Decision of the Management Board 12/2017/MB

On the application of Commission Decision 443/2015 by analogy at CEPOL

Adopted by the Management Board

on 10 May 2017

THE MANAGEMENT BOARD,

Having regard to Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA[1] , and in particular Article 30 thereof,

Having regard to Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on security in the Commission,

Having regard to the Headquarters Agreement concluded between CEPOL and the Government of Hungary,

Whereas:

(1) The objective of security within CEPOL is to enable CEPOL to operate in a safe and secure environment by establishing a coherent, integrated approach as regards its security, providing appropriate levels of protection for persons, assets and information commensurate with identified risks, and ensuring efficient and timely delivery of security.

(2) CEPOL, like other international bodies, faces threats and challenges in the field of security, in particular as regards terrorism, cyberattacks and political espionage.

(3) In order to ensure security of persons, assets and information, CEPOL may need to take measures in areas protected by fundamental rights as enshrined in the Charter of Fundamental Rights and in the European Convention on Human Rights and as recognised by the European Court of Justice.

(4) CEPOL has entered into instruments on security matters for its head quarter with the government of Hungary ([2]). These instruments confirm that the Hungarian authorities are responsible for the security of CEPOL's headquarter and staff in Hungary.

(5) Any such measure should therefore be justified by the importance of the interest it is designed to protect, be proportionate and ensure full respect for fundamental rights, including especially the rights of privacy and data protection.

1 OJ L319, 4.12.2015, p.1
2 https://www.cepol.europa.eu/sites/default/files/hq-agreement-text.pdf

(6) Within a system committed to the rule of law and the respect of fundamental rights, CEPOL has to strive for an appropriate level of security for its staff, assets and information that ensures it can carry out its operations, while not limiting fundamental rights beyond what is strictly necessary.

(7) Security in CEPOL shall be based on the principles of legality, transparency, proportionality and accountability.

(8) Members of staff mandated to take security measures should not be placed at any disadvantage because of their actions unless they acted outside the scope of their mandate or in violation of the law, and hence in this respect this Decision is to be considered as a service instruction within the meaning of the Staff Regulations.

(9) CEPOL should take appropriate initiatives to foster and strengthen its security culture, ensuring a more efficient delivery of security, improving its security governance, further intensifying networks and cooperation with relevant authorities at international, European and national level, and improving monitoring and control of the implementation of security measures.

(10) The security policy of CEPOL should be implemented in a manner which is consistent with other internal processes and procedures that may involve a security element. These include, in particular, Business Continuity Management which aims at preserving the critical functions of CEPOL in case of an operational disruption.

(11) Notwithstanding the measures already in place at the time of adoption of this Decision and notified to the European Data Protection Supervisor (1[3]), any measure under this Decision involving the processing of personal data shall be subject to implementing rules in accordance with Article 21, which shall lay down appropriate safeguards for data subjects.

(12) Therefore, there is a need for CEPOL to establish a regulatory basis for security at CEPOL.

[3] As indicated in the website of the European Data Protection Supervisor rules on: Leave and Flexitime (2013-0315), Health data at work (2013-0893), Processing of grant applications to organise courses and seminars (residential activities) (2013-1394), Processing of tender applications and contracts to manage public procurement procedures (2013-1395), Selection of temporary agents, contract agents and trainees (2017-0187).

HAS DECIDED AS FOLLOWS:

Article 1

The objectives, basic principles, organisation and responsibilities regarding security at CEPOL as detailed in the Annex to the present Decision are hereby adopted.

Article 2

The present Decision shall take effect on the day following that of its adoption.

Done at Malta, 10 May 2017

For the Management Board

<Signature on file>

……..

