COMMISSION DECISION (EU, Euratom) 2015/443

of 13 March 2015

on Security in the Commission

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community,

Having regard to the Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaties, and in particular Article 18 thereof,

Whereas:

(1) The objective of security within the Commission is to enable the Commission 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) The Commission, like other international bodies, faces major threats and challenges in the field of security, in particular as regards terrorism, cyberattacks and political and commercial espionage.

(3) The European Commission has entered into instruments on security matters for its principal sites with the governments of Belgium, Luxembourg and Italy ([1]). These instruments confirm that the Commission is responsible for its security.

(4) In order to ensure security of persons, assets and information, the Commission 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.

(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.

(6) Within a system committed to the rule of law and the respect of fundamental rights, the Commission 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 the Commission 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) The Commission 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 establishment of the European External Action Service (EEAS) as a functionally autonomous body of the Union has had a significant impact on the Commission's security interests, and hence requires that rules and procedures for cooperation as regards safety and security be established between the EEAS and the Commission, in particular with regard to the fulfilment of the Commission's duty-of-care responsibilities towards Commission staff in Union Delegations.

([1]) Cf. the 'Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité' of 31 December 2004, the 'Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois' of 20 January 2007, and the 'Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale' of 22 July 1959.

(11) The security policy of the Commission 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 the Commission in case of an operational disruption, and the ARGUS process for multisectoral crisis coordination.

(12) Notwithstanding the measures already in place at the time of adoption of this Decision and notified to the European Data Protection Supervisor ([1]), 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.

(13) Therefore, there is a need for the Commission to review, update, and consolidate the existing regulatory basis for security at the Commission.

(14) The Commission Decision C(94) 2129 ([2]) should therefore be repealed,

HAS ADOPTED THIS DECISION:

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 the Commission;

(2) 'Commission department' means a Commission Directorate-General or service, or a Cabinet of a Member of the Commission;

(3) '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;

(4) '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;

(5) '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 the Commission regardless of its origin;

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

(7) 'Member of the Commission responsible for security' means a Member of the Commission under whose authority the Directorate-General for Human Resources and Security falls;

(8) '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 ([3]);

(9) 'premises' shall mean any immovable or assimilated property and possessions of the Commission;

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

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

(12) 'security in the Commission' means the security of persons, assets and information in the Commission, 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 Commission operations;

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

([2]) Commission Decision C(94) 2129 of 8 September 1994 on the tasks of the Security Office.

([3]) 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).

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

(14) '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 [1] and its amending acts;

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

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

(17) '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 the Commission;

(18) 'vulnerability' means a weakness of any nature that can reasonably be expected to adversely affect security in the Commission, 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 the Commission.

2. This Decision shall apply to all Commission departments and in all premises of the Commission. Commission staff working in Union Delegations shall be subject to the security rules for the European External Action Service [2].

3. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to the Members of the Commission, to Commission 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 the Commission (SNEs), to service providers and their staff, to trainees and to any individual with access to Commission buildings or other assets, or to information handled by the Commission.

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 C(2006) 3602 [6].

CHAPTER 2

PRINCIPLES

Article 3

Principles for security in the Commission

1. In implementing this Decision, the Commission 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 the Commission 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.

---

[1] 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).

[2] Decision of the High Representative of the Union for Foreign Affairs and Security Policy 2013/C 190/01 of 19 April 2013 on the security rules for the European External Action Service (OJ C 190, 29.6.2013, p. 1).

[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] C(2006) 3602 of 16 August 2006 concerning the security of information systems used by 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. Commission departments shall ensure that security issues are taken into account from the start of the development and implementation of Commission policies, decisions, programmes, projects and activities for which they are responsible. In order to do so, they shall involve the Directorate-General for Human Resources and Security in general and the Chief Information Security Officer of the Commission as regards IT systems from the earliest stages of preparation.

6. The Commission shall, where appropriate, seek cooperation with the competent authorities of the host state, of other Member States and of other 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 Director-General for Human Resources and Security, 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 hold 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, the Commission 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 [1], in accordance with Article 9 of Regulation (EC) No 45/2001;

[1] 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).

