



Council of the European Union
General Secretariat

Brussels, 06 May 2025

Interinstitutional files:
2022/0084 (COD)

WK 4576/2025 REV 1

**DOCUMENT ACCESSIBLE TO THE
PUBLIC (04.11.2025). ONLY
MARGINAL PERSONAL DATA
HAVE BEEN REDACTED.**

LIMITE

CSC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

CONTRIBUTION

From:	General Secretariat of the Council
To:	Security Committee
<hr/>	
N° prev. doc.:	6457/25
<hr/>	
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 2 Personnel Security + Annex II – comments by the Austrian, Belgian, French and Polish delegations and by the Commission

Delegations will find in the Annex comments by the Austrian, Belgian, French and Polish delegations and by the Commission on Chapter 5 EUCI, Section 2 Personnel Security + Annex II of the proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union, set out in doc. 6457/25 .

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 2 Personnel Security + Annex II (doc. 6457/25)

- comments by the Austrian, French and Polish delegations and by the Commission

1. Comments by the Austrian delegation

Article 23

Basic principles

1. The Security Authority of a Union ~~entity institution or body~~ may grant ~~individuals~~ access to EUCI where all the following conditions are met:
- (a) the individuals' ~~have a need-to-know~~ **has been determined**;
 - (b) the individuals have been briefed on the security rules and procedures for protecting EUCI and the relevant security standards and guidelines, and have acknowledged in writing their responsibilities with regard to protecting such information;
 - (c) for information classified **at level** CONFIDENTIEL UE/EU CONFIDENTIAL or ~~higher~~ **above**, the individuals have been granted **a personnel** security clearance (**PSC**) and have been authorised **to access EUCI** ~~to~~ **at** the relevant level.

[...]

- ~~3.~~ The Security Authority of each Union ~~entity institution and body~~ shall keep records of ~~their~~ **personal** security clearances, ~~briefings~~, written acknowledgements **of briefings** and authorisations to access EUCI.

[...]

Commented [REDACTED]: AT: Singular (align with CSR-wording). Please consider throughout document.

Commented [REDACTED]: AT: According to our national understanding, the "authorisation to access EUCI at the relevant level" can only be granted if lit a – c are fulfilled and is not a separate, additional requirement. We recognise the GSC might have a different understanding.

Following our logic, we suggest to clarify the article by moving the last part of lit c to a new lit d and to specify, that this does not apply to EUCI at level R-UE/EU-R.

Commented [REDACTED]: AT: Please see suggestion in the text.



Article 24

Authorisation to access EUCI

[...]

[2. Whenever an individual needs to be authorised to access information classified **at level CONFIDENTIEL UE/EU CONFIDENTIAL or higher above, a request for authorisation to access EUCI shall be sent to the Security Authority of the Union entity institution or body concerned shall inform the competent Security Authority, which shall proceed with the formalities required in point 1 of Annex II. - to be moved to Article 26a as paragraph 0]**

Commented [REDACTED]: AT: It is not self-explanatory by whom such a request must be sent (e.g. the individual itself may not send it). Please consider clarifying this responsibility in the text.

[...]

Article 25a

Change of employment within Union entities

1. **Where the holder of an authorisation to access EUCI takes up employment in another Union entity, the Security Authority of that Union entity shall notify the NSA or other national competent authority that had issued the PSC about this change.**

[...]

Article 26

EUCI Security briefings

1. The Security Authority of a Union ~~entity institution or body~~ shall brief all individuals who need to access EUCI, **including EUCI classified at level RESTREINT UE/EU RESTRICTED**, on any threats to security and about their **obligation to report any suspicious activity**. The briefing shall take place before access to EUCI is granted and **at regular intervals** at least every ~~53~~ years thereafter.

