 'CD 2015/444') and its implementing rules <sup>(3)</sup>. If the grant beneficiary faces a problem of application of the applicable legal framework in a Member State, it must refer to the Commission security authority and the national security authority (NSA) or designated security authority (DSA).
3. Classified information generated when performing the grant agreement must be marked as EU classified information (EUCI) at security classification level, as determined in the security classification guide (SCG) in Appendix B to this letter. Deviation from the security classification level stipulated by the SCG is permissible only with the written authorisation of the granting authority.
4. The rights pertaining to the originator of any EUCI created and handled for the performance of the classified grant agreement are exercised by the Commission, as the granting authority.
5. Without the written consent of the granting authority, the beneficiary or subcontractor must not make use of any information or material furnished by the granting authority or produced on behalf of that authority for any purpose other than that of the grant agreement.
6. Where a facility security clearance (FSC) is required for the performance of a grant agreement, the beneficiary must ask the granting authority to proceed with the FSC request.
7. The beneficiary must investigate all security breaches related to EUCI and report them to the granting authority as soon as is practicable. The beneficiary or subcontractor must immediately report to its NSA or DSA, and, where national laws and regulations so permit, to the Commission security authority, all cases in which it is known or there is reason to suspect that EUCI provided or generated pursuant to the grant agreement has been lost or disclosed to unauthorised persons.

<sup>(2)</sup> Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

<sup>(3)</sup> The granting authority should insert the references once these implementing rules have been adopted.

8. After the end of the grant agreement, the beneficiary or subcontractor must return any EUCI it holds to the granting authority as soon as possible. Where practicable, the beneficiary or subcontractor may destroy EUCI instead of returning it. This must be done in accordance with the national laws and regulations of the country where the beneficiary is based, with the prior agreement of the Commission security authority, and under the latter's instruction. EUCI must be destroyed in such a way that it cannot be reconstructed, either wholly or in part.
9. Where the beneficiary or subcontractor is authorised to retain EUCI after termination or conclusion of the grant agreement, the EUCI must continue to be protected in accordance with CD 2015/444 and with its implementing rules <sup>(4)</sup>.
10. Any electronic handling, processing and transmission of EUCI must abide by the provisions laid down in Chapters 5 and 6 of CD 2015/444. These include, *inter alia*, the requirement that communication and information systems owned by the beneficiary and used to handle EUCI for the purpose of the grant agreement (hereinafter 'beneficiary CIS') must be subject to accreditation <sup>(5)</sup>; that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 36(4) of CD 2015/444, and that TEMPEST security measures must be implemented in accordance with Article 36(6) of CD 2015/444.
11. The beneficiary or subcontractor shall have business contingency plans (BCPs) to protect any EUCI handled in the performance of the classified grant agreement in emergency situations and shall put in place preventive and recovery measures to minimise the impact of incidents associated with the handling and storage of EUCI. The beneficiary or subcontractor must inform the granting authority of its BCP.

**GRANT AGREEMENTS REQUIRING ACCESS TO INFORMATION CLASSIFIED RESTREINT UE/EU  
RESTRICTED**

12. In principle, personnel security clearance (PSC) is not required for compliance with the grant agreement <sup>(6)</sup>. However, information or material classified RESTREINT UE/EU RESTRICTED must be accessible only to beneficiary personnel who require such information to perform the grant agreement (*need-to-know principle*), who have been briefed by the beneficiary's security officer on their responsibilities and on the consequences of any compromise or breach of security of such information, and who have acknowledged in writing the consequences of a failure to protect EUCI.
13. Except where the granting authority has given its written consent, the beneficiary or subcontractor must not provide access to information or material classified RESTREINT UE/EU RESTRICTED to any entity or person other than those of its personnel who have a need-to-know.
14. The beneficiary or subcontractor must maintain the security classification markings of classified information generated by or provided during the performance of a grant agreement and must not declassify information without written consent from the granting authority.
15. Information or material classified RESTREINT UE/EU RESTRICTED must be stored in locked office furniture when not in use. When in transit, documents must be carried inside an opaque envelope. The documents must not leave the possession of the bearer and they must not be opened *en route*.

---

<sup>(4)</sup> The granting authority should insert the references once these implementing rules have been adopted.

<sup>(5)</sup> The party undertaking the accreditation will have to provide the granting authority with a statement of compliance, through the Commission security authority, and in co-ordination with the relevant national security accreditation authority (SAA).

<sup>(6)</sup> Where beneficiaries are from Member States requiring PSCs and/or FSCs for grants classified RESTREINT UE/EU RESTRICTED, the granting authority lists in the SAL these PSC and FSC requirements for the beneficiaries in question.

16. The beneficiary or subcontractor may transmit documents classified RESTREINT UE/EU RESTRICTED to the granting authority using commercial courier companies, postal services, hand carriage or electronic means. To this end, the beneficiary or subcontractor must follow the programme (or project) security instruction (PSI) issued by the Commission and/or the Commission implementing rules on industrial security with regard to classified grants <sup>(7)</sup>.
17. When no longer required, documents classified RESTREINT UE/EU RESTRICTED must be destroyed in such a way that they cannot be reconstructed, either wholly or in part.
18. The security accreditation of beneficiary CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the beneficiary's security officer if national laws and regulations so permit. Where accreditation is thus delegated, the NSAs, DSAs or security accreditation authorities (SAAs) retain responsibility for protecting any RESTREINT UE/EU RESTRICTED information that is handled by the beneficiary and the right to inspect the security measures taken by the beneficiary. In addition, the beneficiary shall provide the granting authority and, where required by national laws and regulations, the competent national SAA with a statement of compliance certifying that the beneficiary CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.