(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;

(b) the Commission 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 Security Directorate of the Directorate-General for Human Resources and Security 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 States hosting Commission premises.

3. The Security Directorate of the Directorate-General for Human Resources and Security may turn to a contractor to carry out, under the direction and supervision of the Security Directorate, 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 the Commission, taking into account security and safety requirements.

2. In case of major risks to security, the Directorate-General for Human Resources and Security shall provide close protection for Members of the Commission or other 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, the Commission may order the evacuation of its premises.

4. Victims of accidents or attacks within Commission 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 Commission 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 the Commission, taking into account the reliability of the source of information;

(b) access the personnel file or data the Commission 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 the Commission as well as to protect assets.

3. Physical security shall have the following objectives:

— preventing acts of violence directed against Members of the Commission or 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 Commission buildings and assets,

— 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 22(2) hereunder and other information sources.

4. Physical security shall include:

— an access policy applicable to any person or vehicle requiring access to Commission 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 Commission 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 Commission premises.

Article 9

Security measures regarding information

1. Security of information covers all information handled by the Commission.

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 classify 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 the Commission 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 [1] 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 Director-General for Human Resources and Security. When handled or stored on Communication and Information Systems, such information shall be protected also in compliance with Decision C(2006) 3602, 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.

[1] 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).

Article 10

Security measures regarding Communication and Information Systems

1. All Communication and Information Systems ('CIS') used by the Commission shall comply with the Commission's Information Systems Security Policy, as set out in Decision C(2006) 3602, its implementing rules and corresponding security standards.

2. Commission services owning, managing or operating CIS shall only allow other Union institutions, agencies, bodies or other organisations to have access to those systems provided that those Union institutions, agencies, bodies or other organisations can provide reasonable assurance that their IT systems are protected at a level equivalent to the Commission's Information Systems Security Policy as set out in Decision C(2006) 3602, its implementing rules and corresponding security standards. The Commission 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 Directorate-General for Human Resources and Security 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 the Commission 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 the Commission's premises, escorting persons from the Commission's premises, banning persons from the Commission'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 Commission 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 Commission's rights as a landlord or as an employer in accordance with the applicable national laws.

2. Under exceptional circumstances, staff members of the Security Directorate of the Directorate-General for Human Resources and Security, 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, they shall inform the Director of the Security Directorate, who shall seek the appropriate mandate from the Director-General for Human Resources and Security, 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), the Commission 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 and to any special arrangement between the Commission and the EEAS, such as the special arrangement signed on 28 May 2014 between the Directorate General for Human Resources and Security of the European Commission and the European External Action Service on the duty of care towards Commission staff posted in Union Delegations, security inquiries may be conducted:

(a) in case of incidents affecting security at the Commission, 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 Director-General for Human Resources and Security who will also be the recipient of the inquiry report.

3. Security inquiries shall be conducted only by dedicated members of staff of the Directorate-General for Human Resources and Security, duly mandated in accordance with Article 5.

4. The mandated staff shall exercise their powers of security inquiry independently, as specified in the mandate and shall have the powers listed in Article 12.

5. Mandated staff having the competence to conduct security inquiries may gather information from all available sources related to any administrative or criminal offences committed within the Commission premises or involving persons referred to in Article 2(3) either as victim or perpetrator of such offences.

6. The Directorate-General for Human Resources and Security shall inform the competent authorities of the host Member State or any other Member State concerned, where appropriate, and in particular if the inquiry has given rise to indications of a criminal act having been perpetrated. In this context, the Directorate-General for Human Resources and Security 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 Directorate-General for Informatics shall collaborate closely with the Directorate-General for Human Resources and Security to provide support on all technical matters. The Directorate-General for Human Resources and Security shall decide, in consultation with the Directorate-General for Informatics, when it is appropriate to inform the competent authorities of the host country or any other Member State concerned. The incident coordination services of Computer Emergency Response Team for the European institutions, bodies and agencies ('CERT-EU') will be used as regards support to other 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 Security Directorate of the Directorate-General for Human Resources and Security 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 Security Directorate of the Directorate-General for Human Resources and Security 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 Security Directorate of the Directorate-General for Human Resources and Security may be requested to provide technical assistance for inquiries initiated by OLAF or IDOC.