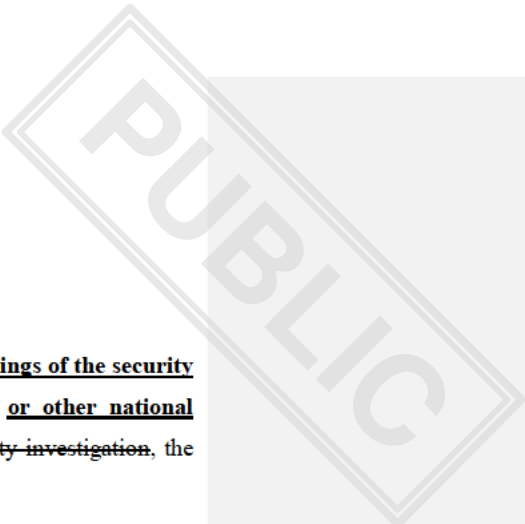
2. After receiving the briefing referred to in paragraph 1, all individuals concerned shall acknowledge in writing that they have understood their **obligations regarding the protection of EUCI and the consequences where in the event that EUCI is compromised.**

Commented [REDACTED]: AT: This briefing needs to cover both the obligation to protect and to report.

Commented [REDACTED]: AT: Should the "obligations regarding the protection etc." not be specified in para 1? Otherwise the specification in para 3 (which references para 1) does not make sense.

In the respective CSR provision (Art 7i – row 201) the ISR Article 26 para 1 and 2 (and their content) are merged.

[...]



Article 26a

Granting an authorisation to access EUCI

[...]

3. ~~Following notification~~ **After having received the outcome of the findings of the security vetting carried out by the relevant National Security Authority²⁵ or other national competent authority** ~~overall assessment of the findings of the security investigation, the competent Security~~ **Appointing Authority of the Union entity:**

(a) may grant an authorisation to access EUCI **in accordance with Art. 23** to the individual concerned up to the relevant level **until a specified date** ~~for a limited period of time,~~ in so far as the security ~~investigation~~ **vetting results in an assurance that nothing adverse is known which would call into question** ~~concludes on~~ the loyalty, trustworthiness and reliability of the individual; **or**

Commented [REDACTED]: AT: See AT Comment regarding Art 23 lit c.

[...]

Article 26c

Renewal of authorisation

[...]

9.3. The individual concerned must take **a refresher course** on handling and storing EUCI each time their security clearance is renewed. - *Article 26c to be discussed, drafting proposals to be provided as appropriate*

Commented [REDACTED]: AT: Please clarify.

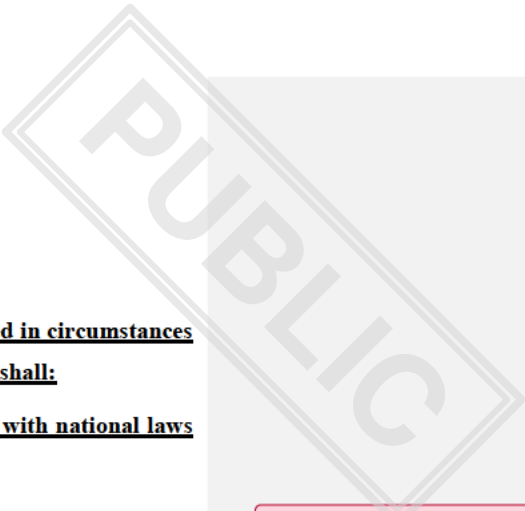
Article 26d

[...]

12.3. After receiving a briefing in accordance with Article 26, all individuals who have been granted **a** temporary authorisation to access EUCI ~~must~~ **shall** acknowledge in writing that they have understood their **obligations in respect of protecting EUCI and the consequences if EUCI is compromised.** The Security Authority of the Union ~~entity~~ **institution or body** concerned ~~must~~ **shall** keep a record of the written acknowledgement.

Commented [REDACTED]: AT: Please see comment above. The content/scope of the briefing in Art 26 needs to be clarified.

[...]



