Council of the European Union
General Secretariat

Brussels, 21 October 2022

WK 14299/2022 INIT

LIMITE

CSC
CSCI

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
N° Cion doc.:	7670/22
Subject:	Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union - comments by the Czech, Cyprus, Estonian, Greek and Netherlands delegations

Delegations will find in Annex comments by the Czech, Cyprus, Estonian, Greek and Netherlands delegations on the proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union.

ANNEX

Comments by the Czech, Cyprus, Estonian, Greek and Netherlands delegations on 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

1. CZ comments

General comments

We consider the draft regulation to be **unbalanced** regarding the two covered groups of information. **The rules** for the **protection of non-classified EU information (non-EUCI)** are set only in few articles (article 12 to 17), are **very general and incomplete**. As the framework proposed by the EC is general and vague, it is very difficult to foresee how the protection of non-EUCI will work in practice. **Many provisions are missing**, e.g. 1) concrete rules for the transmission of non-EUCI outside Union institutions and bodies, mainly to authorities in Member States, 2) impact on natural and/or legal person handling non-EUCI in line with article 13 and 14 of the draft regulation, 3) rules for the whole document management system of non-EUCI.

Without clearly specifying it, the **draft regulation will have an impact on Member States**. **Union institutions and bodies are sharing and exchanging information not only among themselves but also and more often with the authorities of the Member States**. As the draft regulation sets new rules for the protection and handling of non-EUCI, these rules will have to be implemented by the Member States and therefore, enough time will also be needed for such implementation in national legislation.

An example of cooperation and exchange of information between EU institution and national authorities is the European Central Bank (ECB). The salient feature of the ECB's mandate is that it does not perform its tasks in isolation, but in close cooperation with the relevant national bodies within the frameworks of the European System of Central Banks (ESCB) and of the Single Supervisory Mechanism (SSM). The ESCB and SSM represent highly integrated structures with a particular legal construction in which the national central banks, national supervisory authorities, and the ECB work in close cooperation. This fact implies that it is impossible to regulate handling of information within the ECB without causing major impact on the particular authorities of the Member States. **This specific structure does not seem to be taken into account. However, it should be reflected in further examination and revision of the text.**

Given these concrete examples of shortcomings, we consider as a possible way forward following steps:

1) **exclude the whole chapter 4 on non-EUCI from the draft regulation;**
2) **substantially clarify and complement the provisions on non-EUCI;**
3) **present a separate legislative proposal accompanied with a detailed impact assessment including the impact on Member States.**

These comments are only preliminary and without prejudice to possible future comments and suggestions.

2. CY comments

REPUBLIC OF CYPRUS
MINISTRY OF DEFENCE

NATIONAL SECURITY AUTHORITY

File No.: NSA/4.2.07.2

Nicosia, 14 October, 2022

To: Council Security Committee

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**

REF:
a. WK 7670/28 March 2022/European Commission
b. WK 7670 ADD 1 – 8/29 March 2022/European Commission
c. WK 4542/28 March 2022/Presidency
d. Document 9288/20 May 2022/European Data Protection Supervisor
e. Document 10091/13 June 2022/CSC
f. Document 10231/14 June 2022/Presidency
g. WK 8619/14 June 2022/GSC
h. WK 9492/05 July 2022/GSC
i. WK 12916/12 October 2022/GSC

With reference to the above mentioned subject and following the meeting of the Council Security Committee on the 26th and 27th September 2022, we hereby forward our comments regarding Articles 1 to 16 of the Proposal for the Regulation on information security in the institutions, bodies, offices and agencies of the Union.

2. After the initial discussion at the CSC, we feel necessary to reiterate the comments and the opinion of the CSC as stated in WK10091/2022. Additionally, we also state that entering into the discussion of this Regulation does not in any way imply our acceptance or approval. The total dismissal of this Regulation is still an option for us if we are not convinced that the new security framework is better than the one already at place.

