Council of the European Union
General Secretariat

Interinstitutional files:
2022/0084 (COD)

Brussels, 26 June 2023

WK 7653/2023 INIT

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: To:	General Secretariat of the Council Security Committee
N° prev. doc.:	doc. 8453/23
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 - Comments on the governance structure by the Greek, Netherlands, Portuguese and Cypriot delegations

In the Annex, delegations will find comments on the governance structure by the Greek, Netherlands, Portuguese and Cypriot delegations.

ANNEX

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 (doc. 7670/2022) – Governance structure

Comments from the Greek, Netherlands, Portuguese and Cypriot delegations

1. Comments from the Greek delegation

The Delegation of the Hellenic Republic understands the need and supports the task of establishing unified rules for the handling of EUCI throughout EU institutions, bodies and agencies. Moreover, and under specific conditions, our side supports the regulation of the non-EUCI segment. However, the Hellenic Delegation has serious concerns regarding the proposed governance model, as described in document WK8453/ 23/ 27.04.2023.

Our side prefers to avoid repeating the concerns raised by the Member States (MS) during the last two CSC meetings, endorses the concerns expressed on the WK 5655/2023 of the German Delegation, furthermore, wants to present the following three issues, as seen from the Hellenic point of view:

- According to the WK 8453 /23/ 27.04.2023, the proposed Regulation "*...entrusts the governance to an Interinstitutional Information Security Coordination Group (IISCG)...*" (paragraph II, page 2), which will, actually, be the main governance body. The role of the MS is transferred to the Information Security Committee (ISC) that "*... shall provide advice to the IISCG...*" (draft article Annex II, 6a(new)(5)). However, the ISC's "advises"/suggestions are not binding for the IISCG, as reflected throughout the Articles 6 – 8. The Hellenic side does not agree neither to this wording nor to its content.

  The Hellenic Republic would agree to a more clearly substantive role for the Member States (MS) or even to a reversal of the roles as follows: entrust the governance of the Regulation to the ISC (where all MS will be represented, as well as the European Council, the European Commission, the EEAS with the addition of 2-3 bodies/agencies), while offering to the IISCG the advisory role.

- The presentation of ECB (WK 6280/2023 INIT) - one of the members of the proposed IISCG (Annex II, Article 6, 1(ab)) - revealed a different approach on the issue of Information Security with several security "shortcuts" and exceptions, pointing to established procedures and fiscal constraints. Although one might show understanding for

this approach for the specific sector, as a MS we are deeply concerned about the skills of several agencies for drafting EUCI security rules or even to give them the authority to draft rules that would be addressed to others (and more specifically to the MS) and only partially applied by the EU Institutions.

- In respect to the above-mentioned point, the Hellenic side is, also, concerned about the provision of Article 8 that "*Each Union Institution and body shall designate a Security Authority to assume responsibilities assigned by this regulation...*" (Annex II, Article 8(1)). Some of the Union Institutions and bodies will, also, have to establish additional Authorities, as described in Article 8(3).
  There is no clear concept concerning the way in which each Union institution and body will establish these Authorities, since it is a demanding task. Therefore, there is a risk that, finally, the majority of EU Institutions and bodies will assign these responsibilities only to a small number of Security Authorities (Article 8(4)), as not all of them will have neither the capacity nor the will to establish their own Authorities. This may lead to the overturning of the main argument behind the formation of the IISCG (which is to have more competent Authorities to decide on security rules in the EU that will automatically be imposed to MS).

As the Hellenic side does appreciate the effort of the GSC to draft a new text taking into account the MS concerns, we remain at your disposal for further cooperation.