Article XX

Potential access to EUCI

1. Where an individual who does not have a need to know is employed in circumstances in which that individual might have access to EUCI, the individual shall:
 - (a) hold a PSC or undergo a security verification in accordance with national laws and regulations;
 - (b) have been briefed on the security rules and procedures for protecting EUCI and on their responsibilities with regard to protecting EUCI in case they have to access it.
2. Couriers shall hold a valid PSC in accordance with national laws and regulations, have been briefed on the security procedures for protecting EUCI and on their responsibilities with regard to protecting such EUCI entrusted to them.

Commented [REDACTED]: AT: Please consider AT comment in row 130 of doc 6935/25. Individuals should have to be briefed on their responsibilities and on the "consequences in the event that EUCI is compromised".

Commented [REDACTED]: AT: Please see comment above.

Article 26e

National experts seconded to Union ~~entities institutions and bodies~~

13. All Union ~~entities institutions and bodies~~ shall ~~must~~ ensure that national experts seconded to them for a position requiring a personnel security clearance ~~present~~, prior to taking up their assignment, a valid ~~Ppersonnel Ssecurity Cclearance or a Ppersonnel Ssecurity Cclearance Ccertificate~~, granted according to national laws and regulations, to the competent Security Authority. Provided that the requirements referred to in Article 23(1) are met, the Security Authority may ~~then~~ grant an authorisation to access EUCI up to the level equivalent to the one referred to in the ~~national security clearance~~ PSC, with a maximum validity not longer than the duration of their assignment.

Commented [REDACTED]: AT: Please consider rewording the first sentence and to find an alternative for "present". An individual seconded to a EUIBA technically is not able to present a PSC themselves. They might hold one but it is the respective NSA's responsibility to confirm it.

2. Comments by the Belgian delegation

General comment:

- The use of terminology 'competent Security Authority' and 'Appointing Authority' is not entirely clear throughout the text. Can they be clearly defined in the first articles?

Article 23 - Basic principles

Paragraph 1

- Suggestion to clearly define 'authorisation' in this context, and the instance that authorises
- Can explicit mention be made of the principle that a person should always have a *valid* PSC in order to have access to EUCI?

Paragraph 2, 2: security office of the Union entity' or 'security offices of the Union entities'. Or are there multiple security offices for a Union entity?

Could you specify the exact function of the Commission in case an SLA is concluded? Is the consequence only that the Commission becomes the contact point for the NSA, or does the Commission take up several tasks within the authorisation process?

Article 25a – Change of employment within Union entities

Paragraph 2 : Does the NSA inform the Security Authority of the Union entity explicitly that there is no objection, or does this article include a 'tacit non-objection'? Belgium is not in favor of a tacit non-objection, a change in employer requires a new PSC or an approval of transfer.

Article 26 – Security briefings

Paragraph 1

- Is the scope of a security briefing as described in this paragraph not larger (e.g. also includes the obligations of the individual concerning the storage, transport etc of EUCI)?
- We are not sure whether an interval of maximum 3 years between security briefings suffices. For information : Belgium requests a briefing annually (S) or bi-annually (TS).

Paragraph 3a: BE: Not clear why a distinction is made between different briefings in this article? Suggestion to enlarge the scope of the briefing in §1 in order to delete §3a?

Since a briefing should also take place for the level R-UE/EU-R, it is not clear why there is made reference to 'in particular EUCI classified at level C-UE/EU-C or above'.

Article 26a – Granting authorisation to access EUCI

Paragraph 3 :

- First line: Would it be clearer to mention 'after the individual concerned received the PSC from the NSA or other national competent authority, the Appointing Authority of the Union entity':...
- Lit 2 and 3 (see also article 26b, §2): It is not clear how this 'possibility to be heard' relates to existing national appeal mechanisms. In Belgium f.ex. an appeal at the Appeal Court is possible against a refusal of a PSC for EUCI, but only in the case of a refusal or a lack of decision within the time limits provided for in the legal framework. Moreover, the law provides for strict appeal deadlines (30 days), which might be difficult to respect if
- Lit 2 : 'the information' => 'the decision from the NSA or other'.