#### HANDLING OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

19. Minimum requirements for CIS handling information classified RESTREINT UE/EU RESTRICTED are laid down in Appendix E to this SAL.

#### CONDITIONS UNDER WHICH THE BENEFICIARY MAY SUBCONTRACT

20. The beneficiary must obtain permission from the granting authority before subcontracting any part of a classified grant agreement.
21. No subcontract may be awarded to an entity registered in a non-EU country or to an entity belonging to an international organisation, if that non-EU country or international organisation has not concluded a security of information agreement with the EU or an administrative arrangement with the Commission.
22. Where the beneficiary has let a subcontract, the security provisions of the grant agreement shall apply *mutatis mutandis* to the subcontractor(s) and its (their) personnel. In such a case, it is the beneficiary's responsibility to ensure that all subcontractors apply these principles to their own subcontracting arrangements. To ensure appropriate security oversight, the beneficiary's and subcontractor's NSAs and/or DSAs shall be notified by the Commission security authority of the letting of all related classified subcontracts at the levels of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET. Where appropriate, the beneficiary's and subcontractor's NSAs and/or DSAs shall be provided with a copy of the subcontract-specific security provisions. NSAs and DSAs requiring notification about the security provisions of classified grant agreements at RESTREINT UE/EU RESTRICTED level are listed in the annex to the Commission's implementing rules on industrial security with regard to classified grant agreements <sup>(8)</sup>.
23. The beneficiary may not release any EUCI to a subcontractor without the prior written approval of the granting authority. If EUCI to subcontractors is to be sent frequently or as a matter of routine, then the granting authority may give its approval for a specified length of time (e.g. 12 months) or for the duration of the subcontract.

<sup>(7)</sup> The granting authority should insert the references once these implementing rules have been adopted.

<sup>(8)</sup> The granting authority should insert the references once these implementing rules have been adopted.

### VISITS

*If the standard request for visit (RFV) procedure is to be applied to visits involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, the granting authority must include paragraphs 24, 25 and 26 and delete paragraph 27. If visits involving information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET are arranged directly between the sending and receiving establishments, the granting authority must delete paragraphs 25 and 26 and include paragraph 27 only.*

24. Visits involving access or potential access to information classified RESTREINT UE/EU RESTRICTED shall be arranged directly between the sending and receiving establishments without the need to follow the procedure described in paragraphs 25 to 27 below.
- [25. Visits involving access or potential access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be subject to the following procedure:
  - (a) the security officer of the facility sending the visitor shall complete all relevant parts of the RFV form (Appendix C) and submit the request to the facility's NSA or DSA;
  - (b) the sending facility's NSA or DSA needs to confirm the visitor's PSC before submitting the RFV to the host facility's NSA or DSA (or to the Commission security authority if the visit is to the premises of the granting authority);
  - (c) the security officer of the sending facility shall then obtain from its NSA or DSA the reply of the host facility's NSA or DSA (or the Commission security authority) either authorising or denying the RFV;
  - (d) an RFV is considered approved if no objections are raised until five working days before the date of the visit.]
- [26. Before giving the visitor(s) access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, the host facility must have received authorisation from its NSA or DSA.]
- [27. Visits involving access or potential access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET shall be arranged directly between the sending and receiving establishments (an example of the form that may be used for this purpose is provided in Appendix C).]
28. Visitors must prove their identity on arrival at the host facility by presenting a valid ID card or passport.
29. The facility hosting the visit must ensure that records are kept of all visitors. These must include their names, the organisation they represent, the date of expiry of the PSC (if applicable), the date of the visit and the name(s) of the person(s) visited. Without prejudice to European data protection rules, such records are to be retained for a period of no less than five years or in accordance with national rules and regulations, as appropriate.

### ASSESSMENT VISITS

30. The Commission security authority may, in cooperation with the relevant NSAs or DSAs, conduct visits to beneficiaries' or subcontractors' facilities to check that the security requirements for handling EUCI are being complied with.

### SECURITY CLASSIFICATION GUIDE

31. A list of all the elements in the grant agreement which are classified or to be classified in the course of the performance of the grant agreement, the rules for so doing and the specification of the applicable security classification levels are contained in the security classification guide (SCG). The SCG is an integral part of this grant agreement and can be found in Appendix B to this Annex.