Mrs Frederike Everts MPA
Chair of the Management Board

European Union Agency for Law Enforcement Training
Offices: H-1066 Budapest, Ó utca 27., Hungary • Correspondence: H-1903 Budapest, Pf. 314, Hungary
Telephone: +36 1 803 8030 • Fax: +36 1 803 8032 • E-mail: info@cepol.europa.eu • www.cepol.europa.eu

ANNEX

Chapter 1 – General Provisions

Article 1 - Definitions

For the purposes of this Decision the following definitions apply:

(1) 'Assets' means all movable and immovable property and possessions of CEPOL;

(2) 'Communication and Information System' or 'CIS' means any system enabling the handling of information in electronic form, including all assets required for its operation, as well as the infrastructure, organisation, personnel and information resources;

(3) 'Control of risks' shall mean any security measure that can reasonably be expected to effectively control a risk to security by its prevention, mitigation, avoidance or transfer;

(4) 'Crisis situation' means a circumstance, event, incident or emergency (or a succession or combination thereof) posing a major or an immediate threat to security in CEPOL regardless of its origin;

(5) 'Data' means information in a form that allows it to be communicated, recorded or processed;

(6) 'Personal data' means personal data as defined in Article 2(a) of Regulation (EC) No 45/2001 of the European Parliament and of the Council ([1]);

(7) 'Premises' shall mean any immovable or assimilated property and possessions of CEPOL or made available to CEPOL;

(8) 'Prevention of risk' shall mean security measures that can reasonably be expected to impede, delay or stop a risk to security;

---

1 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1)

(9) 'Risk to security' means the combination of the threat level, the level of vulnerability and the possible impact of an event;

(10) 'Security in CEPOL' means the security of persons, assets and information in CEPOL, and in particular the physical integrity of persons and assets, the integrity, confidentiality and availability of information and communication and information systems, as well as the unobstructed functioning of CEPOL operations;

(11) 'Security measure' means any measure taken in accordance with this Decision for purposes of controlling risks to security;

(12) 'Staff Regulations' means the Staff Regulations of officials of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No 259/68 of the Council ([2]) and its amending acts;

(13) 'Threat to security' means an event or agent that can reasonably be expected to adversely affect security if not responded to and controlled;

(14) 'Immediate threat to security' means a threat to security which occurs with no or with extremely short advance warning; and

(15) 'Major threat to security' means a threat to security that can reasonably be expected to lead to loss of life, serious injury or harm, significant damage to property, compromise of highly sensitive information, disruption of IT systems or of essential operational capacities of CEPOL;

(16) 'Vulnerability' means a weakness of any nature that can reasonably be expected to adversely affect security in CEPOL, if exploited by one or more threats.

Article 2 – Subject matter

1. This Decision sets out the objectives, basic principles, organisation and responsibilities regarding security at CEPOL.

2. This Decision shall apply to all CEPOL departments and in all premises of CEPOL. CEPOL staff working in EU institutions, bodies or entities shall be subject to the security rules for those organisations.

[2] Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (Conditions of Employment of Other Servants) (OJ L 56, 4.3.1968, p. 1).

3. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to CEPOL staff under the scope of the Staff Regulations and of the Conditions of Employment of other servants of the European Union, to national experts seconded to CEPOL (SNEs), to service providers and their staff, to trainees and to any individual with access to CEPOL buildings or other assets, or to information handled by CEPOL.

4. The provisions of this Decision shall be without prejudice to Commission Decision 2002/47/EC, ECSC, Euratom ([3]) and Commission Decision 2004/563/EC, Euratom ([4]), Commission Decision C(2006) 1623 ([5]) and Commission Decision (EU, Euratom) 2017/46([6]) or rules equivalent to these decisions.

Chapter 2 – Principles

Article 3 – Principles for security in CEPOL

1. In implementing this Decision, CEPOL shall comply with the Treaties and in particular the Charter of Fundamental Rights and Protocol No 7 on the Privileges and Immunities of the European Union, with the instruments referred to in recital 2 with any applicable rules of national law as well as with the terms of the present Decision. If necessary, a security notice in the sense of Article 21(2) providing guidance in this respect shall be issued.

2. Security in CEPOL shall be based on the principles of legality, transparency, proportionality and accountability.

3. The principle of legality indicates the need to stay strictly within the legal framework in implementing this Decision and the need to conform to the legal requirements.