PUBLIC

Paragraph 4: A request for a clearance has to be personal, specific and current. As a consequence, a delayed entry into service should not be accepted and a break of more than 6 months means the invalidity of the actual clearance and the start of a new request/investigation if clearance needed.

Article 26b – Suspension and withdrawal of authorisation to access EUCI

Paragraph 2: The NSA does not withdraw the 'assurance the nothing adverse is known', but withdraws the PSC. From the moment a PSC is withdrawn, the 'authorisation to access EUCI' becomes invalid, because it is no longer 'covered' by a valid PSC.

Article 26c – Renewal of authorisation

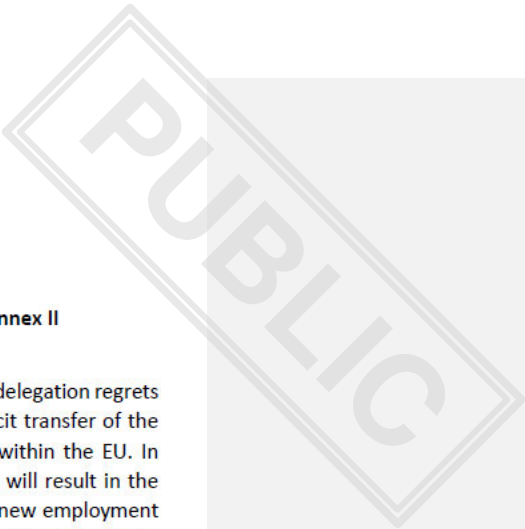
Paragraph 2: Belgium is not in favor of a possible 'tacit' extension of the PSC. A timely renewal should be asked at the NSA, if the renewal is not received before the expiration of the PSC, the individual cannot be assigned to duties that require a PSC.

Article 26d – Temporary authorisation to access EUCI

Is our understanding correct that this article allows a (temporary) authorisation without (valid) PSC? Belgium supports the principle that an authorisation to access EUCI should always be covered by a valid PSC (see comment on article 23, paragraph 1).

Article 26f – access to classified meetings

Paragraph 2 : since it is the NSA who delivers the PSC, should it not be the NSA who delivers a PSC Certificate? Following the logic of the text, the Security Authority could deliver an 'authorisation to access EUCI certificate'.



3. Comments by the French delegation

FR Written comments: Chapter 5 EUCI, Section 2 Personnel Security + Annex II

With regard to Article 25a (change of employment within Union entities), the French delegation regrets the lack of time allowed for the national security authority (NSA) to object to a tacit transfer of the validity of the authorisation in the event of an individual changing employment within the EU. In France, a security clearance is valid for a specific position. Any change of position will result in the termination of the clearance and a new procedure will have to be initiated by the new employment authority with the national security authority. The proposal made by the Swedish delegation at the Security Committee meeting on 17-18 March to share a list specifying national procedures and obligations with regard to clearance for EU entities could be a possible option to consider.

With regard to Article 26 (security briefings), the French delegation would not want an individual's responsibility in the event of a compromise to be restricted solely to compromises 'resulting from a breach of security'. The delegation proposes maintaining the original paragraph, and therefore deleting 'following a breach of security'.

With regard to Article 26a (granting an authorisation to access EUCI), paragraph b (last paragraph), the French delegation proposes not to limit the reasons that may prompt an individual to inform his security officer of changes in his personal situation that may have an impact on his clearance. The delegation therefore proposes adding the word 'including' before the list of proposed situations.

With regard to Article 26c (renewal of authorisation), the French delegation is in favour of retaining Article 26c in order to harmonise the procedures relating to the renewal of clearances for all EU entities - the objective pursued by this Regulation. To this end, the delegation proposes that the procedure defined in the Council security rules be used as a basis.

4. Comments by the Polish delegation

Regarding doc. 6457/25 art 26a p.4 we propose not to list information concerning the changes in individuals life- just make the provision more general.

