EUROPEAN PUBLIC PROSECUTOR'S OFFICE

DECISION OF THE COLLEGE OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE OF 7 FEBRUARY 2024

ON SECURITY RULES APPLICABLE TO THE DIGITAL COMMUNICATION AND INFORMATION SYSTEMS OF THE EUROPEAN PUBLIC PROSECUTOR'S OFFICE ('EPPO')

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

Having regard to Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('EPPO') (hereinafter referred to as 'the EPPO Regulation')[1], and in particular Article 73 thereof,

Having regard to College Decision 011/2021 adopting the Security Rules of the EPPO for the Protection of EU Classified Information as amended by College Decision 101/2021 (hereinafter referred to as 'College Decision 011/2021'),

Having regard to College Decision 012/2021 adopting the Security Rules of the EPPO for the Protection of Sensitive Non-Classified Information (hereinafter referred to as 'College Decision 012/2021'),

Having regard to international standards and IT security good practices including ISO/IEC series 27000 and 31000,

Having regard to College Decision 009/2020 of 28 October 2020 on the Rules Concerning the Processing of Personal Data by EPPO (hereinafter referred to as 'College Decision 009/2020'),

Considering the EPPO Policy on Reporting Security Incidents[2],

Whereas:

(1) The EPPO's Digital Communication and Information Systems (hereinafter referred to as 'EPPO CIS') are an integral part of the functioning of the EPPO and security incidents can have a serious impact on the EPPO's operations as well as on third parties, including individuals whose data is stored in its CIS.

[1] OJ L 283 31.10.2017, p. 1.
[2] EPPO/2022/AD/067.

(2) There are many threats that can harm the confidentiality, integrity and availability of EPPO CIS, and the information processed therein. These may include accidents, errors, deliberate attacks and they need to be recognised as risks.

(3) In line with international standards ISO/IEC 31000 on risk management and ISO/IEC 27000 on information technology, EPPO CIS should be provided with a level of protection commensurate with the risk to which they are exposed.

(4) In line with Article 73 of the EPPO regulation, EPPO shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the processing of personal data.

(5) The digital security processes in EPPO should be implemented in a manner which is consistent with other policies, including on handling EU classified information as defined in College Decision 011/2021 and Sensitive Non-Classified information as defined in College Decision 012/2021. All CIS handling EU classified information and Sensitive Non-Classified information shall be aligned with these College Decisions.

Has adopted the following decision:

Article 1

Subject matter and scope

This Decision sets out the main principles, organisation and responsibilities regarding the security of all Communication and Information Systems which are owned, procured, managed or operated by or on behalf of EPPO.

Article 2

Definitions

For the purpose of this Decision the following definitions apply:

(1) Digital Communication and Information System (CIS) – means any system enabling the handling of information in electronic form, including all assets required for its operation, as well as infrastructure, organisation, personnel and information resources. This includes business applications, shared IT services, outsourced systems and end-user devices.

(2) Digital security* or *security of CIS – means the preservation of confidentiality, integrity and availability of CIS and the data that it processes

(3) IT asset – means a piece of software or hardware within an information system

(4) Residual risk – means the risk remaining after risk treatment

(5) Risk treatment – means the process of mitigating risk, which may include risk avoidance, risk reduction, removing the source of the risk, changing the likelihood of risk, changing the consequence of the risk, sharing the risk, and retaining the risk

(6) CIS Technical Manager – is the function responsible for the technical development, implementation, modification, operation and technical maintenance of a CIS

(7) ***Business Owner*** – is the function responsible for the overall scope of, use of and data processed in a CIS

(8) ***User*** – means an individual who uses functionalities provided by an EPPO CIS.

Article 3

Principles for security of CIS in the EPPO

1. The security of CIS in EPPO shall be based on the principles of legality, transparency, proportionality and accountability.
2. For an effective security of CIS, the following aspects shall be implemented:
    a. Authenticity: the guarantee that information is genuine and from *bona fide* sources;
    b. Availability: the property of being accessible and usable upon request by authorised entities;
    c. Confidentiality: the property that information is not disclosed to unauthorised individuals, entities or processes;
    d. Integrity: the property of safeguarding the accuracy and completeness of assets and information;
    e. Non-repudiation: the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied;
    f. Protection of personal data: the provision or appropriate safeguards in regards to personal data in full compliance with Regulation (EU) 2018/1725, as regards administrative personal data, and the EPPO Regulation, as regards operational personal data;
    g. Professional secrecy: the protection of information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components as laid down in the Staff Regulation and in Article 108 of the EPPO Regulation.

Article 4

Risk management process

1. For each CIS, a security risk assessment process shall be carried out. This process shall aim at determining the security risks, their risk level and defining security measures to mitigate such risks or reduce them to an acceptable level. The risks and security measures shall be documented in a security plan for each CIS.
2. All CIS shall be identified and shall have a Business Owner and a CIS Technical Manager assigned and recorded in an inventory.
3. The CIS security plan and digital security measures shall be proportionate to the security needs of the CIS and aligned with the legal requirements applicable to the data handled within.