---

3 Commission Decision 2002/47/EC, ECSC, Euratom of 23 January 2002 amending its Rules of Procedure (OJ L 21, 24.1.2002, p. 23) annexing the provisions on document management

4 Commission Decision 2004/563/EC, Euratom of 7 July 2004 amending its Rules of Procedure (OJ L 251, 27.7.2004, p. 9) annexing the provisions on electronic and digitised documents

5 C(2006) 1623 of 21 April 2006 establishing a harmonised policy for health and safety at work for all European Commission staff

6 Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 (OJ L 6, 11.1.2017, p. 40) on the security of communication and information system in the European Commission

4. Any security measure shall be taken overtly unless this can reasonably be expected to impair its effect. Addressees of a security measure shall be informed in advance of the reasons for and the impact of the measure, unless the effect of the measure can reasonably be expected to be impaired by providing such information. In this case, the addressee of the security measure shall be informed after the risk of impairing the effect of the security measure has ceased.
5. CEPOL departments shall ensure that security issues are taken into account from the start of the development and implementation of its policies, decisions, programmes, projects and activities for which it is responsible. In order to do so, it shall involve the Head of Corporate Services Department, the CEPOL Security Officer and the ICT Officer as regards IT systems from the earliest stages of preparation.
6. CEPOL shall, where appropriate, seek cooperation with the competent authorities of the host state and of EU institutions, agencies or bodies, where feasible, taking account of the measures taken or planned by those authorities to address the risk to security concerned.

Article 4 – Obligation to comply

1. Compliance with this Decision and its implementing rules and with the security measures and the instructions given by mandated staff shall be mandatory.
2. Non-compliance with the security rules may trigger liability to disciplinary action in accordance with the Treaties, the Staff Regulations, to contractual sanctions and/or to legal action under national laws and regulations.

Chapter 3 – Delivering Security

Article 5 – Mandated staff

1. Only staff authorised on the basis of a nominative mandate conferred to them by the Executive Director, given their current duties, may be entrusted with the power to take one or several of the following measures:

   (1) Carry side arms;

   (2) Conduct security inquiries as referred to in Article 13;

(3) Take security measures as referred to in Article 12 as specified in the mandate.

2. The mandates referred to in paragraph 1 shall be conferred for a duration which shall not exceed the period during which the person concerned holds the post or function in respect of which the mandate has been conferred. They shall be conferred in compliance with the applicable provisions set out in Article 3(1).

3. As regards mandated staff, this Decision constitutes a service instruction within the meaning of Article 21 of the Staff Regulations.

Article 6 – General provisions regarding security measures

1. When taking security measures, CEPOL shall in particular ensure so far as reasonably possible, that:

(a) it only seeks support or assistance from the state concerned, provided that that state either is a Member State of the European Union or, if not, party to the European Convention on Human Rights, or guarantees rights which are at least equivalent to the rights guaranteed in this Convention;

(b) it shall only transfer information on an individual to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC of the European Parliament and of the Council ([7]), in accordance with Article 9 of Regulation (EC) No 45/2001;

(c) where an individual poses a threat to security, any security measure shall be directed against that individual and that individual may be subjected to bearing the incurring costs. Those security measures may only be directed against other individuals if an immediate or major threat to security must be controlled and the following conditions are fulfilled:

(a) the envisaged measures against the individual posing the threat to security cannot be taken or are not likely to be effective;

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(b) CEPOL cannot control the threat to security by its own actions or cannot do so in a timely manner;

(c) the measure does not constitute a disproportionate danger for the other individual and his rights.

2. The Executive Director shall establish an overview of security measures which may require an order by a judge in accordance with the laws and regulations of the Member State hosting CEPOL premises.

3. The Executive Director may turn to a contractor to carry out, under the direction and supervision of the Security Officer, tasks relating to security.

Article 7 – Security measures regarding persons

1. An appropriate level of protection shall be afforded to persons in the premises of CEPOL, taking into account security and safety requirements.