./.

Ministry of Defence / National Security Authority,
172 – 174, Strovolos Avenue, 1432, Strovolos – Nicosia – Cyprus, P.C. 2048.
Tel: +35722807678, Fax: +35722302351, E-mail: cynsa@mod.gov.cy

3. Following the initial article to article discussion, we identified several issues and have the following comments:

a. The existence of non-classified information (NCI) and EUCI in the same document still remains a major drawback for this proposal and something that is expected to create significant administrative problems for both EUIBAs and Member States (MSs).

b. We still believe that the overall impact on MS will be much greater than the one anticipated by the Commission since EUCI and EU-NCI are handled within national structures but also because EUCI may be related to MSs' national security and interests. For this reason, we find that Article 298 of the TFEU may not fully support the scope of this Regulation and thus cannot minimize the impact on MSs.

c. The current definitions of "Normal" and "Sensitive Non-classified" will create confusion and thus need to be revisited and amended accordingly by the Commission. Moreover, the existence of the "Sensitive non-classified" category poses a potential threat to EUCI marked as "Restreint UE/EU Restricted". Paragraph 1 of Article 14 states:

*"1. Union institutions and bodies shall categorise, handle and stored as sensitive non-classified all information that is not classified but which they must protect due to legal obligations or because of the **harm** that may be caused to the legitimate private and public interests, including those of the Union institutions and bodies, Member States or individuals by its unauthorised disclosure."*

The definition of EUCI marked as "Confidentiel UE/EU Confidential" according to the CSR (Art. 2, Para 2c) is:

"(c)…information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States;".

Consequently, if "Sensitive Non-classified" information and "Confidentiel UE/EU Confidential" information have similar definitions causing harm to interests, then choosing between them becomes a challenge but also cancels the category that already exists between them, which is the "Restreint UE/EU Restricted" level.

d. Regarding the governance and organization of security as proposed by the Regulation, it becomes clear that decision taking will be a cumbersome task for the Coordination Group, the amendment of the Regulation itself after coming into force seems quite challenging and the way that this regulation will be imposed on EUIBAs is at least vague. Additionally, it is not clear to us how the new governance system will affect the previous, current and future work of the CSC and its sub-committees. For example, the CSC-IA through the CSC has published over the years a number of relevant guidelines and policies which derived from MSs' expertise. Supposing that the new sub-group on IA finds the necessary expertise and publishes new and different policies, how these new policies will affect the work of the CSC-IA? If the CSC-IA policies will be affected, then MSs will obviously be affected too.

./.

Ministry of Defence / National Security Authority,
172 – 174, Strovolos Avenue, 1432, Strovolos – Nicosia – Cyprus, P.C. 2048.
Tel: +35722807678, Fax: +35722302351, E-mail: cynsa@mod.gov.cy

e. The limited role of MSs within the whole proposed governance system finds us diametrically opposite since we believe that MSs' expertise is essential for ensuring the security of EUCI. EUCI is related to MSs' national security, so MSs' role and contribution should be substantial and meaningful within the Coordination Group.

4. We feel compelled to state here that for us the CSR, as the most mature EUCI security document, should continue to be the cornerstone for EUCI security. The CSR evolved through time in order to address contemporary threats and new adversaries and at this stage we could be more patient in order to complete the review of the CSR and then incorporate the new security elements within the proposed Regulation.

5. Since handling of NCI does not belong within the sphere of responsibilities of the Cyprus NSA, we have informed a number of internal stakeholders regarding the new Regulation and we are in anticipation of their input. We will forward their comments, if any, at a later stage.

