Council of the European Union

Brussels, 20 June 2025
(OR. en)

5307/3/25
REV 3

LIMITE

CSC 32

Interinstitutional File:
2022/0084 (COD)

NOTE

From:	General Secretariat of the Council
To:	Security Committee
No. prev. doc.:	5307/2/25 REV 2; 7670/22 + ADD 3
Subject:	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 – Chapter 5 EUCI, Section 3 Physical Security + Annex III - final draft proposal

1. In the context of the written consultation on document 5307/2/25 REV 2, the GSC received comments from the Czech delegation outlined in WK 7507/25.

2. Consequently, the GSC launched a second written consultation informing the delegations of the intention of the GSC to issue a final revised version 5307/3/25 REV 3 which would incorporate the modifications proposed by the Czech delegation.

3. Since no objection was received by the General Secretariat by the deadline set for that written consultation, the GSC has prepared the final revised version as set out in the Annex to this note.

4. New text compared to the previous version is in **bold underlined**, deletions are indicated in **~~bold strikethrough~~**. Deleted original text is indicated in ~~strikethrough~~.

5. Given the outcome of the second written consultation, the final revised version as set out in 5307/3/25 REV 3 is now considered as provisionally approved.

ANNEX

SECTION 3
PHYSICAL SECURITY

Article 27

Basic principles

1. Each Union ~~institution and body~~ **entity** shall determine the physical security measures appropriate to its sites **to prevent unauthorised access to EUCI** ~~in accordance with Annex III and the principle of defence in depth~~ on the basis of a risk assessment performed ~~by its Security Authority~~ **in accordance with Article 5**.

1a. Union ~~institutions and bodies~~ **entities** shall put in place physical security measures for all sites where EUCI is discussed, stored or handled, including areas housing communication and information systems as referred to in Section 5 of this Chapter. *[moved from paragraph 2]*

1b. **In line with the principle of defence in depth, such** ~~The~~ **physical security** measures shall ensure the following objectives:

(a) to ~~deny~~ **prevent** ~~access to EUCI or~~ **surreptitious or** forced entry by an **unauthorised individual** ~~intruder~~;

(b) to deter, impede and detect unauthorised actions and respond to security incidents as soon as possible;

(c) to allow for segregation of personnel in their access to EUCI on **the basis of** ~~a~~ **their** need-to-know ~~basis~~ and**,** where appropriate, ~~on a~~ **their personnel** security clearance ~~basis~~.

~~2. Union institutions and bodies shall put in place physical security measures for all sites where EUCI is discussed, stored or handled, including areas housing communication and information systems as referred to in Section 5 of this Chapter.~~ *[moved to paragraph 1a]*

~~3~~ **2**. Only ~~security~~ equipment approved by the Security Authority of a Union ~~institution or body~~ **entity** shall be used for physically protecting information classified CONFIDENTIEL UE/EU CONFIDENTIAL or **above** ~~higher~~.

2a. Sites where EUCI is handled, stored or discussed shall be subject to regular assessment by the Security Authority of a Union entity.

~~4~~ **3**. Union ~~institutions and bodies~~ **entities** may share Secured Areas, as referred to in **Article 29b** ~~Annex III,~~ for handling**,** ~~and~~ storing **or discussing** EUCI, upon conclusion of an agreement.

Article 28

Sub-group on physical security

1. The sub-group on physical security as referred to in Article 7(1)~~, point~~ (c), shall have the following roles and responsibilities:

(a) preparing **for the Coordination Group recommendations for** guidance documents relative to physical security matters~~; (b) defining the~~**, in particular** general security criteria for acquiring equipment such as security containers, shredding machines, door**s,** locks, ~~electronic~~ access control systems **(ACS),** intrusion detection systems **(IDS)** and alarm systems for the physical protection of EUCI;

~~(c)~~**(b)** assisting Union ~~institutions and bodies~~ **entities** in determining the appropriate security measures ~~for their sites; (d) proposing compensatory measures~~ for the protection of EUCI **on their sites and compensatory measures** when EUCI is handled**, stored or discussed** outside **such sites** ~~the physically protected areas of a Union institution and body~~.

Article 29

Physical protection of EUCI

1. **Two types of physically protected areas shall be established for** ~~To ensure~~ the physical protection of EUCI~~, the Union institutions and bodies shall establish the following physically protected areas~~:

   (a) **Aa**dministrative **Aa**reas, as referred to in **Article 29a** ~~Annex III~~;

   (b) ~~where appropriate,~~ Secured Areas**,** ~~including Class I, Class II and technically Secured Areas~~ as referred to in **Article 29a** ~~Annex III~~.