2. In case of major risks to security, the Executive Director in cooperation with the relevant authorities of the Host Member State shall provide for appropriate security measures for staff where a threat assessment has indicated that such protection is needed to ensure their safety and security.

3. In case of major risks to security, CEPOL may order the evacuation of its premises.

4. Victims of accidents or attacks within CEPOL premises shall receive assistance.

5. In order to prevent and control risks to security, mandated staff may carry out background checks of persons falling under the scope of this Decision, so as to determine whether giving such persons access to CEPOL premises or information presents a threat to security. For that purpose, and in compliance with Regulation (EC) No 45/2001 and provisions referred to under Article 3(1), the mandated staff concerned may:

(a) use any source of information available to CEPOL, taking into account the reliability of the source of information;

(b) access the personnel file or data CEPOL holds with regard to individuals it employs or intends to employ, or for contractors' staff when duly justified.

Article 8 – Security measures regarding physical security and assets

1. Security of assets shall be ensured by applying appropriate physical and technical protective measures and corresponding procedures, hereinafter called 'physical security', creating a multi-layered system.
2. Measures may be adopted pursuant to this Article in order to protect persons or information in CEPOL as well as to protect assets.
3. Physical security shall have the following objectives:
   - preventing acts of violence directed against persons falling within the scope of this Decision,
   - preventing espionage and eavesdropping on sensitive or classified information,
   - preventing theft, acts of vandalism, sabotage and other violent actions aimed at damaging or destroying CEPOL premises,
   - enabling investigation and inquiry into security incidents including through checks on access and exit control log files, CCTV coverage, telephone call recordings and similar data as referred to in Article 21(1) hereunder and other information sources.
4. Physical security shall include:
   - an access policy applicable to any person or vehicle requiring access to CEPOL premises, including the parking lots,
   - an access control system comprising guards, technical equipment and measures, information systems or a combination of all of those elements.
5. In order to ensure physical security, the following actions may be taken:
   - recording entry to and exit from CEPOL premises of persons, vehicles, goods and equipment,
   - identity controls at its premises,
   - inspection of vehicles, goods and equipment by visual or technical means,
   - preventing unauthorised persons, vehicles and goods, from entering CEPOL premises.

Article 9 – Security measures regarding information

1. Security of information covers all information handled by CEPOL.
2. Security of information, regardless of its form, shall balance transparency, proportionality, accountability and efficiency with the need to protect

information from unauthorised access, use, disclosure, modification or destruction.

3. Security of information shall be aimed at protecting confidentiality, integrity and availability.

4. Risk management processes shall therefore be used to categorise information assets and to develop proportionate security measures, procedures and standards, including mitigating measures.

5. These general principles underlying security of information shall be applied in particular as regards:

   (a) 'European Union Classified Information' (hereafter 'EUCI'), that is to say any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States;

   (b) 'Sensitive non-classified information', that is to say information or material CEPOL must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information includes, but is not limited to, information or material covered by the obligation of professional secrecy, as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([8]) read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EC) No 45/2001.

6. Sensitive non-classified information shall be subject to rules regarding its handling and storage. It shall only be released to those individuals who have a 'need-to-know'. When deemed necessary for the effective protection of its confidentiality, it shall be identified by a security marking and corresponding handling instructions approved by the CEPOL Security Officer. When handled or stored on Communication and Information Systems, such information shall be protected also in compliance with

[8] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

Commission Decision (EU, Euratom) 2017/46, its implementing rules and corresponding standards.

7. Any individual who is responsible for compromising or losing EUCI or sensitive non-classified information, which is identified as such in the rules regarding its handling and storage, may be liable to disciplinary action in accordance with the Staff Regulations. That disciplinary action shall be without prejudice to any further legal or criminal proceedings by the competent national authorities of the Member States in accordance with their laws and regulations and to contractual remedies.