*Appendix B***SECURITY CLASSIFICATION GUIDE**

[specific text to be adjusted depending on the subject of the grant agreement]

## Appendix C

## REQUEST FOR VISIT (MODEL)

## DETAILED INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT

(The application must be submitted in English only)

HEADING	Check boxes for visit type, information type, and indicate how many sites are to be visited and the number of visitors.
4. ADMINISTRATIVE DATA	To be completed by requesting NSA/DSA.
5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY	Give full name and postal address. Include city, state and post code as applicable.
6. ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED	Give full name and postal address. Include city, state, post code, telex or fax number (if applicable), telephone number and e-mail. Give the name and telephone/fax numbers and e-mail of your main point of contact or the person with whom you have made the appointment for the visit. Remarks: (1) Giving the correct post code (zip code) is important because a company may have various different facilities. (2) When applying manually, Annex 1 can be used when two or more facilities have to be visited in connection with the same subject. When an Annex is used, item 3 should state: 'SEE ANNEX 1, NUMBER OF FAC...' (state number of facilities).
7. DATES OF VISIT	Give the actual date or period (date-to-date) of the visit in the format 'day – month – year'. Where applicable, give an alternate date or period in brackets.
8. TYPE OF INITIATIVE	Specify whether the visit has been initiated by the requesting organisation or facility or by invitation of the facility to be visited.
9. THE VISIT RELATES TO:	Specify the full name of the project, contract or call for tender using commonly used abbreviations only.
10. SUBJECT TO BE DISCUSSED/ JUSTIFICATION	Give a brief description of the reason(s) for the visit. Do not use unexplained abbreviations. Remarks: In the case of recurring visits this item should state 'Recurring visits' as the first words in the data element (e. g. Recurring visits to discuss_____).
11. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED	State SECRET UE/EU SECRET (S-UE/EU-S) or CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C), as appropriate.

12. PARTICULARS OF VISITOR	Remark: when more than two visitors are involved in the visit, Annex 2 should be used.
13. THE SECURITY OFFICER OF THE REQUESTING ENTITY	This item requires the name, telephone number, fax number and e-mail of the requesting facility's Security Officer.
14. CERTIFICATION OF SECURITY CLEARANCE	This field is to be completed by the certifying authority. Notes for the certifying authority: a. Give name, address, telephone number, fax number and e-mail (can be pre-printed). b. This item should be signed and stamped (if applicable).
15. REQUESTING SECURITY AUTHORITY	This field is to be completed by the NSA/DSA. Note for the NSA/DSA: a. Give name, address, telephone number, fax number and e-mail (can be pre-printed). b. This item should be signed and stamped (if applicable).

All fields must be completed and the form submitted via Government-to-Government channels (\*)

<p style="text-align: center;"><b>REQUEST FOR VISIT</b> <b>(MODEL)</b></p> <p style="text-align: center;">TO: _____</p>		
1. TYPE OF VISIT REQUEST	2. TYPE OF INFORMATION	3. SUMMARY
<input type="checkbox"/> Single <input type="checkbox"/> Recurring <input type="checkbox"/> Emergency <input type="checkbox"/> Amendment <input type="checkbox"/> Dates <input type="checkbox"/> Visitors <input type="checkbox"/> Facility  For an amendment, insert the NSA/DSA original RFV Reference No _____	<input type="checkbox"/> C-UE/EU-C <input type="checkbox"/> S-UE/EU-S	No of sites: _____  No of visitors: _____
<b>4. ADMINISTRATIVE DATA:</b>		
Requester:  To:	NSA/DSA RFV Reference No _____  Date (dd/mm/yyyy): ____/____/____	

(\*) If it has been agreed that visits involving access or potential access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level can be arranged directly, the completed form can be submitted directly to the Security Officer of the establishment to be visited.



<b>15. REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:</b>	
NAME:	<div style="border: 2px solid black; padding: 10px; width: fit-content; margin: 0 auto;">STAMP</div>
ADDRESS:	
TELEPHONE NO:	
E-MAIL ADDRESS:	
SIGNATURE:	
	DATE (dd/mm/yyyy): ____/____/____
<b>16. REMARKS (Mandatory justification required in the case of an emergency visit):</b>	

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation <sup>(10)</sup> is implemented.>

<sup>(10)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

## ANNEX 1 to RFV FORM

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: <b>(Continue as required)</b>

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation <sup>(1)</sup> is implemented.>

<sup>(1)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

## ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)
<p>1.</p> <p>SURNAME:</p> <p>FIRST NAMES (<i>as per passport</i>):</p> <p>DATE OF BIRTH (<i>dd/mm/yyyy</i>): ____/____/____</p> <p>PLACE OF BIRTH:</p> <p>NATIONALITY:</p> <p>SECURITY CLEARANCE LEVEL:</p> <p>PP/ID NUMBER:</p> <p>POSITION:</p> <p>COMPANY/ORGANISATION:</p>
<p>2.</p> <p>SURNAME:</p> <p>FIRST NAMES (<i>as per passport</i>):</p> <p>DATE OF BIRTH (<i>dd/mm/yyyy</i>): ____/____/____</p> <p>PLACE OF BIRTH:</p> <p>NATIONALITY:</p> <p>SECURITY CLEARANCE LEVEL:</p> <p>PP/ID NUMBER:</p> <p>POSITION:</p> <p>COMPANY/ORGANISATION:</p> <p><b>(Continue as required)</b></p>

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation <sup>(12)</sup> is implemented.>

<sup>(12)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

## Appendix D

**FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS) (MODEL)****1. INTRODUCTION**

- 1.1. Attached is a sample Facility Security Clearance Information Sheet (FSCIS) for the rapid exchange of information between the National Security Authority (NSA) or Designated Security Authority (DSA), other competent national security authorities and the Commission Security Authority (acting on behalf of granting authorities) with regard to the Facility Security Clearance (FSC) of a facility involved in application for, and implementation of, classified grants or subcontracts.
- 1.2. The FSCIS is valid only if stamped by the relevant NSA, DSA or other competent authority.
- 1.3. The FSCIS is divided into a request and reply section and can be used for the purposes identified above or for any other purposes for which the FSC status of a particular facility is required. The reason for the enquiry must be identified by the requesting NSA or DSA in field 7 of the request section.
- 1.4. The details contained in the FSCIS are not normally classified; accordingly, when an FSCIS is to be sent between the respective NSAs/DSAs/Commission this should preferably be done by electronic means.
- 1.5. NSAs/DSAs should make every effort to respond to an FSCIS request within ten working days.
- 1.6. Should any classified information be transferred or a grant or subcontract awarded in relation to this assurance, the issuing NSA or DSA must be informed.

