DECISION OF THE COLLEGE OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE OF 24 FEBRUARY 2021

ADOPTING THE INTERNAL RULES OF THE EUROPEAN PUBLIC PROSECUTORS' OFFICE ON THE PROTECTION OF SENSITIVE NON-CLASSIFIED INFORMATION

The College of the European Public Prosecutor's Office (EPPO),

Having regard the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), hereinafter referred to as the "EPPO Regulation", and in particular Article 111(1) thereof,

Having regard the Article 108 of the "EPPO Regulation", and in particular paragraphs (4) and (5) thereof,

Aware of the sensitivity of especially operational information, even in the absence of a formal classification in line with the respective framework dealing with the protection of classified information,

Aware of the necessity to protect information of the EPPO efficiently and effectively,

Has adopted the following decision:

Article 1

Internal Rules of the European Public Prosecutors' Office on the protection of sensitive non-classified information

The *Internal Rules of the European Public Prosecutors' Office on the protection of sensitive non-classified information* in Annex to this Decision are adopted and shall be fully applicable and binding as of the entry into force of this Decision.

Article 2

Entry into force

This decision shall enter into force on the date of its adoption by the College.

Done at Luxembourg on 24 February 2021.

On behalf of the College,

Laura Codruța KÖVESI
European Chief Prosecutor

EUROPEAN PUBLIC PROSECUTORS OFFICE

ANNEX: Internal Rules of the European Public Prosecutors' Office on the protection of sensitive non-classified information

1. INTRODUCTION

1.1. Key elements

By definition, the work of the EPPO, being law enforcement and judicial in nature, is sensitive. The obligation to adopt internal rules on the protection of sensitive non-classified (SNC) information is provided by Art 111(1) of the EPPO Regulation.

EPPO staff must mark all documents containing sensitive information as EPPO Sensitive, in line with this decision.

The purpose of marking information is to ensure and allow the ability to ensure a sufficient level of confidentiality for the information. Markings are based on the fundamental security principles of need-to-know. A marking consists of a security marking plus, if applicable, any distribution markings, as described in this decision. Information must be protected adequately in information systems, where possible by using encryption.

1.2. Categorization and definitions

1.2.1. Marking: SENSITIVE

Any information which is not suitable for public release, and in addition could cause damage to the EPPO, to investigations, individuals, etc.

Formal classification as EUCI should be considered where the above is not sufficient.

1.3. Inter-institutional markings

When exchanging non-classified documents with other EU institutions, their internal markings may be used to ensure the proper handling of the documents by the recipients. In particular, the 'Limité/Limited' marking of the Council may be used which restricts distribution to the EU institutions, EU member states and EEA states. Documents bearing this marking should be marked as **SENSITIVE** inside the EPPO.

2. APPLICATION OF MARKINGS

2.1. Markings in documents

The main security marking (**SENSITIVE**) must be in font size 14, bold, and in capital letters.

In text documents (e.g. Word documents), whether in paper or digital form, the markings must be indicated on the top right side of the front page of the document, under the reference number of the document where applicable (see the example below and the sample

documents in sections 5 and 6 below). In other types of documents (e.g. Excel or PowerPoint documents), the marking must be positioned in a similar position on the first printed page.

SENSITIVE

UNTIL 31/12/2018

In the above example, the main security marking is **SENSITIVE**. If a deadline has been added, as per the example, after the deadline, the marking is no longer applicable.

The main security marking may also be included in the header of a document on each subsequent page. In this case, it must be included in normal text at the standard font size of the header, on the right side of the header (see Section 5). The use of watermarks or headers such as CONFIDENTIAL' or 'RESTRICTED' or any other indication of confidentiality is prohibited.

Draft documents can be marked, and a watermark may indicate that the document is a draft (this is not a security marking).

2.2. Markings in communication and information systems (CISs)

2.2.1. Email

Users should mark emails containing SNC information. The subject line should not contain SNC information. The first line of the email, before any salutation or other text, should include all markings and other instructions, on one line and separated by dashes. The main security markings should be in bold and not smaller than the main text, as in the example below (see also the sample email in Section 6):

> **SENSITIVE**
>
> Dear colleague,
>
> I enclose the list of candidates for the post of … [etc.]
>
> …

In accordance with the handling instructions in Section 3 below, all emails marked as SENSITIVE must be signed and encrypted using SECEM[1] or equivalent encryption products.

In line with the established practices, such encrypted emails should be handled as **SENSITIVE**, even when not marked.

2.2.2. Web-based CISs

It is recommended that CISs implemented with web interfaces display the appropriate marking on all screens that may contain SNC information. As an example, the marking should appear towards the top right of the screen, and should include a link to the relevant handling instructions.

[1] SECEM (SECure EMail) is the function in Outlook that enables users to encrypt and sign emails, based on the S/MIME standard.

All printouts containing SNC information must bear the appropriate markings.

2.2.3. Document handling systems

Document handling systems must clearly indicate any security markings applied to the document before it is opened, as well as in the document itself as described in Sections 2.1 and 2.2 above. See Section 4.1 below for instructions on document metadata.

Further information on the implementation of security markings in individual systems must be provided by the system owner. The EPPO Security Officer can provide advice on this subject upon request.

The principles of need-to-know and the handling instructions for security markings must be implemented in the rules defined in the CIS's access control policy and automated as far as possible in the CIS.

2.2.4. Other CISs

When all of the information in a CIS is SNC, the recommended approach for CISs that handle SNC is to present a warning screen to the user when entering the system. This may be shown on the authentication screen or as a separate message after authentication.