2. The Security Authority of the Union ~~institution and body~~ **entity** concerned shall **be responsible for ensuring that only those areas that meet the requirements** ~~conduct an internal inspection to verify whether the conditions for an area to be established as an Administrative Area or a Secured Area,~~ set out in **Article 29a be designated as Administrative Areas or Secured Areas** ~~Annex III, are met~~. ~~Where the inspection report indicates that the conditions are met, the Security Authority may issue an accreditation for the Secured Area~~

   A Secured Area may be designated as such only upon approval by the Security Authority of the Union entity concerned that the area can ~~to~~ protect EUCI up to the stated **security classification** level ~~for a period not exceeding 5 years~~. ~~The Security Authority of the Union institution or body concerned shall be responsible for carrying out the re-accreditation process of its Secured Areas, before the expiry of the accreditation or whenever changes have been implemented within the accredited area.~~

3. Each Union ~~institution and body~~ **entity** shall ~~adopt~~ **establish** procedures for managing **security** keys and combination settings ~~for offices, rooms~~ **used for protecting EUCI at level CONFIDENTIEL UE/EU CONFIDENTIAL and above against unauthorised access at sites and in** strong rooms and security containers ~~for level CONFIDENTIEL UE/EU CONFIDENTIAL and for higher levels~~.

4. The Security Authority **of the Union entity concerned** may authorise entry and exit searches to deter and detect the unauthorised introduction of material or the unauthorised removal of EUCI from sites.

~~5. Union institutions and bodies shall establish the measures for the physical protection of the EUCI in accordance with Annex III.~~

Article 29a

Physically protected areas

1. An Administrative Area **shall** ~~must~~ meet the following requirements:

(a) ~~have~~ **the area has** a ~~visibly~~ **clearly** defined **and protected** perimeter ~~which allows individuals and, where possible, vehicles to be checked~~ **through which all entries and exits are controlled at all times**;

(b) ~~ensure that~~ windows that ~~might~~ **could** allow unauthorised visual access to EUCI within the area are ~~made~~ opaque or equipped with blinds, curtains, or other coverings;

(c) the area is equipped with access control carried out by electronic or electro-mechanical means, by security personnel or by any other physical means;

~~(c)~~**(d)** unescorted access **to the area** is ~~to be~~ granted only to individuals who are ~~duly~~ authorised by the Security Authority of the Union ~~institution or body~~ **entity** concerned;

~~(d)~~**(e)** all other individuals are escorted at all times or ~~be~~ subject to equivalent **measures** ~~controls~~.

2. ~~In addition to the requirements provided in point 1, a~~ **A** Secured Area **shall** ~~must~~ meet the following requirements:

(a) ~~have~~ **the area has** a ~~visibly~~ **clearly** defined and protected perimeter through which **all** entr~~y~~**ies** and exit**s** ~~is~~ **are** controlled at all times;

~~(b) be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment;~~

~~(c) be equipped with access control and real time monitoring intrusion detection system ('IDS') combined with response security personnel;~~

~~(d) be inspected at the end of normal working hours and at random intervals outside normal working hours where it is not occupied by duty personnel on a 24-hour basis and there is no real time monitoring (IDS) in place;~~

(b) the area is equipped with access control carried out by electronic or electro-mechanical means, by security personnel or by any other physical means;

(c) when not occupied by duty personnel on a 24-hour basis, the area is:

(i) equipped with a real-time surveillance intrusion detection system (IDS) in combination with response security personnel; or

(ii) locked and inspected at the end of working hours and at random intervals outside working hours;

~~(e)~~**(d)** ~~be managed~~ **the area is operated** by trained, supervised and appropriately security-cleared security personnel;

(e) windows that could allow unauthorised visual access to EUCI within the area are opaque or equipped with blinds, curtains, or other coverings;

(f) ~~have~~ **the area has** security operating procedures (**SecOPs) established by the Security Authority of the Union entity concerned** including the following elements:

(i) the level of EUCI which may be handled, **stored or** discussed ~~and stored~~ in the area;

(ii) the surveillance and protective measures to be maintained;

(iii) **a list of** the individuals **who are** authorised ~~**by the Security Authority of the Union entity concerned**~~ to have unescorted access to the area by virtue of their **need-to-know and, where appropriate, their personnel security clearance** ~~authorisation to access EUCI and need-to-know~~;

(iv) ~~where appropriate,~~ the procedures for escorts ~~or for protecting EUCI when authorising any other individuals to access the area,~~;

(v) rules on the presence and use of personal electronic devices in the area;

(v**i**) any other relevant measures and procedures.