Article 10 – Security measures regarding Communication and Information Systems

1. All Communication and Information Systems ('CIS') used by CEPOL shall comply with the Commission's Information Systems Security Policy, as set out in Commission Decision (EU, Euratom) 2017/46, its implementing rules and corresponding security standards.
2. CEPOL services owning, managing or operating CIS shall only allow Union institutions, agencies, bodies or other organisations to have access to those systems provided that those entities have IT systems that are protected at a level equivalent to the Commission's Information Systems Security Policy as set out in Commission Decision (EU, Euratom) 2017/46, its implementing rules and corresponding security standards. CEPOL shall monitor such compliance, and in case of serious non-compliance or continued failure to comply, be entitled to prohibit access.

Article 11 – Forensic analysis regarding cyber-security

The CEPOL Security Officer shall in particular be responsible for conducting forensic technical analysis in cooperation with the competent Commission departments in support of the security inquiries referred to in Article 13, related to counterintelligence, data leakage, cyberattacks and information systems security.

Article 12 – Security measures regarding persons and objects

1. In order to ensure the security in CEPOL and to prevent and control risks, staff mandated in accordance with Article 5 may, in compliance with the principles set out in Article 3, take inter alia one or more of the following security measures:

(a) securing of scenes and evidence, including access and exit control log files, CCTV images, in case of incidents or conduct that may lead to administrative, disciplinary, civil or criminal procedures;

(b) limited measures concerning persons posing a threat to security, including ordering persons to leave CEPOL's premises, escorting persons from CEPOL's premises, banning persons from CEPOL's premises for a period of time, the latter defined in accordance with criteria to be defined in implementing rules;

(c) limited measures concerning objects posing a threat to security including removal, seizure and disposal of objects;

(d) searching of CEPOL premises, including of offices, within such premises;

(e) searching of CIS and equipment, telephone and telecommunications traffic data, log files, user accounts, etc.;

(f) other specific security measures with similar effect in order to prevent or control risks to security, in particular in the context of the CEPOL's rights as an employer in accordance with the applicable national laws.

2. Under exceptional circumstances, the CEPOL Security Officer, mandated in accordance with Article 5, may take any urgent measures needed, in strict compliance with the principles laid down in Article 3. As soon as possible after having taken those measures, she/he shall inform the Executive Director, confirming the measures taken and authorising any further necessary actions and shall liaise, where appropriate with the competent national authorities.

3. Security measures pursuant to this Article shall be documented at the time they are taken or, in the event of an immediate risk or a crisis situation, within reasonable delay after they are taken. In the latter case, the documentation must also include the elements on which the assessment regarding the existence of an immediate risk or a crisis situation was based. The documentation can be concise, but should be constituted in such a way as to allow the person subjected to the measure to exercise his rights of defence and of protection of personal data in accordance with Regulation (EC) No 45/2001, and to allow a scrutiny as to the legality of the measure. No information about specific security measures addressed to a member of staff shall be part of the person's personnel file.

4. When taking security measures pursuant to point (b), CEPOL shall in addition guarantee that the individual concerned is given the opportunity to contact a lawyer or a person of his confidence and be made aware of their right to have recourse to the European Data Protection Supervisor.

Article 13 – Inquiries

1. Without prejudice to Article 86 and Annex IX of the Staff Regulations, security inquiries may be conducted:
   (a) in case of incidents affecting security at CEPOL, including suspected criminal offences;
   (b) in case of potential leakage, mishandling or compromise of sensitive non-classified information, EUCI or Euratom Classified Information;
   (c) in the context of counter-intelligence and counter-terrorism;
   (d) in case of serious cyber-incidents.
2. The decision to conduct a security inquiry shall be taken by the Executive Director who will also be the recipient of the inquiry report.
3. Security inquiries shall be conducted only by the CEPOL Security Officer, duly mandated in accordance with Article 5. The CEPOL Security Officer may request support from EU institutions, bodies and agencies as necessary to conduct the inquiry.
4. The CEPOL Security Officer shall exercise her/his powers of security inquiry independently, as specified in the mandate and shall have the powers listed in Article 12.
5. CEPOL Security Officer having the competence to conduct security inquiries may gather information from all available sources related to any administrative or criminal offences committed within the CEPOL premises or involving persons referred to in Article 2(3) either as victim or perpetrator of such offences.
6. The CEPOL Security Officer shall inform the competent authorities of the host Member State, any other Member State concerned or the respective NSA, where appropriate, and in particular if the inquiry has given rise to indications of a criminal act having been perpetrated. In this context, the CEPOL Security Officer may, where appropriate or required, provide support to the authorities of the host Member State or any other Member State concerned.