**Procedures and instructions for the use of the Facility Security Clearance Information Sheet (FSCIS)**

These detailed instructions are for the NSA or DSA, or the granting authority and the Commission Security Authority that complete the FSCIS. The request should preferably be typed in capital letters.

<b>HEADER</b>	The requester inserts full NSA/DSA and country name.
<b>1. REQUEST TYPE</b>	The requesting granting authority selects the appropriate checkbox for the type of FSCIS request. Include the level of security clearance requested. The following abbreviations should be used:  SECRET UE/EU SECRET = S-UE/EU-S  CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C  CIS = Communication and information systems for processing classified information.
<b>2. SUBJECT DETAILS</b>	Fields 1 to 6 are self-evident. In field 4 the standard two-letter country code should be used. Field 5 is optional.
<b>3. REASON FOR REQUEST</b>	Give the specific reason for the request, provide project indicators, number of the call or grant. Please specify the need for storage capability, CIS classification level, etc.  Any deadline/expiry/award dates which may have a bearing on the completion of an FSC should be included.

<b>4. REQUESTING NSA/DSA</b>	State the name of the actual requester (on behalf of the NSA/DSA) and the date of the request in number format (dd/mm/yyyy).
<b>5. REPLY SECTION</b>	Fields 1-5: select appropriate fields.  Field 2: if an FSC is in progress, it is recommended to give the requester an indication of the required processing time (if known).  Field 6:  (a) Although validation differs by country or even by facility, it is recommended that the expiry date of the FSC be given. (b) In cases where the expiry date of the FSC assurance is indefinite, this field may be crossed out. (c) In compliance with respective national rules and regulations, the requester or either the beneficiary or subcontractor is responsible for applying for a renewal of the FSC.
<b>6. REMARKS</b>	May be used for additional information with regard to the FSC, the facility or the foregoing items.
<b>7. ISSUING NSA/DSA</b>	State the name of the providing authority (on behalf of the NSA/DSA) and the date of the reply in number format (dd/mm/yyyy).

## FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS) (MODEL)

All fields must be completed and the form communicated via Government-to-Government or Government-to-international organisation channels.

**REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE**

TO: \_\_\_\_\_

**(NSA/DSA Country name)**

Please complete the reply boxes, where applicable:

[ ] Provide an FSC assurance at the level of: [ ] S-UE/EU-S [ ] C-UE/EU-C

for the facility listed below

[ ] Including safeguarding of classified material/information

[ ] Including Communication and Information Systems (CIS) for processing classified information

[ ] Initiate, directly or upon a corresponding request of a beneficiary or subcontractor, the process of obtaining an FSC up to and including the level of ..... with ..... level of safeguarding and ..... level of CIS, if the facility does not currently hold these levels of capabilities.

Confirm accuracy of the details of the facility listed below and provide corrections/additions as required.

1. Full facility name:

Corrections/Additions:

.....

2. Full facility address:

.....

3. Postal address (if different from 2)

.....

4. Zip/post code/city/country

.....

5. Name of the Security Officer

.....

.....

6. Telephone/Fax/E-mail of the Security Officer

.....

7. This request is made for the following reason(s): (provide details of the pre-contractual (proposal selection) stage, grant or subcontract, programme/project, etc.)

.....

Requesting NSA/DSA/granting authority:

Date: (dd/mm/yyyy).....

Name: .....

**REPLY (within ten working days)**

This is to certify that:

- 1.  the abovementioned facility holds an FSC up to and including the level of  S-UE/EU-S  
 C-UE/EU-C.
- 2. The abovementioned facility has the capability to safeguard classified information/material:  
 yes, level: .....  no.
- 3. the abovementioned facility has accredited/authorised CIS:  
 yes, level: .....  no.
- 4.  in relation to the abovementioned request, the FSC process has been initiated. You will be informed when the FSC has been established or refused.
- 5.  the abovementioned facility does not hold an FSC.
- 6. This FSC assurance expires on: ..... (dd/mm/yyyy), or as advised otherwise by the NSA/DSA. In the case of earlier invalidation or any changes to the information listed above, you will be informed.
- 7. Remarks:  
.....

Issuing NSA/DSA Name:..... Date:(dd/mm/yyyy).....