PUBLIC

5. Comments by the Commission

Article 23

Basic principles

1. The Security Authority of a Union ~~entity institution or body~~ may grant individuals access to EUCI where all the following conditions are met:

[...]

(c) for information classified **at level** CONFIDENTIEL UE/EU CONFIDENTIAL or ~~higher~~ **above**, the individuals have been granted **a personnel** security clearance (**PSC**) and have been authorised **to access EUCI to at** the relevant level.

[...]

Commented [REDACTED]: Consistency in the whole document: either CONFIDENTIEL UE/EU CONFIDENTIAL or above OR higher

Article 25

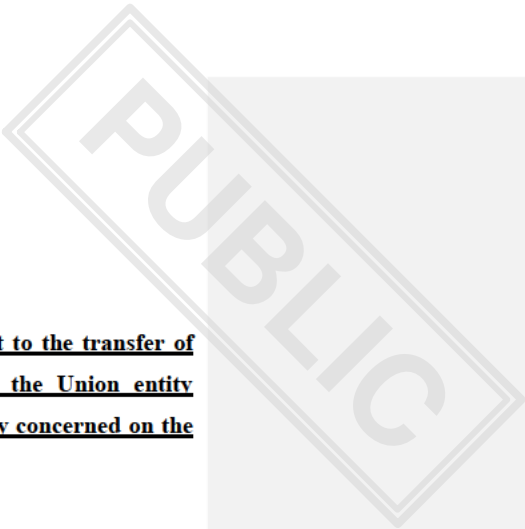
Recognition of authorisations to access EUCI

[1. An authorisation to access EUCI up to the specified level shall be valid in any Union **entity** ~~institution or body~~ to which the individual is assigned.

2. Union ~~entities institutions and bodies~~ shall accept authorisations to access EUCI granted by other Union **entity** ~~institution or body~~. - *paragraphs 1 and 2 will be discussed at a later stage in the context of classified meetings, see Article 26f*

~~[3. Where the holder of an authorisation to access EUCI takes up employment in another Union institution or body, that Union institution or body shall notify the relevant NSA of a change of employer, through the competent Security Authority. - paragraph moved to new Article 25a paragraph 1, see below]~~

Commented [REDACTED] COM insists to keep this article here as its content is not limited to classified meetings only but broader, to access to classified information or Secured Areas.



Article 25a

Change of employment within Union entities

[...]

2. If the NSA or other national competent authority does not object to the transfer of the PSC to the new employment, the Security Authority of the Union entity concerned may grant an authorisation to access EUCI in the entity concerned on the basis of the existing PSC.

[...]

Article 26

EUCI Security briefings

1. The Security Authority of a Union ~~entity institution or body~~ shall brief all individuals who need to access EUCI, including EUCI classified at level RESTREINT UE/EU RESTRICTED, on any threats to security and about their obligation to report any suspicious activity. The briefing shall take place before access to EUCI is granted and at regular intervals at least every 53 years thereafter.

[...]

- 3a. In addition to the briefing referred to in paragraph 1, all individuals to whom a PSC has been issued, shall also receive a briefing on the responsibility to protect EUCI, including EUCI classified at level CONFIDENTIEL UE/EU CONFIDENTIAL or above, and at regular intervals thereafter not exceeding 3 years. They shall acknowledge in writing that they have understood their obligations with respect to the protection of EUCI, in particular EUCI classified at level CONFIDENTIEL UE/EU CONFIDENTIAL or above, and the consequences in the event that EUCI is compromised.

4. Where individuals who have been granted authorisations to access EUCI no longer require such access, the Security Authority of the Union entity institutions and bodies shall ensure that those individuals ~~are aware of, and where appropriate acknowledge in writing,~~ receive a briefing on their obligations in respect of the continued protection of EUCI and on the consequences of non-compliance. They shall acknowledge in writing that they have understood those obligations and the consequences in the event the EUCI is compromised.

[...]

Commented [REDACTED]: I would add «and at issuance of a new security autorisation».