6. We remain at your disposal for anything you may further need.

[redacted]

For the Director of the Cyprus National Security Authority

3. EE comments

VÄLISLUUREAMET
Estonian Foreign Intelligence Service

Estonian Foreign Intelligence Service
FOR OFFICIAL USE ONLY
Marking on 14.10.2022
Valid until 13.10.2027
Legal basis: Public Information Security Act § 35(1)(3)

General Secretariat Council of the European Union
Council of the European Union

EFIS reg 14.10.2022 No 16-6/22/63

Comments by the Estonian Council Security Committee Delegation to the Commission Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and the agencies of the Union (EUIBA)

Estonia supports the approach that the institutions, bodies, offices and agencies of the Union need common rules to protect information, including sensitive information. For that purpose, uniform rules must be set for all EUIBAs. We consider it necessary that common principles (minimum requirements) of information security for classified information are compulsory for EUIBAs to protect, process and trace information. It is reasonable to follow the principle of autonomy only after common security rules are followed.

Estonia does not support the situation where the European Commission instructs its Member States how one of the areas of their national security – protection of classified information - should be regulated. Furthermore, Estonia does not support the currently proposed wording which according to our assessment diminishes the decisive role of the Member States competent authorities in formulating the requirements for the protection of European Union Classified Information (EUCI). Therefore, we consider it necessary that the Security Committee of the Council of the European Union (EU CSC) maintains their leading role in formulating requirements for the protection of EU classified information, specifically through commonly agreed Council Security Rules.

According to Estonia's assessment, protection of classified information is part of national security, which, in accordance with the Treaty of the European Union remains the sole responsibility of each Member State. Based on the current Commission Proposal, EUIBA's must align their security rules with the planned regulation (Preamble Point 3, 27 Article 1, 4, 27). As the provision would apply to the security rules of the Council of the European Union, which Member States need to follow, there would be a situation where the Commission prescribes rules to Member States to organise one of the domains of their national security.

In our opinion the Proposal excludes Member States from the actual decision-making process, while EUCI is mostly comprised of the classified information of its Member States, and therefore the protection of such information must be agreed in a format which involves Member States and would not jeopardise the information forwarded by a Member State. For that purpose, the EU CSC has been the most important institution responsible for that area. However, in our understanding the governance model and the type of legislation suggested do not guarantee that; in our reading the protection of classified information should be organised by the Interinstitutional Information Security Coordination Group, while the Member States will have only secondary role.

Estonia does not support the establishment of new EU bodies (Interinstitutional Coordination Group, Information Protection Committee), prescribed by European Commission's draft Proposal. We believe

Rahumäe tee 4b, Tallinn 13415 Reg nr 70005938 Telefon (+372)693 5000 E-mail info@valisluureamet.ee

that the existing mechanisms for organising the protection of EU classified information are sufficient and must be used to the fullest and updated, if necessary.

Estonia considers it necessary to protect unclassified information in the same was as classified information – based on the same framework of definitions and basis. However, we do not support the concept of regulating unclassified and classified information in the same regulation.

The protection of classified information and the protection of unclassified information are different fields, with different protection measures and principles; as a rule, the topics are nationally regulated by different laws and the protection is provided and supervised by different state authorities with different competences.

More detailed input **on the protection of unclassified information**:

1. Estonia does not support the establishment of different protection categories for unclassified information, as that would make the differentiation between sensitive unclassified and classified information unclear.

We would like to keep the categorisation of unclassified documents as simple as possible. It remains unclear why the Commission Proposal considers it is necessary to establish three categories for sensitive unclassified information along with different protection measures: SENSITIVE, EU NORMAL and PUBLIC. The difference between the essence and protection of SENSITIVE and EU NORMAL remains unclear. Such differentiation and the attempt to establish protective measures may lead to the distinction between classified and unclassified information becoming blurred and makes European Union's public administration more closed. The confusion regarding the protection of sensitive unclassified information may foster overclassification, if the effect of protective measures is not convincing. On the other hand, adding the elements of classified information protection to the measures of sensitive unclassified information protection may lead to the situation where information that requires classification remains unclassified. Moreover, in practice, multi-level protection of unclassified information generates unnecessary bureaucracy and contradicts national legislation.