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

2. Comments from the Netherlands delegation

The NL NSA would like to thank the GSC for its continuing effort to find a way forward with 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 (Articles 6-8). The NL NSA would also like to reiterate the previous comments regarding this proposal and emphasize the following:

The protection of EUCI is part of national security, which is the sole responsibility of the Member States. The proposed governance structure gives the Member States only an advisory function regarding the protection of EUCI. The NL NSA remains of the opinion that this not sufficient and does not reflect the exclusive competence of the Member States in this area. The Member States should have both supervisory and executive roles when it comes to the protection of EUCI.

Since the publication of the proposal, significant time and effort has been invested in discussing and examining alternative governance structures. The NL NSA is of the opinion that so far, not a satisfactory solution has been found and has its doubts whether it will be found if the legal basis and the scope of the proposal remain the same. Therefore, the NL NSA would like to ask the GSC and the Council Legal Service to examine if it would be legally conceivable to change the scope of the proposed regulation and only include agencies in the governance model.

3. Comments from the Portuguese delegation

PT Comments to ST 8453/23 - 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 - Discussion paper on the main issues regarding governance

Generic comments:

Although PT recognizes and welcomes the amount of effort put into this proposal by the GSC, it is our believe that this text still needs refinement, considering the requirement for a governance model that keeps the roles and responsibilities of the MS and the Council at the appropriate level.

Also, a clear separation between EUCI and non EUCI it is not visible in this governance model proposal, though such purpose must be properly highlighted in the objective and scope of the regulation. Thus, further discussion and development of this proposal is highly suggested.

Specific comments:

Annex I – Main Issues

A. The Interinstitutional Information Security Coordination Group (IISCG)

II.A.7. In this regard, the Council should be given additional prerogatives, given its competences, the specificities of its work and functioning, not only in political terms but also in particular for instance in the area of protection of EUCI.

PT considers those prerogatives also need to be defined, and identified/stated, in the text.

II.A.8. As a Union's institution within the meaning of Article 13(1) TEU, the European Council should be given a seat in the IISCG.

Even considering decisions will be taken by consensus, it seems that, unless some compromise solution is found to balance this, the Council will be represented with only one (direct) vote among 17, and, while representing the 27 MS, will be standing at the same level as every other IBA, regarding matters (EUCI), where it needs to have (and always had) a leading role.

II.A.9. to limit the participation to the IISCG to a specific list which would include all the institutions and a limited number of a few relevant bodies and agencies. All other agencies would be represented by representatives of the Union Agencies Network (EUAN) and may be invited on a case-by-case basis;

PT considers that, this limitation, still doesn´t address the issue expressed above. It is though, another opportunity to reinforce the idea, regarding the relevance that each IBA should have in the IISCG.

B. The Information Security Committee (ISC)

II.B.10. it is mandatory for the IISCG [and thematic subgroups] to consult the ISC on any guidance document the implementation of which could have an impact on the Member States or require their contribution.

The ISC will basically replicate (duplicate) the current organization for the CSC and, unless the role and relevance are changed (reinforced), it will have no practical impact in the (decision)

process. Mandatory consultation does not avoid the fact that contributions may not be taken in consideration.

Such amendments would also make it easier for the CSC to articulate its works with those of the ISC.

Regarding this, PT truly believes the maintenance of the current "Battle Rhythm" will no longer be possible, or useful, to sustain two Committees.

C. The thematic subgroups

II.C.12.... Another possibility would be to maintain a single IISCG, but to entrust all questions regarding NCI, including those on the information assurance of CIS handling NCI, to a single new subgroup on NCI.

Considered a preferable possibility if (and only) a clear separation for the two areas is achieved in the text (not limited to governance, as already mentioned).

Rationale: Regardless the fact of not being EUCI related, a dedicated IISCG will represent a heavy resource burden to all entities involved.

Annex II – Text - Articles 6th, 7th and 8th

Article 6a.5.(new) - The Information Security Committee shall have an advisory role. The Information Security Committee shall be consulted by the Coordination Group [and thematic subgroups] and shall provide advice on any envisaged guidance the implementation of which could have an impact for Member States or require their contribution.