4. As part of the risk management process at least the following actions shall be implemented for each CIS:

    a. The Business Owner shall identify and document the context and scope of the CIS, the CIS functional and legal requirements, including the ones related to the security of the data processed within. This shall include, where applicable, the level of classification of information handled by the CIS[3].

    b. The CIS Technical Manager shall prepare and document the CIS design, including assets, infrastructure, hardware and software, technical processes and interdependencies with other CIS. In the development of the design they shall consult the EPPO's structure in charge of security (hereinafter referred to as 'Security Unit'). If the CIS handles personal data, the CIS Technical Manager shall consult the Data Protection Officer.

    c. The Security Unit, with the support of the relevant stakeholders, in particular the CIS Technical Manager and Data Protection Officer, shall carry-out a business impact assessment and a risk assessment on the required levels of confidentiality, integrity and availability of the CIS and prepare a security plan and a business continuity and disaster recovery plan. The risk management process shall include at least the following:

        i. Security needs

        ii. Security measures and selection rationale (e.g. security controls and related threat scenarios)

        iii. Residual risk

        iv. Risk acceptance criteria and exceptions

        For CIS handling personal data that require a Data Protection Impact Assessment, the risk management process shall support the Data Protection Impact Assessment related process.

    d. The CIS Technical Manager, the Business Owner, the Security Unit and the Data Protection Officer shall cooperate on the design and implementation of the identified security measures part of the security plan and business continuity and disaster recovery plan to facilitate compliance and manage the risks.

    e. All risks that are mitigated shall be validated by the Security Unit or Data Protection Officer according to their source. Risks that are not fully mitigated shall be documented in a residual risk report.

    f. Before deployment of CIS, the Business Owner shall adopt the security implementation report, CIS business continuity plan and disaster recovery plan and residual risks report.

    g. The CIS Technical Manager, the Data Protection Officer, and the Security Unit shall monitor any changes to the security risks and inform the Business

[3] The College Decision 011/2021 and College Decision 012/2021 may be used to assess if the information is part of any of the following categories: EU classified information or Sensitive non-classified information, respectively.

Owner. In case of substantial changes in the security risks (e.g. changes to the CIS design raising new security risks, suspension of mitigation measures), a new risk assessment shall be carried out in line with this Article.

Article 5

Secure IT operations

1. Secure IT operations management shall comprise planning and sustaining day-to-day processes for maintaining the security of EPPO CIS environments.
2. As part of the secure IT operations management process at least the following actions shall be implemented:
    a. The Business Owner shall confirm the priorities for managing secure operations of the CIS, in line with the results of the risk management process and available resources.
    b. The CIS Technical Manager shall implement the operational security measures identified through the risk management process and included in the security plan and business continuity and disaster recovery plan. In particular, the CIS Technical Manager shall:
        i. Perform system monitoring and logging, including security logs and alerts,
        ii. Perform and test back-ups according with the agreed schedule,
        iii. Carry-out vulnerability and patch management, including interdependencies with risks related to other CIS,
        iv. Ensure IT assets registration in the relevant inventory,
        v. Maintain a register of user access rights (including approvals), enforcing and monitoring access control mechanisms, and review access periodically (in particular privileged access) in line with the access control policy.
    c. The Security Unit shall provide guidance on the implementation of the security measures.

Article 6

Secure development and acquisition

1. Security and data protection shall be considered in the development or acquisition of all CIS. In this context, the principle of *security by design* and *data protection by design* shall be part of every phase of the CIS development lifecycle, including system conception, design and development, testing, deployment, and ongoing maintenance.
2. When a CIS is acquired from a third party (e.g. Commercial off-the-shelf product), the security and data protection of the CIS shall be assessed against the security and legal requirements of the data handled within.

Article 7

Security incident management

Security incidents impacting EPPO CIS shall be managed in line with the EPPO Policy on Reporting Incidents and relevant procedures governing personal data breaches.

Article 8

IT Asset management

The EPPO shall define an IT asset management process. This process shall be approved by the Administrative Director and it shall include the roles and responsibilities related to the process, security needs for different types of assets as well as security requirements for the different stages of asset management (e.g. acquisition, registration, configuration, allocation, maintenance, storage, transfer, and disposal).