<Placeholder for reference to applicable personal data legislation and link to mandatory information for the data subject, e.g. how Article 13 of the General Data Protection Regulation <sup>(13)</sup> is implemented.>

<sup>(13)</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

*Appendix E***Minimum requirements for protection of EUCI in electronic form at RESTREINT UE/EU RESTRICTED level handled in the beneficiary's CIS****General**

1. The beneficiary must be responsible for ensuring that the protection of RESTREINT UE/EU RESTRICTED information complies with the minimum security requirements as laid down in this security clause and with any other additional requirements advised by the granting authority or, if applicable, by the national security authority (NSA) or designated security authority (DSA).
2. It is the beneficiary's responsibility to implement the security requirements identified in this document.
3. For the purpose of this document, a communication and information system (CIS) covers all equipment used to handle, store and transmit EUCI, including workstations, printers, copiers, fax machines, servers, network management systems, network controllers and communications controllers, laptops, notebooks, tablet PCs, smart phones and removable storage devices such as USB-sticks, CDs, SD-cards, etc.
4. Special equipment, such as cryptographic products, must be protected in accordance with its dedicated security operating procedures (SecOPs).
5. Beneficiary must establish a structure responsible for the security management of the CIS handling information classified RESTREINT UE/EU RESTRICTED and appoint a security officer responsible for the facility concerned.
6. The use of IT solutions (hardware, software or services) privately owned by beneficiary staff for storing or processing RESTREINT UE/EU RESTRICTED information is not permitted.
7. Accreditation of the beneficiary's CIS handling information classified RESTREINT UE/EU RESTRICTED must be approved by the security accreditation authority (SAA) of the Member State concerned or delegated to the beneficiary's security officer as permitted by national laws and regulations.
8. Only information classified RESTREINT UE/EU RESTRICTED that is encrypted using approved cryptographic products may be handled, stored or transmitted (by wired or wireless means) as any other unclassified information under the grant agreement. Such cryptographic products must be approved by the EU or a Member State.
9. External facilities involved in maintenance/repair work must be contractually obliged to comply with the applicable provisions for handling of information classified RESTREINT UE/EU RESTRICTED, as set out in this document.
10. At the request of the granting authority or relevant NSA, DSA, or SAA, the beneficiary must provide evidence of compliance with the security clause of the grant agreement. If an audit and inspection of the beneficiary's processes and facilities are also requested, to ensure compliance with these requirements, beneficiaries shall permit representatives of the granting authority, the NSA, DSA and/or SAA, or the relevant EU security authority to conduct such an audit and inspection.

**Physical security**

11. Areas in which CIS are used to display, store, process or transmit RESTREINT UE/EU RESTRICTED information or areas housing servers, network management systems, network controllers and communications controllers for such CIS should be established as separate and controlled areas with an appropriate access control system. Access to these separate and controlled areas should be restricted to individuals with specific authorisation. Without prejudice to paragraph 8, equipment as described in paragraph 3 must be stored in such separate and controlled areas.

12. Security mechanisms and/or procedures must be implemented to regulate the introduction or connection of removable computer storage media (such as USBs, mass storage devices or CD-RWs) to components on the CIS.

#### ***Access to CIS***

13. Access to a beneficiary's CIS handling EUCI is allowed on a basis of strict need-to-know and authorisation of personnel.
14. All CIS must have up-to-date lists of authorised users. All users must be authenticated at the start of each processing session.
15. Passwords, which are part of most identification and authentication security measures, must be at least nine characters long and must include numeric and 'special' characters (if permitted by the system) as well as alphabetic characters. Passwords must be changed at least every 180 days. They must be changed as soon as possible if they have been compromised or disclosed to an unauthorised person, or if such compromise or disclosure is suspected.
16. All CIS must have internal access controls to prevent unauthorised users from accessing or modifying information classified RESTREINT UE/EU RESTRICTED and from modifying system and security controls. Users are to be automatically logged off the CIS if their terminals have been inactive for some predetermined period of time, or the CIS must activate a password-protected screen saver after 15 minutes of inactivity.
17. Each user of the CIS is allocated a unique user account and ID. User accounts must be automatically locked once at least five successive incorrect login attempts have been made.
18. All users of the CIS must be made aware of their responsibilities and the procedures to be followed to protect information classified RESTREINT UE/EU RESTRICTED on the CIS. The responsibilities and procedures to be followed must be documented and acknowledged by users in writing.
19. SecOPs must be available for the users and administrators and must include descriptions of security roles and associated list of tasks, instructions and plans.

#### ***Accounting, audit and incident response***

20. Any access to the CIS must be logged.
21. The following events must be recorded:
  - (a) all attempts to log on, whether successful or failed;
  - (b) logging off (including being timed out, where applicable);
  - (c) creation, deletion or alteration of access rights and privileges;
  - (d) creation, deletion or alteration of passwords.
22. For all of the events listed above, the following information must be communicated as a minimum:
  - (a) type of event;
  - (b) user ID;
  - (c) date and time;
  - (d) device ID.

23. The accounting records should provide help to a security officer to examine the potential security incidents. They can also be used to support any legal investigations in the event of a security incident. All security records should be regularly checked to identify potential security incidents. The accounting records must be protected from unauthorised deletion or modification.
24. The beneficiary must have an established response strategy to deal with security incidents. Users and administrators must be instructed on how to respond to incidents, how to report them and what to do in the event of emergency.
25. The compromise or suspected compromise of information classified RESTREINT UE/EU RESTRICTED must be reported to the granting authority. The report must contain a description of the information involved and a description of the circumstances of the compromise or suspected compromise. All users of the CIS must be made aware of how to report any actual or suspected security incident to the security officer.