Commented [REDACTED]: COM finds this paragraph redundant as the briefing already mentioned under para 1 covers all levels of classification. Same for the acknowledgement, there is no need to repeat same requirements from para 2.

Commented [REDACTED]: This is again a repetition of the same text, can be replaced with a reference to para 2.

Article 26a

Granting an authorisation to access EUCI

1. The Security Authority of the Union ~~entity institution and body~~ concerned ~~must~~ **shall** seek the written consent of the individual for the security clearance procedure before sending a completed **national** security clearance questionnaire to the National Security Authority **or other competent authority** of the Member State of ~~which nationality~~ of the applicant is **a national or which otherwise has a responsibility for vetting the individual.**

[...]

3. ~~Following notification~~ **After having received the outcome of the findings of the security vetting carried out by the relevant National Security Authority's or other national competent authority overall assessment of the findings of the security investigation, the competent Security** ~~Appointing Security Authority of the Union entity:~~

[...]

In these circumstances the individual may ask to be heard by the Appointing Security Authority of the Union entity concerned. Any complaint concerning the information provided by an NSA or other national competent authority shall be directed to the national competent authority and be treated in accordance with the relevant laws and regulations in force in the Member State concerned.

If, after having heard the individual, the Appointing Security Authority considers that there are elements that may have an impact on the initial outcome of the security vetting, it shall inform the NSA or other national competent authority thereof without delay. Where the NSA or other national competent authority maintains that the initial outcome of the security vetting did not result in an assurance as referred to in point (b), the Appointing Security Authority shall not grant an authorisation to access EUCI.

4. Where the individual starts service 12 months or more after the date of the notification of the result of the security ~~investigation~~ **vetting**, or when there is a break of 12 months **or more** in the individual's service, the competent Security Authority ~~must~~ **shall** seek confirmation from the ~~relevant~~ National Security Authority **or other national competent authority** about the validity of ~~that~~ **the personnel** security clearance **remains valid and appropriate.**

Commented [REDACTED]: COM opposes to the extending of the possibility for Union entities to ask for the security vetting of individuals with other nationalities then those of MSs.

Commented [REDACTED]: In accordance with the Staff Regulations, the Appointing Authority of a Union entity is the Authority assigning officials to a certain post or function. Pls revert to Security or other competent authority.

Commented [REDACTED]: Unclear to what these circumstances refer to, to be redrafted and refer to point (b) above

Commented [REDACTED]: It is the competence of Union entities to treat the complaints against their administrative decisions. It is not the complaint that is redirected to the MSs but the complainant.

Commented [REDACTED]: Union entities are not in a position to «consider» if there are elements that can impact the security vetting findings as they are not aware of such findings, apart from the negative or positive outcome.

Individuals who have an authorisation to access to EUCI shall immediately notify the Security Authority of the Union entity concerned of any significant change to any of the following personal circumstances that could have an impact on their personnel security clearance or authorisation to access EUCI:

Commented [REDACTED]: The text adds obligations to the individuals working for the Union entities, who are not the addressees of this Regulation. To be redrafted in respect of the Commission proposal and its original scope.

[...]

Article 26b

Suspension and withdrawal of authorisation to access EUCI

5.1. Where information concerning a security risk posed by an individual who has authorisation to access EUCI **or information concerning any such individual that could be relevant for security vetting** becomes known to the Union ~~entity institution or body~~ concerned, the Security Authority of that Union ~~entity institution or body~~ **shall must** notify the relevant National Security Authority **or other national competent authority** thereof. ~~The Appointing Security Authority~~ **and** may suspend ~~the individual's access to EUCI~~ or withdraw **the individual's** authorisation to access EUCI.

1a. **Where the Appointing Security Authority decides to suspend or withdraw the authorisation of an individual to access EUCI, the Security Authority shall notify the individual concerned and the NSA or other national competent authority thereof.**

The individual concerned may ask to be heard by the Appointing Security authority. Any complaint concerning the information provided by an NSA or other national competent authority shall be directed to the national competent authority and be treated in accordance with the relevant laws and regulations in force in the Member State concerned.