3. The Security Directorate of the Directorate-General for Human Resources and Security may be asked to assist OLAF's agents when they access Commission 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 [1], in order to facilitate their tasks. The Security

[1] 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).

Directorate informs of such requests for assistance the Secretary-General and the Director-General of the Directorate-General for Human Resources and Security or, if such investigation is carried out on premises of the Commission occupied by its Members or by the Secretary-General, the President of the Commission and the Commissioner in charge of Human Resources.

4. Without prejudice to Article 22(a) of the Staff Regulations, where a case may fall within the competence of both the Security Directorate of the Directorate-General for Human Resources and Security and IDOC, the Security Directorate shall, when it reports to the Director-General of Human Resources in compliance with Article 13 at the earliest possible stage advise whether there are grounds that justify that IDOC is seized with the matter. This stage shall in particular be considered to have been reached when an immediate threat to security has come to an end. The Director-General of Human Resources and Security shall decide on the matter.

5. Where a case may fall within the competence of both the Security Directorate of the Directorate-General for Human Resources and Security and OLAF, the Security Directorate shall without delay report to the Director-General of Human Resources and Security 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 Directorate-General for Human Resources and Security shall undertake security inspections in order to verify compliance by Commission services and individuals with this Decision and its implementing rules and to formulate recommendations when deemed necessary.

2. Where appropriate, the Directorate-General for Human Resources and Security shall undertake security inspections or security monitoring or assessment visits to verify whether the security of Commission staff, assets and information falling under the responsibility of other Union institutions, agencies or bodies, Member States, third states or international organisations, is appropriately protected in accordance with security rules, regulations and standards which are at least equivalent to those of the Commission. Where appropriate and in the spirit of good cooperation between administrations, those security inspections shall also include inspections conducted in the context of the exchange of classified information with other Union institutions, bodies and agencies, Member States or with third states or international organisations.

3. This Article shall be implemented, mutatis mutandis, for Commission staff in Union Delegations, without prejudice to any special arrangement between the Commission and the EEAS, such as the special arrangement signed on 28 May 2014 between the Directorate General for Human Resources and Security of the European Commission and the European External Action Service on the duty of care towards Commission staff posted in Union Delegations.

Article 16

Alert states and management of crisis situations

1. The Directorate-General for Human Resources and Security shall be responsible for putting in place appropriate alert state measures in anticipation of or in response to threats and incidents affecting security at the Commission, 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 other Union institutions, agencies and bodies, and of the Member State or Member States hosting Commission premises.

3. The Directorate-General for Human Resources and Security shall be the contact point for alert states and management of crisis situations.

CHAPTER 4

ORGANISATION

Article 17

General responsibilities of Commission services

1. The responsibilities of the Commission referred to in this Decision shall be exercised by the Directorate-General for Human Resources and Security under the authority and responsibility of the Member of the Commission responsible for security.

2. The specific arrangements as regards cyber-security are defined in Decision C(2006) 3602.

3. The responsibilities for implementing this Decision and its implementing rules and for day-to-day compliance may be delegated to other Commission departments, 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 Directorate-General for Human Resources and Security, and where appropriate the Director-General for Informatics, shall conclude arrangements with individual Commission departments establishing clear roles and responsibilities for the implementation and monitoring of security policies.

Article 18

The Directorate-General for Human Resources and Security

1. The Directorate-General for Human Resources and Security shall in particular be responsible for:

(1) developing the Commission'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 the Commission;

(3) providing counter electronic surveillance and protection to all the sites of the Commission, taking due account of threat assessments and evidence of unauthorised activities against the Commission's interests;

(4) providing a 24-hour/7-day emergency service for Commission 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 the Commission, in view of promoting a security culture and creating a pool of personnel appropriately trained in security matters.