7. In the case of serious cyber-incidents the CEPOL Security Officer shall collaborate closely with the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) to provide support on all technical matters. The CEPOL Security Officer shall decide, in consultation with CERT-EU, when it is appropriate to inform the competent authorities of the host country or any other Member State concerned. The incident coordination services of CERT-EU will be used as regards support to EU institutions and agencies that may be affected.
8. Security inquiries shall be documented.

Article 14 – Delineation of competences with regard to security inquiries and other types of investigations

1. Where the CEPOL Security Officer conducts security inquiries, as referred to in Article 13, and if these enquiries fall within the competences of the European Anti-Fraud Office (OLAF) or the Investigation and Disciplinary Office of the Commission (IDOC), it shall liaise with those bodies at once with a view, in particular, not to compromise later steps by either OLAF or IDOC. Where appropriate, the CEPOL Security Officer shall invite OLAF or IDOC to be involved in the investigation.
2. The security enquiries, as referred to in Article 13, shall be without prejudice to the powers of OLAF and IDOC as laid down in the rules governing those bodies. The CEPOL Security Officer may be requested to provide technical assistance for inquiries initiated by OLAF or IDOC.
3. The CEPOL Security Officer may be asked to assist OLAF's agents when they access CEPOL premises in accordance with Articles 3(5) and 4(4) of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council ([9]), in order to facilitate their tasks. The CEPOL Security Officer shall inform the Executive Director of such requests for assistance.
4. Without prejudice to Article 22(a) of the Staff Regulations, where a case may fall within the competence of both the CEPOL Security Officer and IDOC, the CEPOL Security Officer shall, when it reports to the Executive Director in compliance with Article 13 at the earliest possible stage advise whether there are grounds that justify that IDOC is seized with the matter.

[9] Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).

This stage shall in particular be considered to have been reached when an immediate threat to security has come to an end. The Executive Director shall decide on the matter.

5. Where a case may fall within the competence of both the CEPOL Security Officer and OLAF, the Security Officer shall without delay report to the Executive Director and shall inform the Director-General of OLAF at the earliest possible stage. This stage shall in particular be considered to have been reached when an immediate threat to security has come to an end.

Article 15 - Security inspections

1. The following inspections are to be conducted:
   a. Internal inspections by CEPOL staff as a measure to ensure compliance with this decision;
   b. Inspections conducted by or on behalf of CEPOL to ensure that CEPOL staff, assets and/or information managed by Union institutions, agencies or bodies is being managed correctly.
2. Any support from the Directorate-General for Human Resources and Security (DG HR) of the European Commission in conducting these security inspections shall be covered by an SLA.

Article 16 - Alert states and management of crisis situations

1. The CEPOL Security Officer shall be responsible for putting in place appropriate alert state measures in anticipation of or in response to threats and incidents affecting security at CEPOL, and for measures required for managing crisis situations.
2. The alert state measures referred to in paragraph 1 shall be commensurate with the level of threat to security. The alert states levels shall be defined in close cooperation with the competent services of Union institutions, agencies and bodies, and of the Member State hosting CEPOL premises.

CHAPTER 4 - ORGANISATION

Article 17 - General responsibilities of CEPOL services

1. The responsibilities of CEPOL referred to in this Decision shall be exercised by the CEPOL Security Officer under the authority and responsibility of the Executive Director.
2. The specific arrangements as regards cyber-security are defined in Commission Decision (EU, Euratom) 2017/46.
3. The responsibilities for implementing this Decision and its implementing rules and for day-to-day compliance may be delegated to other CEPOL departments or individuals, whenever decentralised delivery of security offers significant efficiency, resource or time savings, for instance because of the geographical location of the services concerned.
4. Where paragraph 3 applies, the CEPOL Security Officer shall conclude arrangements with individual CEPOL departments or officers establishing clear roles and responsibilities for the implementation and monitoring of security policies.