6.2. Where ~~a an~~ National Security Authority **or other national competent authority** notifies the relevant Union ~~entity institution or body~~ that there is no longer **that it has withdrawn an** assurance **given in accordance with Article 26a(3)(a)** for an individual who has **an authorisation to** access to EUCI, the Security ~~Appointing Security~~ Authority of the Union ~~entity institution or body~~ concerned **shall must immediately suspend** ~~withdraw~~ its security authorisation **to access EUCI** and **and shall notify the individual accordingly** ~~exclude the individual from access to EUCI,~~ in accordance with its relevant rules.

Commented [REDACTED]: This is a repetition of 2nd paragraph of Article 26(a)(3) therefore can be replaced with a reference to it. Same remark as previously.

In these circumstances the individual may ask to be heard by the Appointing Security Authority of the Union entity concerned.

Commented [REDACTED]: Again a repetition

If, after having heard the individual, the ~~Appointing Security~~ Authority considers that there are elements that may have an impact on the initial outcome of the security vetting, it shall inform the NSA or other national competent authority thereof without delay. Where the NSA or other national competent authority maintains its decision on withdrawal, the ~~Appointing Security~~ Authority shall withdraw the individual's authorisation to access EUCI. Any complaint concerning the information provided by an NSA or other national competent authority shall be directed to the national competent authority and be treated in accordance with the relevant laws and regulations in force in the Member State concerned.

Commented [REDACTED]: It's not the initial outcome questioned here, as we are in a situation of potential suspension or withdrawal of assurance.

Commented [REDACTED]: Pls see our remarks above, on the same text in the 3rd para of Article 3a(3).

[Article 26c]

Renewal of authorisation

[...]

8-2. The Security Authority of the Union institution and body concerned may extend the validity of an authorisation to access EUCI for a period of up to 12 months, where no adverse information has been received from the relevant National Security Authority or other competent national authority within a period of 2 months from the date of transmission of the request for renewal and the corresponding clearance questionnaire.

Commented [REDACTED]: COM insists on keeping this possibility for Union entities to renew an authorisation in absence of adverse information received from the competent NSA. This is essential to allow the continuity of access to EUCI for individuals who have been already vetted and for whom no negative information has been received in the context of the after care process.

Commented [REDACTED]: This is where COM issue a temporary authorisation for 6 months and then again 6 months

[...]

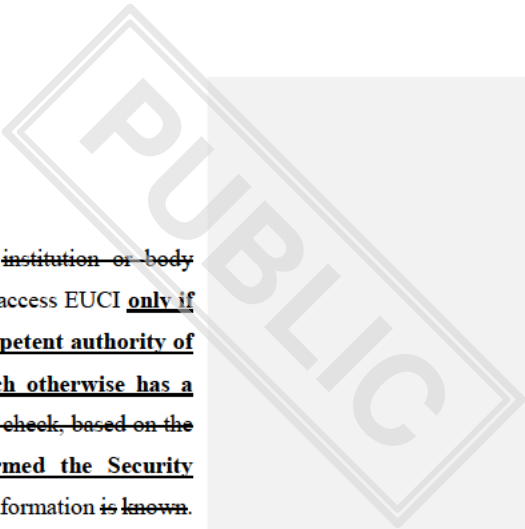
Article 26d

Exceptional Temporary security authorisation to access EUCI

0. ~~In exceptional circumstances, w~~Where duly justified in the interests of the service and pending completion of a full security investigation personnel security clearance procedures, the Security ~~Appointing Security~~ Authority of a Union ~~entity institution or body~~ may grant a temporary authorisation for individuals to access EUCI for a specific position function [without prejudice to the provisions regarding renewal of authorisation to access EUCI and] upon verification ~~by of the relevant~~ by the relevant National Security Authority. [- moved here from Article 24(4) and reworded]

Commented [REDACTED]: COM insists to have the possibility of granting an initial temporary authorisation only as exception, provided that Article 26c is kept and allows the temporary renewal.