2. The Directorate-General for Human Resources and Security shall, without prejudice to other Commission services' competences and responsibilities, ensure external liaison:

(1) with the security departments of the other Union institutions, agencies and bodies on issues relating to the security of the persons, assets and information in the Commission;

(2) with security, intelligence and threat assessment services, including national security authorities, of the Member States, of third countries and international organisations and bodies on issues affecting the security of persons, assets and information in the Commission;

(3) with police and other emergency services on all routine and emergency issues affecting the Commission's security;

(4) with the security authorities of other Union institutions, of agencies and bodies, of the Member States and of third countries in the field of response to cyberattacks with a potential impact on security in the Commission;

(5) regarding the receipt, assessment and distribution of intelligence concerning threats posed by terrorist and espionage activities affecting security in the Commission;

(6) regarding issues relating to classified information, as specified further in the Commission Decision (EU, Euratom) 2015/444 ([1]).

3. The Directorate-General for Human Resources and Security shall be responsible for the secure transmission of information performed under this Article, including the transmission of personal data.

Article 19

The Commission Security Expert Group (ComSEG)

A Commission Security Expert Group shall be established, with the mandate to advise the Commission, where appropriate, on matters relating to its internal security policy and more particularly on protection of EU classified information.

([1]) 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).

Article 20

Local Security Officers (LSOs)

1. Each Commission department or Cabinet shall appoint a Local Security Officer (LSO), who shall act as the principal point of contact between their service and the Directorate-General for Human Resources and Security on all matters related to security in the Commission. Where appropriate one or more deputy LSO may be appointed. The LSO shall be an official or a temporary agent.

2. As the main point of contact on security within his Commission department or Cabinet, the LSO shall, at regular intervals, report to the Directorate-General for Human Resources and Security and to his hierarchy on security issues involving his Commission department and, immediately, on any security incidents, including those where EUCI or sensitive non-classified information may have been compromised.

3. For matters related to security of communication and information systems, the LSO shall liaise with the Local Informatics Security Officer (LISO) of his Commission department, whose role and responsibilities are laid down in Decision C(2006) 3602.

4. He shall contribute to security training and awareness activities addressing the specific needs of staff, contractors and other individuals working under the authority of his Commission department.

5. The LSO may be assigned specific tasks in cases of major or immediate risks to security or of emergencies at the request of the Directorate-General for Human Resources and Security. The Director-General or the Director for Human Resources of the local Directorate-General of the LSO shall be informed about those specific tasks by the Directorate-General for Human Resources and Security.

6. The responsibilities of the LSO shall be without prejudice to the role and responsibilities assigned to Local Informatics Security Officers (LISOs), Health and Safety Managers, Registry Control Officers (RCOs) or any other function implying security or safety-related responsibilities. The LSO shall liaise with them in order to ensure a coherent and consistent approach to security and an efficient flow of information on matters related to security at the Commission.

7. The LSO shall have direct access to his Director-General or Head of Service, while informing his direct hierarchy. He shall hold a security authorisation to access EUCI, at least up to the level of SECRET UE/EU SECRET.

8. In order to promote the exchange of information and best practices, the Directorate-General for Human Resources and Security shall organise at least twice a year a LSO conference. Attendance by LSOs at these conferences shall be mandatory.

CHAPTER 5

IMPLEMENTATION

Article 21

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 Commission in favour of the Member of the Commission responsible for security matters, in full compliance with the internal rules of procedure.

2. After being empowered following the abovementioned Commission decision, the Member of the Commission responsible for security matters may develop security notices setting out security guidelines and best practices within the scope of this Decision and its implementing rules.

3. The Commission may delegate the tasks mentioned in the first and second paragraph of this Article to the Director-General for Human Resources and Security by a separate delegation decision, in full compliance with the internal rules of procedure.

CHAPTER 6

MISCELLANEOUS AND FINAL PROVISIONS

Article 22

Processing of personal data

1. The Commission 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 ([1]), 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 21, which shall lay down appropriate safeguards for data subjects.

3. The Director-General of the Directorate-General for Human Resources and Security 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 23

Transparency

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

Article 24

Repeal of previous decisions

Decision C(94) 2129 is repealed.

Article 25

Entry into force

This Decision shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 13 March 2015.

For the Commission
The President
Jean-Claude JUNCKER

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.