The warning screen should clearly show all markings (the main security marking and any distribution markings). The warning screen should show the handling instructions that relate to the system or output from the system (e.g. printouts), or include a link to those instructions. A link to the acceptable use policy of the system may also be included.

When the CIS contains both SNC and non-sensitive information, any SNC information should be clearly marked on screen before the user can access the contents.

All printouts containing SNC information must bear the appropriate markings.

3. HANDLING INSTRUCTIONS

3.1. SENSITIVE

The standard handling instructions apply to all documents bearing the marking **SENSITIVE**.

Creation

Creation covers any restrictions on the drafting of a document or the creation of information. Generally, there are no restrictions on the creation of documents at the SNC level, although the use of CISs containing functions for automatically adding markings in the correct formats is recommended.

The author of a document must select the appropriate distribution marking, based on the subject matter and the level of damage that may be caused by unauthorised disclosure.

Handling

Handling includes the instructions for reading, editing, copying, scanning, printing and storing documents.

Recipients may further distribute the information on a need-to-know basis, in full compliance with the respective provisions of the EPPO Regulation as regards the sharing of information, and bearing in mind the principle of professional confidentiality and the obligations under the Staff Regulations (Article 17). However, recipients must be aware that the document must not be released without permission from the originator, if applicable, and depending on any restrictions on their use

Care should be taken not to leave documents unattended on office desks. Where possible, documents should be stored in a locked office or a locked cupboard when not in use.

Documents should not be read or edited in public places where there is a risk of them being read by unauthorised people.

Electronic copies should be stored on platforms that can only be accessed by the target audience. The use of encryption and digital signatures is recommended, taking into account the risks and other countermeasures in place.

Scanned copies of documents, including both electronic and hard copies, should be removed from any insufficiently secured locations as soon as possible, including shared drives, unencrypted emails, scanner device memory and printers in unsecured office areas.

Documents should be removed from printers, photocopiers, faxes or other shared devices immediately. Care should be taken to limit the number of copies to the minimum necessary.

Distribution

Distribution covers the definition of the authorised recipients, methods of transmitting the information to those recipients (including carriage and electronic transmission) and the rules to be followed by the recipients, with particular regard to the further distribution by recipients. Distribution also includes any restrictions on translation.

Distribution is on a need-to-know basis, and the information is not to be distributed outside of the audience indicated.

All recipients should be aware of the applicable handling instructions.

Any person receiving SNC information who is not the intended recipient must inform the sender, where possible, and destroy the information by appropriate secure procedures (see under 'Destruction' below).

Where internal mail is used, the information must be closed[2] inside an opaque envelope.

Where email is used to transmit information marked as SENSITIVE, the use of the SECEM application (or similar) is mandatory, i.e. the emails must be signed and encrypted.

Downgrading

When a document no longer needs to be marked, the markings and handling instructions should be removed or struck out. Only the originator may downgrade a document.

[2] In this context, 'closed' indicates that an envelope has been closed in a way that makes it evident that the contents may have been accessed, whether deliberately or accidentally. This includes gluing or stapling the flap of the envelope closed; it does not require the use of a specific seal or stamp.

Destruction

Paper documents must be shredded using at least a standard level 3 shredder (straight cut 1.9 or cross cut 4 x 80 mm, max 320 mm2). Shredded documents may be disposed of in the normal office waste.

Documents stored on electronic media must be purged[3]. If the media is not to be reused, they must be disposed of in a manner to be approved by the responsible EPPO Security Officer.

4. OTHER ISSUES

4.1. Markings in document metadata

Document handling systems often record metadata about the documents, which contain information such as the title, author, creation date, etc. of the document. Where a system records metadata, this must also include the security markings to enable the system to display the markings to users and to transfer documents to other systems and ensure consistent handling.

Each document should include a property named 'Security marking' which will contain the marking 'SENSITIVE'.

4.2. Translation

When documents bearing a security marking need to be translated, the workflow and any associated systems must take account of the markings. In particular:

- The principles of need-to-know must be applied;
- Translators must be aware of and follow the handling instructions;
- Marked documents must be encrypted when transmitted electronically;
- Marked documents and translations must be securely deleted[4] from non-EPPO systems when the translation has been completed.

[3] The method of purging depends on the type of medium as follows:
- Magnetic tapes — degaussing;
- Magnetic disks — degaussing or overwriting with approved software;
- Flash memory (USB keys, SD cards, SSD drives, etc.) — overwriting with approved software;
- Non-rewriteable media (optical disks, non-volatile solid state devices, smart cards …) — physical destruction.

[4] Secure deletion ensures that the contents of a file are overwritten in the storage media (hard disk, etc.), leaving no traces of the file.

4.3. Use of markings with external partners

In certain circumstances it might be necessary to exchange information with one or more third parties outside the EPPO.

As a marking is only legally enforceable within the EPPO, a memorandum of understanding, contract or security convention should be drawn up between the EPPO and the external party, setting out the handling instructions for all information exchanged between them. This is done on the basis of trust, and each entity is responsible for the compliance by its own staff handling the information exchanged.

The appropriate handling instructions must be included with any document bearing a marking that is shared with third parties.

The EPPO Security Officer can provide assistance on this topic upon request.

5. Sample marked note

EUROPEAN PUBLIC PROSECUTOR'S OFFICE

Luxembourg, xx Month 2020
EPPO/*XX/2020/0XX*

SENSITIVE

Note on the Security Procedures of the EPPO

Subject: Example markings

This note includes an example of marking.

Administrative Director

EPPO, L-1499 Luxembourg

SENSITIVE

Table of Contents

6. Sample e-mail