~~3. Where entry into a Secured Area constitutes direct access to the classified information contained in it, the area must be established as a Class I Area and where that is not the case the area must be established as a Class II area.~~

~~For both classes of Secured Area referred to in the first subparagraph and in addition to the requirements provided in point 2, the Security Department/Officer of the Union institution or body concerned must clearly indicate the level of the highest security classification of the information normally held in the area and must clearly define a perimeter which allows individuals and, where possible, vehicles to be checked.~~

~~Union institutions and bodies must ensure that individuals accessing a Secured Area fulfil the following criteria:~~

~~(a) require specific authorisation to enter the area;~~

~~(b) be escorted at all times;~~

~~(c) be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible.~~

3. A Secured Area the entry to which implies direct access to EUCI shall be designated as a Class I Secured Area. It shall meet the following ~~additional~~ requirements in addition to those defined in paragraph 2:

(a) at the entry to the area there is a clear indication of its class and of the highest classification level of EUCI to which the entry gives access; and

(b) the area has an entry control system which admits access only to those individuals who hold an appropriate personnel security clearance and who are specifically authorised to enter the area.

3a. A Secured Area the entry to which does not imply direct access to EUCI shall be designated as a Class II Secured Area. It shall meet the following ~~additional~~ requirements in addition to those defined in paragraph 2:

(a) the area has an entry control system which admits access to those individuals who have an appropriate security clearance and who are specifically authorised to enter the area; and

(b) all other individuals are escorted at all times or subject to equivalent measures.

~~6.~~ **4.** A Secured Area ~~protected against passive and active eavesdropping~~ **may** ~~must~~ be designated as a ~~t~~**T**echnically Secured Area. **It shall meet** ~~T~~**t**he following requirements ~~apply~~ in addition to those **defined in paragraph 2, and in paragraphs 3 or 3a, as appropriate** ~~for Secured Areas~~:

(a) the area is protected against passive and active eavesdropping;

(b)~~(a) it must be~~ **the area is** equipped with a~~n~~ **real-time monitoring** IDS **in combination with response security personnel**, ~~be~~ **is** locked when not occupied and ~~be~~ **is** guarded when occupied. Any **security** keys **and combination settings are** ~~must be~~ managed in accordance with Article 29(3);

(c)~~(b) it must be~~ **the area is** ~~inspected~~ regularly physically or technically **inspected**, **including technical surveillance countermeasures (TSCM) inspection**, or both, **as required** by the Security Authority of the Union ~~institution or body~~ **entity** concerned **and**~~. Such inspections must also be conducted~~ following any unauthorised ~~entry~~ or ~~suspicion of such~~ **suspected unauthorised** entry **or after any reconstruction or renovation**;

(d) the area is free of communication lines, telephones or other communication devices or electrical or electronic equipment with recording or transmitting capabilities that have not been authorised by the Security Authority of the Union entity concerned; and

(e)~~(c)~~ ~~it must have~~ **the area has** appropriate acoustic ~~and TEMPEST~~ protection.

5. All persons entering ~~t~~**T**echnically Secured Areas ~~must~~ **shall** comply with the requirements set out in **paragraphs** ~~point~~ **3 or 3a**.

~~6. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.~~

~~7~~ **6.** ~~Strong rooms must be constructed within Secured Areas.~~ [A strong room is a room ~~with,~~ **which has a** reinforced physical construction **comprising** ~~where the Security Authority of the Union institution or body concerned approves~~ the walls, floors, ceilings, windows and lockable doors **approved by the Security Authority of the Union entity concerned**. Such **strong** rooms **shall** ~~must~~ afford ~~equivalent~~ protection **equivalent** to **that of** a security container approved for the storage of EUCI of the same classification level. - *this part will be moved to Article 3 Definitions*]

Article 29b

Physical ~~protective measures~~ security requirements for handling and storing EUCI

~~8~~ **1**. EUCI ~~which is~~ classified **at level** RESTREINT UE/EU RESTRICTED ~~must~~ **shall** be handled ~~and stored~~ ~~in any of the following areas~~:

(a) in a Secured Area; **or**

(b) in an Administrative Area ~~provided the EUCI is protected from access by unauthorised individuals~~ or **other areas with equivalent physical protection.**

~~(c)~~ **In exceptional cases and provided the volume of EUCI is limited, it may be handled temporarily** outside a Secured Area or **an** Administrative Area **or other areas with equivalent physical protection** provided **that** the holder has undertaken to comply with compensatory measures decided by the Security Authority of ~~each~~ **the** Union ~~institution and body~~ **entity concerned to ensure that EUCI is protected from access by unauthorised individuals**.

~~9~~ **2**. EUCI ~~which is~~ classified **at level** RESTREINT UE/EU RESTRICTED **shall** ~~must~~ be stored **at least** in locked office furniture in an Administrative Area ~~or a Secured Area~~. **In exceptional cases and provided the volume of EUCI is limited, i**~~I~~t may ~~temporarily~~ be stored outside an Administrative Area or a Secured Area provided **that** the holder has undertaken ~~to store the documents concerned in appropriate locked office furniture when they are not being read or discussed~~ **to comply with compensatory measures decided by the Security Authority of the Union entity concerned to ensure that EUCI is protected from access by unauthorised individuals.**

~~10. Union institutions and bodies may handle and store RESTREINT UE/EU RESTRICTED information outside their sites provided the relevant information be protected appropriately. For such purpose, Union institutions and bodies must comply with the measures provided in point 8(c).~~

~~11~~ **3**. CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information ~~must~~ **shall** be handled ~~and stored~~ ~~in one of the following areas~~:

(a) in a Secured Area; **or**

(b) in an Administrative Area ~~provided the EUCI is protected from access by unauthorised individuals;~~.

~~(c)~~ **In exceptional cases and provided the volume of EUCI is limited, it may be handled temporarily** outside a Secured Area or an Administrative Area ~~where limited in volume and time and~~ provided **that** the holder:

(i) has undertaken to comply with compensatory measures decided by the Security Authority of the Union ~~institution or body~~ **entity** concerned **to ensure that EUCI is protected from access by unauthorised individuals;** ~~. In addition,the holder of EUCI must take the following steps:~~

(ii) keeps the EUCI under his or her personal control at all times;

(**iii**) **has** notifi**ed**~~y~~ the relevant registry ~~of the fact~~ that ~~classified documents are~~ **EUCI is** being handled ~~outside protected areas~~ **in accordance with this subparagraph.**

~~(ii) keep the document under their control at all times~~.

~~12~~ **4**. **EUCI classified at level** CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET ~~information must~~ **shall** be stored in a Secured Area ~~accredited to that level by the competent Security Accreditation Authority of the Union institution or body concerned~~, either:

(a) in~~side~~ a security container**;** or

(b) in~~side~~ a strong room**.**

[13. ~~Documents~~ **EUCI** classified **at level** CONFIDENTIEL UE/EU CONFIDENTIAL or higher ~~can~~ **shall** only be copied by the relevant Registry.] *[to be moved to EUCI management chapter]*

~~14~~ **5**. **EUCI classified at level** TR~~E~~**È**S SECRET UE/EU TOP SECRET ~~information must~~ **shall** be handled ~~and stored~~ in a Secured Area**. EUCI classified at level TRÈS SECRET UE/EU TOP SECRET shall be stored in a Secured Area** ~~accredited to that level. To that end, Union institutions and bodies may conclude the necessary arrangements to use a Secured Area hosted and accredited to the appropriate level by the Security Accreditation Authority of another Union institution and body.~~

~~15. TRES SECRET UE/EU TOP SECRET information must be stored in a Secured Area accredited to that level by the Security Accreditation Authority of the competent Union institution or body concerned under one of the following conditions~~ :

(a) in a security container ~~approved by the Security Authority of each Union institution and body~~ with **at least** one of the following supplementary controls:

(i) continuous protection or verification by **security-**cleared security ~~staff~~ **personnel** or **security-cleared** duty personnel; **or**

(ii) a~~n approved~~ **real-time monitoring** IDS in combination with ~~security~~ response **security** personnel~~.~~**; or**

(b) in ~~an IDS equipped~~ **a** strong room **equipped with a real-time monitoring IDS** in combination with ~~security~~ response **security** personnel.