### ***Networking and interconnection***

26. When a beneficiary CIS that handles information classified RESTREINT UE/EU RESTRICTED is interconnected to a CIS that is not accredited, this significantly increases the threat to both the security of the CIS and the RESTREINT UE/EU RESTRICTED information that is handled by that CIS. This includes the internet and other public or private CIS, such as other CIS owned by the beneficiary or subcontractor. In this case, the beneficiary must perform a risk assessment to identify the additional security requirements that need to be implemented as part of the security accreditation process. The beneficiary shall provide to the granting authority, and where required by national laws and regulations, the competent SAA, a statement of compliance certifying that the beneficiary CIS and the related interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.
27. Remote access from other systems to LAN services (e.g. remote access to email and remote SYSTEM support) is prohibited unless special security measures are implemented and agreed by the granting authority, and where required by national laws and regulations, approved by the competent SAA.

### ***Configuration management***

28. A detailed hardware and software configuration, as reflected in the accreditation/approval documentation (including system and network diagrams), must be available and regularly maintained.
29. The beneficiary's security officer must conduct configuration checks on hardware and software to ensure that no unauthorised hardware or software has been introduced.
30. Changes to the beneficiary CIS configuration must be assessed for their security implications and must be approved by the security officer, and where required by national laws and regulations, the SAA.
31. The system must be scanned for any security vulnerabilities at least once a quarter. Software to detect malware must be installed and kept up-to-date. If possible, such software should have a national or recognised international approval, otherwise it should be a widely accepted industry standard.
32. The beneficiary must develop a business continuity plan. Back-up procedures must be established to address the following:
  - (a) frequency of back-ups;
  - (b) storage requirements on-site (fireproof containers) or off-site;
  - (c) control of authorised access to back-up copies.

***Sanitisation and destruction***

33. For CIS or data storage media that have at any time held RESTREINT UE/EU RESTRICTED information the following sanitisation must be performed to the entire system or to storage media before its disposal:
- (a) flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must be overwritten at least three times and then verified to ensure that the original content cannot be recovered, or be deleted using approved deletion software;
  - (b) magnetic media (e.g. hard disks) must be overwritten or degaussed;
  - (c) optical media (e.g. CDs and DVDs) must be shredded or disintegrated;
  - (d) for any other storage media, the granting authority or, if appropriate, the NSA, DSA or SAA should be consulted on the security requirements to be met.
34. Information classified RESTREINT UE/EU RESTRICTED must be sanitised on any data storage media before it is given to any entity that is not authorised to access information classified RESTREINT UE/EU RESTRICTED (e.g. for maintenance work).
-

## ANNEX IV

**Facility and personnel security clearance for beneficiaries or subcontractors involving RESTREINT UE/EU RESTRICTED information and NSAs/DSAs requiring notification of classified grant agreements at RESTREINT UE/EU RESTRICTED level <sup>(1)</sup>**

Member State	FSC		Notification of grant agreement or subcontract involving R-UE/EU-R information to NSA and/or DSA		PSC	
	YES	NO	YES	NO	YES	NO
Belgium		<b>X</b>		<b>X</b>		<b>X</b>
Bulgaria		<b>X</b>		<b>X</b>		<b>X</b>
Czechia		<b>X</b>		<b>X</b>		<b>X</b>
Denmark	<b>X</b>		<b>X</b>		<b>X</b>	
Germany		<b>X</b>		<b>X</b>		<b>X</b>
Estonia	<b>X</b>		<b>X</b>			<b>X</b>
Ireland		<b>X</b>		<b>X</b>		<b>X</b>
Greece	<b>X</b>			<b>X</b>	<b>X</b>	
Spain		<b>X</b>	<b>X</b>			<b>X</b>
France		<b>X</b>		<b>X</b>		<b>X</b>
Croatia		<b>X</b>	<b>X</b>			<b>X</b>
Italy		<b>X</b>	<b>X</b>			<b>X</b>
Cyprus		<b>X</b>	<b>X</b>			<b>X</b>
Latvia		<b>X</b>		<b>X</b>		<b>X</b>
Lithuania	<b>X</b>		<b>X</b>			<b>X</b>
Luxembourg	<b>X</b>		<b>X</b>		<b>X</b>	
Hungary		<b>X</b>		<b>X</b>		<b>X</b>
Malta		<b>X</b>		<b>X</b>		<b>X</b>
Netherlands	<b>X</b> (only for defence-related grant agreements and subcontracts)		<b>X</b> (only for defence-related grant agreements and subcontracts)			<b>X</b>
Austria		<b>X</b>		<b>X</b>		<b>X</b>
Poland		<b>X</b>		<b>X</b>		<b>X</b>

<sup>(1)</sup> These national requirements for FSC/PSC and notifications for grant agreements involving RESTREINT UE/EU RESTRICTED information must not place any additional obligations on other Member States or beneficiaries and subcontractors under their jurisdiction.  
N.B. Notifications of grant agreements involving CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information are obligatory.