Commented [REDACTED]: Same comment, to reinstate the exceptional circumstances.



10.1. The ~~Security~~ Appointing-Security Authority of the Union ~~entity~~ institution or body concerned may ~~exceptionally~~ grant such a temporary authorisation to access EUCI only if ~~provided that the competent~~ National Security Authority or other competent authority of the Member State of which the individual is a national or which otherwise has a responsibility for vetting the individual has ~~conducted a preliminary check, based on the completed and transmitted security questionnaire, to verify~~ informed the Security Authority of the Union entity that ~~no~~ it is not aware of any adverse information is ~~known~~.

11.2. Temporary authorisation to access EUCI ~~can~~ shall be valid for ~~one single~~ a period not exceeding 6 months and may be extended for a further period not exceeding 6 months. ~~must~~ It shall not allow access to information classified ~~TRÈS SECRET UE/EU TOP SECRET~~.

2a. If the Appointing-Security Authority of the Union entity grants a temporary authorisation, it shall inform the competent authority as referred to in paragraph 1 thereof, as well as of any extension.

[...]

4. Without prejudice to this Article, the Appointing-Security Authority of a Union entity may grant a temporary authorisation to access EUCI under exceptional circumstances in accordance with its internal rules.

Article XX

Potential access to EUCI

1. Where an individual who does not have a need to know is employed in circumstances in which that individual might have access to EUCI, the individual shall:

[...]

2. Couriers shall hold a valid PSC in accordance with national laws and regulations, have been briefed on the security procedures for protecting EUCI and on their responsibilities with regard to protecting such EUCI entrusted to them.

[...]

Commented [REDACTED]: Would it not be better to talk about exceptional temporary authorisation for one occasion? COM never issues a temporary authorisation for someone who is not under renewal.

Commented [REDACTED]: Pls see our comment above on 2nd para of Article 26(a)4, which applies here as well: your addition doesn't respect the original scope of the proposal and interferes with the role of the Commission as being the only Union institution empowered to present legislative proposals. To be redrafted as obligations for the Union entities.

Commented [REDACTED]: Do we intend commercial couriers? How can we then ensure that they have been briefed on protection of EUCI?

[Article 26f

Access to classified meetings

~~14.1.~~ As regards the organisation of meetings where information classified CONFIDENTIEL UE/EU CONFIDENTIAL or higher is to be discussed, Union ~~institutions and bodies/entities~~ must ensure that ~~all participants are granted a security clearance or that their security authorisation clearance status of all participants~~ is known.

Commented [REDACTED]: Remain consistent and write «entities»

~~15.2.~~ On the basis of the records for access to EUCI, the competent Security Authority of the Union ~~institution or body/entity~~ concerned may issue a ~~personnel Security Clearance Certificate~~ to an individual where it is needed for attendance at meetings outside that Union ~~institution or body/entity~~. The ~~Personnel Security Clearance Certificate~~ must state the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or higher), the date of validity of relevant authorisation for access to EUCI and the date of expiry of the certificate itself. - *this Article is to be discussed later to determine in which part of the Regulation it should be included*

Commented [REDACTED]: Consistency: either with capitals or lower case

Commented [REDACTED]: Same as above

[Definitions

For the purposes of this Annex, the following definitions apply:

1) ~~'personnel Security Clearance'~~ or 'PSC' means a statement by a relevant authority of a Member State which is made following completion of a security investigation conducted by the competent authority and which certifies that an individual may be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or higher) and for a set period of time;

Commented [REDACTED]: Consistency: all capital letters or lower case

2) ~~'personnel Security Clearance Certificate'~~ means a certificate issued by a competent authority establishing that an individual holds a valid security clearance, or equivalent, or a security authorisation and that shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or higher), the period of validity of the relevant security clearance or authorisation and the date of expiry of the certificate itself. - *to be included in Article 3 Definitions*

Commented [REDACTED]: Same as above