2. Estonia prefers that in the context of protecting unclassified information, except information intended for public use, a practice of validity deadline or conditions for the termination of limitations would be introduced. In addition, we would support the introduction of a clear declassification system, so that all document management system owners would be informed about the abolishment of access limitations through a certain central channel/system.

More detailed input **on the protection of classified information**:

1. We recommend to amend the regulation by adding the possibility to demand information, necessary for conducting security vetting/investigation on the applicant, including follow-up vetting/investigation, from the Member State competent authority where the applicant has lived for a longer period of time.

According to Article 23(2) of the draft regulation, security investigation of an individual is conducted by the competent authority of the Member State of which the applicant is a citizen. In the context of one of EU's fundamental principles – free movement of workers – there is an increasing number of individuals who have resided in another Member State for a long time. Therefore, the competent authority of the Member State that the individual is a citizen may not be able to determine the trustworthiness of the individual. Making queries to another Member State may not be effective and provide necessary guarantees. Effective vetting can only be conducted in a very close cooperation with the competent authority of all Member State, where the applicant has lived for an extended period.

In order to ensure reliable access to EUCI for individuals working in EUIBAs, Estonia proposes to amend the regulation with the possibility to demand additional information on the applicant from the competent authority of the Member State1 where the applicant has lived already for longer time period (e.g. more than 6 months). The procedures necessary for vetting would be conducted by the competent authority of the applicant's country of residence, which would forward the collected information to the competent authority of the applicant's origin.

2. We suggest to amend the wording of the Proposal, to add the possibility for Member State's Competent Authority to acquire information on citizens from third countries working at EUIBAs having access to EUCI.

Considering the worsening of current global security situation and the nature of threats, we are increasingly worried about the labour force at EUIBAs originating from outside of the European Union.

3. Estonia does not support the current wording suggesting that the European Commission could conduct security vetting and grant Personal Security Clearances for handling EUCI.

The Preamble Point 17 of the draft Proposal may leave the impression that according to the regulation, the Commission may conduct vetting and issue security clearances. Even though the text of the regulation does not support the above-mentioned interpretation, Estonia considers it necessary that the text of the Preamble be adjusted in a way that the explanation would correspond to the text as well as the actual aim of the regulation.

4. According to Estonia's assessment, supervision over the protection of classified information must be conducted in cooperation with the Competent Authorities of Member States for a comprehensive result, as the investigation should identify all factors. After the identification of specific individuals, the institution should inform the Competent Authorities of Member State, whose citizens have breached the rules of handling classified information.

We understand that according to Article 4 along with the more detailed rules on the breaches of security and compromise of EUCI in Article 22, the security inquiry is conducted by the internal security unit of the specific EUIBA (the so-called "security authority"). According to Estonia's assessment, the security inquiry referred to should aim to establish all facts and when identifying certain individual(s), the EUIBA should inform the competent authorities of Member States, whose citizen has breached the rules of handling classified information. We understand the inherent logic of EU structures, but according to our assessment, it is problematic that supervision on following the rules of handling classified information is conducted internally by the institution. As the employees of EUIBAs continue to be monitored by Competent Authorities of Member States, it is of high importance to inform them on the inquiry.

[1] There is some analogy to the European Commission's implementing Regulation 2019/103 concerning aviation security measures, in which the second sentence in Point 11.1.6 states: *"Member States shall endeavour to establish appropriate and effective mechanisms in order to ensure information sharing at national level and with other States for the purposes of elaboration and evaluation of information relevant to background check."*

4. EL comments

Hellenic Republic
NIS / Cyber Directorate
Information Assurance Security Authority (INFOSEC)
TEMPEST Authority
Crypto Approval Authority

Athens, 5 October 2022

To : **security.csc@consilium.europa.eu**

Subject: Comments on 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.

