Council of the European Union
General Secretariat

PUBLIC

Brussels, 19 April 2024

WK 5694/2024 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.: N° Cion doc.:	5630/24, 7334/24 7670/22
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 non-classified information by the Dutch delegation

In the Annex, delegations will find comments by the Dutch delegation on non-classified information concerning 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.

ANNEX

PUBLIC

NL Proposal for the Regulation of the European Parliament and of the Council on information security in the institutions, bodies, agencies of the Union

Date: 19/04/24

Dear colleagues,

We would first like to thank all member states and the GSC for the continuous efforts on the Information Security Regulation. As the NL-NSA attaches great importance to a high level of Information Security within the whole Union, we support the goal to establish a common level of Information Security. However, we propose not to overcomplicate rules and want to achieve as much harmonisation of rules and regulations as possible.

To foster the discussion in the Council Security Committee (CSC), we propose the below outlined changes in documents ST 5630/24 and ST 7334/24.

In line with the previous proposal from the Swedish delegation and the joint comments from the Austrian, Danish and Estonian delegations in December'23 (both WK 15904/23), the Dutch NSA supports the two categories on unclassified information and the limitation on the amount of underlying additions of these unclassified forms of information. The latest proposal from the GSC (ST 5630/24) to work with 'public' and 'internal non-classified' is for us a step in the right direction. Moreover, we are reluctant on the amount and gravity of the protection measures as they should not be stricter or equal to the rules on classified information. If further protection of information is necessary information should be classified. Based on the previous proposals by the GSC, the Dutch NSA proposes the following changes.

ST 5630/24:

Art 13: Internal non-classified information

1. Information intended for use by a Union entity in the execution of its functions which is neither public nor classified is internal non-classified information.~~-~~Such information is covered by the obligation of professional secrecy. **Internal non-classified information shall only be used for official purposes and only individuals and entities that require it may have access to it.**

2. Internal non-classified information may be marked visually or in metadata where necessary to enable its protection~~,~~**.** ~~particularly where shared exchanged outside Union entities institutions and bodies. The marking 'EU INTERNAL NON-CLASSIFIED shall be used in that case.~~

3. Union entities shall define standard protective measures for internal non-classified information.~~, taking into account guidance from the sub-group on non-classified information and any specific risks related to their tasks and activities.~~

4. **When created documents shall be marked as 'EU INTERNAL NON-CLASSIFIED'.**

5. **Internal non-classified information may be exchanged outside Union entities only with natural or legal persons having a need-to-know.**

~~5. In cases where internal non-classified information requires specific access restrictions, due to legal obligations or after a risk assessment made by its originator, Union entities shall use additional distribution markings indicating the set of recipients or the sensitive nature of the information. In such cases the marking "SENSITIVE" may also be added.~~ **~~(moved to ST 7334/24. We propose to handle any further specific access restrictions as measures, not as definition).~~**

~~6. Union entities shall notify the sub-group on non-classified information of the additional markings they use, and where possible, take into account any related guidance of this sub-group.~~ **~~(We propose not to use any additional markings than we define in the articles about protective measures (ST 7334/24) to achieve a common level).~~**

<u>ST 7334/24:</u>

<u>Art [X]: Protective measures for handling internal non-classified information</u>

1. **Protective measures for handling internal non-classified information shall not be equal or stricter than the rules for protecting classified information. When internal non-classified information need further protection it shall be classified.**
2. Internal non-classified information shall only be accessible to recipients with a need-to-know. ~~Where additional distribution markings are used, permission shall be requested from the originating Union to extend the distribution of a document beyond its initial recipients.~~
3. **Union entities shall provide a regular training and awareness program to their staff members and contractors, covering security threats to information, the obligation of professional secrecy, and any related guidance or instruction on the protection of internal non-classified information, including in CISs and outside their premises.**
4. **The marking internal non-classified and any administrative or dissemination limitations markings as defined in paragraph 5 and 6, determines handling and protection requirements to restrict access. All marking are applied by the originator and may only be modified by the originator.**
5. **Administrative markings may only be applied to the documents by the originator, where appropriate, to identify the type of information contained therein and to indicate the need for limited access.**
6. **Dissemination limitation markings may be used which restrict access to a named group. When dissemination markings are used information shall not be shared**

outside the named group(s) without consent of the originator. Dissemination limitation markings are:

i. **Releasable to ("NAME OF GROUP") ONLY**

<u>Art 11: requirements for communication and information systems handling and storing non-classified information</u>

4. **Union entities shall manage human aspects of the CIS, raise user awareness, train operational teams, have an full knowledge of the information system and its users, manage control nomadism and ensure identification and authentication at a need to know basis to provide access control.**
5. **Union entities shall secure technical aspects of the CIS : establish uniform security, including partitioning scheme for all IT equipment, network and administration, keep the information system up to date and provide supervision, audit and reaction.**

0. **Contractual Safeguards shall be designed to guarantee at least an equivalent level of protection to that provided by this Regulation, and shall include confidentiality and non-disclosure undertakings to be signed by all relevant service providers involved in the provision of the outsourced systems. Non-classified information shall be stored and processed in the Union.**

PUBLIC