---

Portugal		X		X		X
Romania		X		X		X
Slovenia	X		X			X
Slovakia	X		X			X
Finland		X		X		X
Sweden		X		X		X

---

## ANNEX V

**LIST OF NATIONAL SECURITY AUTHORITY / DESIGNATED SECURITY AUTHORITY DEPARTMENTS  
RESPONSIBLE FOR HANDLING PROCEDURES ASSOCIATED WITH INDUSTRIAL SECURITY****BELGIUM**

National Security Authority  
FPS Foreign Affairs  
Rue des Petits Carmes 15  
1000 Brussels

Tel.: +32 25014542 (Secretariat)

Fax: +32 25014596

Email: nvo-ans@diplobel.fed.be

**BULGARIA**

1. State Commission on Information Security – National Security Authority

4 Kozloduy Street

1202 Sofia

Tel.: +359 29835775

Fax: +359 29873750

Email: dksi@government.bg

2. Defence Information Service at the Ministry of Defence (security service)

3 Dyakon Ignatiy Street

1092 Sofia

Tel.: +359 29227002

Fax: +359 29885211

Email: office@iksbg.org

3. State Intelligence Agency (security service)

12 Hajdushka Polyana Street

1612 Sofia

Tel.: +359 29813221

Fax: +359 29862706

Email: office@dar.bg

4. State Agency for Technical Operations (security service)

29 Shesti Septemvri Street

1000 Sofia

Tel.: +359 29824971

Fax: +359 29461339

Email: dato@dato.bg

*(The competent authorities listed above conduct the vetting procedures for issuing FSCs to legal entities applying to conclude a classified contract, and PSCs to individuals implementing a classified contract for the needs of these authorities.)*

5. State Agency National Security (security service)

45 Cherni Vrah Blvd.

1407 Sofia

Tel.: +359 28147109

Fax: +359 29632188, +359 28147441

Email: dans@dans.bg

*(The above security service conducts the vetting procedures for issuing FSCs and PSCs to all other legal entities and individuals in the country applying to conclude a classified contract or classified grant agreement or implementing a classified contract or classified grant agreement.)*

## CZECHIA

National Security Authority  
Industrial Security Department  
PO BOX 49  
150 06 Praha 56

Tel.: +420 257283129

Email: sbr@nbu.cz

## DENMARK

1. Politiets Efterretningstjeneste  
(Danish Security Intelligence Service)

Klausdalsbrovej 1

2860 Søborg

Tel.: +45 33148888

Fax: +45 33430190

2. Forsvarets Efterretningstjeneste  
(Danish Defence Intelligence Service)

Kastellet 30

2100 Copenhagen Ø

Tel.: +45 33325566

Fax: +45 33931320

## GERMANY

1. For matters concerning industrial security policy, FSCs, transportation plans (except for crypto/CCI):  
Federal Ministry for Economic Affairs and Energy

Industrial Security Division – RS3

Villemombler Str. 76

53123 Bonn

Tel.: +49 228996154028

Fax: +49 228996152676

Email: dsagermany-rs3@bmwi.bund.de (office email address)

2. For standard visit requests from/to German companies:  
Federal Ministry for Economic Affairs and Energy  
Industrial Security Division – RS2  
Villemombler Str. 76  
53123 Bonn  
Tel.: +49 228996152401  
Fax: +49 228996152603  
Email: rs2-international@bmwi.bund.de (office email address)
  
3. Transportation plans for crypto material:  
Federal Office for Information Security (BSI)  
National Distribution Agency / NDA-EU DEU  
Mainzer Str. 84  
53179 Bonn  
Tel.: +49 2289995826052  
Fax: +49 228991095826052  
Email: NDAEU@bsi.bund.de

#### **ESTONIA**

National Security Authority Department  
Estonian Foreign Intelligence Service  
Rahumäe tee 4B  
11316 Tallinn  
Tel.: +372 6939211  
Fax: +372 6935001  
Email: nsa@fis.gov.ee

#### **IRELAND**

National Security Authority Ireland  
Department of Foreign Affairs and Trade  
76-78 Harcourt Street  
Dublin 2  
D02 DX45  
Tel.: +353 14082724  
Email: nsa@dfa.ie

#### **GREECE**

Hellenic National Defence General Staff  
E' Division (Security INTEL, CI BRANCH)  
E3 Directorate  
Industrial Security Office  
227-231 Mesogeion Avenue  
15561 Hologos, Athens  
Tel.: +30 2106572022, +30 2106572178  
Fax: +30 2106527612  
Email: daa.industrial@hndgs.mil.gr

**SPAIN**

Autoridad Nacional de Seguridad  
Oficina Nacional de Seguridad  
Calle Argentona 30  
28023 Madrid

Tel.: +34 912832583, +34 912832752, +34 913725928

Fax: +34 913725808

Email: nsa-sp@areatec.com

For information concerning classified programmes: programas.ons@areatec.com

For matters concerning personnel security clearances: hps.ons@areatec.com

For Transportation plans and international visits: sp-ivtco@areatec.com

**FRANCE**

National Security Authority (NSA) (for policy and for implementation in fields other than the defence industry)  
Secrétariat général de la défense et de la sécurité nationale  
Sous-direction Protection du secret (SGDSN/PSD)  
51 boulevard de la Tour-Maubourg  
75700 Paris 07 SP

Tel.: +33 171758193

Fax: +33 171758200

Email: ANSFrance@sgdsn.gouv.fr

Designated Security Authority (for implementation in the defence industry)  
Direction Générale de l'Armement  
Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)  
60 boulevard du général Martial Valin  
CS 21623  
75509 Paris CEDEX 15