Article 18 - The CEPOL Security Officer

1. The CEPOL Security Officer shall in particular be responsible for:
   (1) developing CEPOL's security policy, implementing rules and security notices;
   (2) gathering information in view of assessing threats and risks to security and on all issues which may affect security in CEPOL;
   (3) providing counter electronic surveillance and protection to all the sites of CEPOL, taking due account of threat assessments and evidence of unauthorised activities against CEPOL's interests;
   (4) providing a 8-hour/5-day emergency service for CEPOL services and staff for any safety- and security-related issues;
   (5) implementing security measures aimed at mitigating risks to security and developing and maintaining appropriate CIS to cover its operational needs, particularly in the domains of physical access control, administration of security authorisations and handling of sensitive and EU classified information;

(6) raising awareness, organising exercises and drills and providing training and advice on all issues related to security at CEPOL, in view of promoting a security culture and creating a pool of personnel appropriately trained in security matters.

2. The CEPOL Security Officer shall, without prejudice to other CEPOL services' competences and responsibilities, ensure external liaison:
   (1) with the security departments of the Union institutions, agencies and bodies on issues relating to the security of the persons, assets and information in CEPOL;
   (2) with security, intelligence and threat assessment services of the Host Member State and the relevant Commission services on issues affecting the security of persons, assets and information in CEPOL;
   (3) with police and other emergency services on all routine and emergency issues affecting CEPOL's security;
   (4) with CERT-EU in the field of response to cyberattacks with a potential impact on security in CEPOL;
   (5) regarding the receipt, assessment and distribution of intelligence concerning threats posed by terrorist and espionage activities affecting security in CEPOL;
   (6) regarding issues relating to classified information, as specified further in the Commission Decision (EU, Euratom) 2015/444 ([10]) as applied by *mutatis mutandis* in CEPOL.

3. The CEPOL Security Officer shall be responsible for the secure transmission of information performed under this Article, including the transmission of personal data.

CHAPTER 5 – IMPLEMENTATION

Article 20 – Implementing rules and security notices

1. As necessary, the adoption of the implementing rules for this Decision will be the subject of a separate empowerment decision of the Management Board to the Executive Director of CEPOL.

2. After being empowered following the abovementioned Management Board decision, the Executive Director of CEPOL may develop security

[10] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the Security rules for protecting EU classified information (see page 53 of this Official Journal).

notices setting out security guidelines and best practices within the scope of this Decision and its implementing rules.

The Commission and in particular DG HR DS, shall be consulted on such notices and/or guidelines, especially those relating to EUCI, prior to formal adoption.

3. The Executive Director of CEPOL may delegate the tasks mentioned in the second paragraph of this Article to the CEPOL Security officer by a separate delegation decision.

CHAPTER 6 – MISCELLANEOUS AND FINAL PROVISIONS

Article 21 – Processing of personal data

1. CEPOL shall process personal data needed for implementing this Decision in accordance with Regulation (EC) No 45/2001.
2. Notwithstanding the measures already in place at the time of adoption of this Decision and notified to the European Data Protection Supervisor ([11]), any measure under this Decision involving the processing of personal data, such as relating to access and exit logs, CCTV recordings, recordings of telephone calls to duty offices or dispatch centres and similar data, which are required for reasons of security or crisis response, shall be subject to implementing rules in accordance with Article 20, which shall lay down appropriate safeguards for data subjects.
3. The CEPOL Security Officer shall be responsible for the security of any processing of personal data undertaken in the context of this Decision.
4. Those implementing rules and procedures shall be adopted after consultation of the Data Protection Officer and the European Data Protection Supervisor in accordance with Regulation (EC) No 45/2001.

Article 22 – Transparency

This Decision and its implementing rules shall be brought to the attention of CEPOL staff and to all individuals to whom they apply.

[11] See footnote 3 of the present Decision.