As already mentioned, the awarded consultation and advice roles for the ISC, even considering a shall clause, without any level of a binding nature, means that, MS and Council positions, not only risk to be underrepresented, but also not even be considered for representation.

Article 7. 1. Thematic sub-groups

Unless some need to change is already identified (and envisaged in the CSR review), PT suggests, for practical reasons, to keep current set up, adding a specific sub-group for NCI.

4. Comments from the Cypriot delegation

With reference to the above mentioned subject and following the meeting of the Council Security Committee on the 3rd and 4th May 2023, we hereby forward our comments regarding Articles 6, 7 and 8 of the Proposal for the Regulation on information security in the institutions, bodies, offices and agencies of the Union, as they are presented in WK 8453/2023.

2. After the discussions at the CSC, it is again necessary to reiterate all our previously expressed concerns regarding the proposed regulation and additionally state that we are in accord with the comments of the German Delegation, as presented in WK 5655/2023.

3. Echoing these comments and taking into account the definition of EUCI, we would also prefer a clearer, decisive and more active role for Member States in the proposed regulation. Unfortunately, with the current governance system and the limited role of the Information Security Committee we foresee that Member States will eventually lose interest in sharing their security expertise at the expense of the security provided to EUCI.

4. Additionally, we remain sceptical about the capacity of some of the proposed EU institutions and bodies, as listed in Paragraph 1ab of Article 6, in terms of providing relevant expertise for drafting security rules at the Coordination Group and thematic sub-groups levels. We estimate that such tasks fall outside their institutional knowledge and core competences something that became obvious to us after the European Central Bank's presentation (WK 6280/2023). This particular presentation by the ECB also gave us the impression that possibly, some institutions and bodies may be willing to cut corners in security matters in order to make their everyday routine easier.

5. The abovementioned current lack of capacity is recognized by the proposed regulation and for this reason Article 8 defines that each Union institution and body shall designate a Security Authority (Paragraph 1) to assume the responsibilities assigned by the regulation and adequately develop a number of relevant functions (Paragraph 3). Firstly, we find the creation of such security authorities with the necessary competences/functions and the capacity to draft legal security texts at least as a very demanding endeavour, given the overall expertise needed in terms of human resources. We note here that even some Member States, including Cyprus, still strive and find some of these functions to be quite challenging to achieve at the level of advanced Member States. Secondly, having in mind that our approach towards the security of EUCI requires centralized control through the NSA, we have serious concerns as regards to the practical issues of aligning the opinions of all these security authorities in a committee like the Coordination Group.

6. The abovementioned lack of capacity of the Union's institutions and bodies and the anticipated practical issues will inevitably have a toll on the work of the Coordination Group. We emphasize here that the works of committees like the CSC, ComSeG and EEAS-SC has led to the development of an institutional memory that cannot just be transferred to the Coordination Group, as if by magic.

7. Moreover, we are compelled to express our disagreement with Paragraph 4 of Article 8 since we do not believe that delegation of security matters is a step towards increased security for EUCI, at least in the way described in this Paragraph. This delegation of security functions could lead also into the delegation of responsibility, reducing thus the security provided to EUCI and the accountability of the Union's institutions and bodies. In our opinion, most Union's institutions and bodies should have a security office which will have the ability to apply the relevant security procedures, provide internal advice related to the security of EUCI and liaise with a competent authority/entity on more technical and complicated matters. However, the responsibility of drafting, overviewing and monitoring security procedures, practices, policies and guidelines should be given to one competent authority/entity outside EU institutions and bodies in a similar governance model to that employed by most Member States, which have NSAs for this purpose. These security offices could participate, if they decide, alongside with Member States in the decision making process of this competent authority/entity. This is a similar model to that applied at the CSC where the Council and Member States participate.

8. Despite all the above-mentioned negative points, we acknowledge and appreciate the hard work and effort of the GSC staff towards the creation of a meaningful security regulation.