Tel.: +33 988670421

Email: for forms and outgoing RFVs: dga-ssdi.ai.fct@intradef.gouv.fr

for incoming RFVs: dga-ssdi.visit.fct@intradef.gouv.fr

**CROATIA**

Office of the National Security Council  
Croatian NSA  
Jurjevska 34  
10000 Zagreb

Tel.: +385 14681222

Fax: +385 14686049

Email: NSACroatia@uvns.hr

**ITALY**

Presidenza del Consiglio dei Ministri  
D.I.S. – U.C.Se.  
Via di Santa Susanna 15  
00187 Roma

Tel.: +39 0661174266

Fax: +39 064885273

**CYPRUS**

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ

Εθνική Αρχή Ασφάλειας (ΕΑΑ)

Λεωφόρος Στροβόλου, 172-174

Στρόβολος, 2048, Λευκωσία

Τηλέφωνα: +357 22807569, +357 22807764

Τηλεομοιότυπο: +357 22302351

Email: cynsa@mod.gov.cy

Ministry of Defence

National Security Authority (NSA)

172-174, Strovolos Avenue

2048 Strovolos, Nicosia

Tel.: +357 22807569, +357 22807764

Fax: +357 22302351

Email: cynsa@mod.gov.cy

**LATVIA**

National Security Authority

Constitution Protection Bureau of the Republic of Latvia

P.O. Box 286

Riga LV-1001

Tel.: +371 67025418, +371 67025463

Fax: +371 67025454

Email: ndi@sab.gov.lv, ndi@zd.gov.lv

**LITHUANIA**

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija

(The Commission for Secrets Protection Coordination of the Republic of Lithuania)

National Security Authority

Pilaitės pr. 19

LT-06264 Vilnius

Tel.: +370 70666128

Email: nsa@vsd.lt

**LUXEMBOURG**

Autorité Nationale de Sécurité

207, route d'Esch

L-1471 Luxembourg

Tel.: +352 24782210

Email: ans@me.etat.lu

**HUNGARY**

National Security Authority of Hungary

H-1399 Budapest P.O. Box 710/50

H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Tel.: +36 13911862

Fax: +36 13911889

Email: nbf@nbf.hu

**MALTA**

Director of Standardisation  
Designated Security Authority for Industrial Security  
Standards & Metrology Institute  
Malta Competition and Consumer Affairs Authority  
Mizzi House  
National Road  
Blata I-Bajda HMR9010  
Tel.: +356 23952000  
Fax: +356 21242406  
Email: certification@mccaa.org.mt

**NETHERLANDS**

1. Ministry of the Interior and Kingdom Relations  
PO Box 20010  
2500 EA The Hague  
Tel.: +31 703204400  
Fax: +31 703200733  
Email: nsa-nl-industry@minbzk.nl
  
2. Ministry of Defence  
Industrial Security Department  
PO Box 20701  
2500 ES The Hague  
Tel.: +31 704419407  
Fax: +31 703459189  
Email: indussec@mindef.nl

**AUSTRIA**

1. Federal Chancellery of Austria  
Department I/10, Federal Office for Information Security  
Ballhausplatz 2  
10104 Vienna  
Tel.: +43 153115202594  
Email: isk@bka.gv.at
  
2. DSA in the military sphere:  
BMLV/Abwehramt  
Postfach 2000  
1030 Vienna  
Email: abwa@bmlvs.gv.at

**POLAND**

Internal Security Agency  
Department for the Protection of Classified Information  
Rakowiecka 2A  
00-993 Warsaw  
Tel.: +48 225857944  
Fax: +48 225857443  
Email: nsa@abw.gov.pl

**PORTUGAL**

Gabinete Nacional de Segurança  
Serviço de Segurança Industrial  
Rua da Junqueira n° 69  
1300-342 Lisbon  
Tel.: +351 213031710  
Fax: +351 213031711  
Email: sind@gns.gov.pt, franco@gns.gov.pt

**ROMANIA**

Oficiul Registrului Național al Informațiilor Secrete de Stat – ORNISS  
Romanian NSA – ORNISS – National Registry Office for Classified Information  
4th Mures Street  
012275 Bucharest  
Tel.: +40 212075115  
Fax: +40 212245830  
Email: relatii publice@orniss.ro, nsa.romania@nsa.ro

**SLOVENIA**

Urad Vlade RS za varovanje tajnih podatkov  
Gregorčičeva 27  
1000 Ljubljana  
Tel.: +386 14781390  
Fax: +386 14781399  
Email: gp.uvtp@gov.si

**SLOVAKIA**

Národný bezpečnostný úrad  
(National Security Authority)  
Security Clearance Department  
Budatínska 30  
851 06 Bratislava  
Tel.: +421 268691111  
Fax: +421 268691700  
Email: podatelna@nbu.gov.sk

**FINLAND**

National Security Authority  
Ministry for Foreign Affairs  
P.O. Box 453  
FI-00023 Government  
Email: NSA@formin.fi

**SWEDEN**

## 1. National Security Authority

Utrikesdepartementet (Ministry for Foreign Affairs)

UD SÄK / NSA

SE-103 39 Stockholm

Tel.: +46 84051000

Fax: +46 87231176

Email: ud-nsa@gov.se

## 2. DSA

Försvarets Materielverk (Swedish Defence Materiel Administration)

FMV Säkerhetsskydd

SE-115 88 Stockholm

Tel.: +46 87824000

Fax: +46 87826900

Email: security@fmv.se

---