Article 9

Digital security governance

1. The governance of EPPO CIS security includes the establishing and maintaining of a security framework based on EPPO's strategic objectives and risk appetite. The security framework for EPPO CIS shall be aligned with the legal requirements applicable to EPPO and its CIS, shall consider the best practices of ISO/IEC 27000 standards and other relevant international standards. In this context the EPPO shall use the Plan-Do-Check-Act methodology for the set-up and continuous review of its digital security framework.
2. In regards to the digital security governance, the following activities shall be implemented:
    a. The Security Unit shall prepare a Security Strategy including at least the long term objectives in terms of security of CIS and activities to be performed in the years ahead. These activities shall be aligned with the EPPO mandate and priorities, the strategy on the management of EPPO digital services, audits and incidents results and available resources
    b. The provisions of this Decision shall, where necessary, be further detailed in implementing rules, policies, standards, procedures, guidelines or best practices. These implementing rules, policies, standards, procedures, guidelines or best practices shall be based on industry best practices, in particular ISO/IEC 27001 Annex A covering the following security aspects:
        (1) Organisation of information security
        (2) Human resources security
        (3) Asset management
        (4) Access control
        (5) Cryptography

(6) Physical and environment security
(7) Operational security
(8) Communication security
(9) System acquisitions, development and maintenance
(10) Supplier security
(11) Information security incident management
(12) Information security aspects of business continuity
(13) Compliance.

Article 10

Roles and responsibilities

1. The Administrative Director shall be the Security Authority for all EPPO CIS. In this role he/she shall hold ultimate accountability for the CIS security, including the overall responsibility of the governance of digital security as a whole in EPPO, including the appointment of the Business Owners for the EPPO CIS.
2. The Security Unit shall be responsible for:
    a. Coordinating the risk assessment process for the EPPO CIS;
    b. Monitoring and evaluating the EPPO's risk landscape, inform the Security Authority, the Business Owners and the CIS Technical Managers about specific threats which could have an impact on the security of the CIS and the data they process, and recommend improvements;
    c. Performing security inspections (directly or through third parties), vulnerability assessments and penetration tests to assess the compliance of the EPPO CIS with the security plans and security requirements and report the results to the Security Authority, the Business Owners and the CIS Technical Managers;
    d. Monitoring the implementation of the security measures in the EPPO CIS;
    e. Provide appropriate documentation to the Business Owner, CIS Technical Manager and Data Protection Officer supporting the risk assessment process and implementation of the security measures in order to facilitate compliance with this Decision;
    f. Proposing a Security Strategy, policies, standards and guidelines addressing the security needs of the EPPO CIS in accordance with Article 9(2) of this Decision;
    g. Reporting regularly on the implementation of this Decision to the Administrative Director.
3. The Business Owner shall be responsible for:
    a. Ensuring compliance of the provisions of this Decision for the CIS under their responsibility;
    b. Support the risk management process;
    c. Issue instructions for users on the use of the CIS and related data as well as responsibilities of users related to CIS;

d. Communicate the security incidents impacting the CIS under their responsibility to the Security Unit, in line with the Policy on Reporting Security Incidents and to the Data Protection Officer in line with the procedures on personal data breaches[4];
e. For outsourced CIS, ensure that the appropriate security provisions are included in the outsourced contracts following consultation of the Security Unit.

4. The CIS Technical Manager shall be responsible for:
   a. Preparing the required documentation of the CIS design, architecture, technical specifications and implementation;
   b. Supporting the risk management process;
   c. Developing and operating the CIS while ensuring proper access management, backup, logging, monitoring, patch management, identify management and change management.
5. The users are responsible for:
   a. Complying with the security requirements and instructions issued by the Business Owner, CIS Technical Manager and Security Unit on the use of the CIS;
   b. Complying with the security rules, policies, procedures, standards, guidelines and other security notices on the use of EPPO CIS and information handling requirements;
   c. Using the CIS to which they have access only for the purpose they have received access;
   d. Participating in the mandatory awareness sessions relevant for their role. This shall include at least an onboarding session, awareness session on information security, and an awareness session on cyber security.

Article 11

Compliance, audit and improvement

1. Security compliance, audit and improvement shall involve the proper implementation and regular update of the security plans, implementing provisions, policies and standards.
2. The Security Unit may carry out inspections, audits, tests and other types of verifications to assess the implementation of security measures related to EPPO CIS
3. The Security Unit shall keep record of lessons learned and recommendations related to the implementation of this Decision
4. The Security Unit shall report on the implementation of this Decision on regular basis to the Administrative Director.
5. Failure to comply with this Decision may lead to the activation of the provisions enabling termination of contract.

[4] Article 8 of the College Decision 009/2020

Article 12

Security training and awareness

The EPPO shall implement digital security awareness and training programmes. This shall include at least the following:

1. A Policy on Security Awareness, to be adopted by the Administrative Director;
2. Provision by the Security Unit of awareness sessions on security requirements for EPPO CIS, information security, and cyber security for all users;
3. Provision by the Security Unit of specific security awareness sessions and/or trainings for users with elevated privileges (e.g. administrators).

Article 13

Final provisions

This Decision shall enter into force on the day of its adoption.

Done at Luxembourg on 7 February 2024.

For the College,

Laura Codruța Kövesi

European Chief Prosecutor

KOVESI Laura

Digitally signed by KOVESI Laura
Date: 2024.02.08 18:44:28 +01'00'