Reference: 7670/22/28-Mar-2022

Dear Colleagues,

Greece appreciates the work done by the staff on the referenced document and supports the following:

1. We propose the inclusion of rules for the protection of EUCI only, as we consider it more useful to include rules for the protection of EU unclassified information in a separate regulation. However, in the case of including rules for both EU classified and unclassified information, we propose that the levels of EU unclassified information are not more than two (2): PUBLIC USE and SENSITIVE NON-CLASSIFIED (*where PUBLIC USE includes all EU unclassified information that can be published or has already been published and SENSITIVE NON-CLASSIFIED includes all EU unclassified information than cannot be published*).

2. We propose that, instead of setting up new thematic sub-groups for the facilitation of the implementation of this Regulation (as referred on Article 7 paragraph 1), the Coordination Group should receive assistance from the already existing sub-groups of the Council Security Committee in this task.

We thank you for your cooperation.

NIS/Cyber Directorate
Information Assurance Security Authority (INFOSEC)
TEMPEST Authority
Crypto Approval Authority
Tel: +302106973150
e-mail: infosec@nis.gr

5. NL comments

NL NSA – Comments on the proposal for the EUIBA's Information Security Regulation (doc. 7670/22)
03-10-22

We would first like to emphasize that the NL NSA strongly supports the goal to establish a common set of rules on information security applicable to all EU institutions, agencies and bodies (UIBA's). The NL NSA attaches great importance to a high level of information security and considers the new regulation as a possible step towards increasing the overall level of information security in the EU. Our concerns mainly relate to the content of the draft regulation and the impact on the Member States. Below we state our main concerns:

1. The protection of EUCI is by definition a part of national security, which remains in the remit of Member States. Member States must therefore assume a leading role in this policy area, by remaining at the helm of information security in the Union. This entails the preponderance of the CSC as the sole decisive body where MS are represented in this field. At least there should be a direct link between the inter-institutional group and the CSC/NSA's.
2. In our opinion, the aim of the proposed regulation should be to create a strong and uniform set of rules information security in the UIBAs. This ambition is in part contradicted by the proposal not replacing and repealing current internal rules and regulations for UIBAs and not offering mechanisms to clarify which piece of legislation prevails in case of conflicts. On top of this, the proposed regulation allows UIBA's to maintain internal markings, which undermines the aim of harmonization.
3. The proposed regulation includes the introduction of the category 'non classified information'. The NL NSA believes that this has direct impact on the Member States. This is especially the case when information in this category is shared with Member States and companies and ministries in Member States are expected to respect the handling instructions accompanying the information. The NL NSA would like to request the Commission to provide more clarity on the implementation of the handling instructions for the category 'sensitive non-classified information' and the obligations for Member States. Furthermore, there is currently no legal framework for the protection of this category of information in Member States and there is no system for monitoring the compliance with the handling instructions. From a member state's perspective, the protection of information in this category cannot be guaranteed. Finally, we believe that the differences between the proposed category sensitive non classified and RESTREINT-UE/EU-RESTRICTED are too small. This may lead to the risk of overprotecting or under classification. The NL NSA is of the opinion that information that needs protection due to potential damage caused by unauthorized disclosure, should be classified as RESTREINT-UE/EU-RESTRICED.
4. Regarding the use of cryptographic products, the regulations refers in article 42 to a list of approved cryptographic products that shall be maintained by the Council, on the basis from input of NSA's. It should be noted that the NL NSA attaches great importance to the system of Second Party Evaluations (SPE's) and the position of the AQUA's. The NL NSA would like to see an explicit reference to the SPE's and AQUA's in this article.
5. Finally, the NL NSA would like to stress that lots of work has been put into the review of the Council Security Rules. After finalizing the review, the CSR will be the most advanced legal text on the protection of EUCI among EU institutions. Therefore the NL NSA believes that the reviewed version of the Council Security Rules must serve as a blueprint for the common Information Security Regulation.