FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

MB DECISION

Decision n°:	2019/03
Subject:	DECISION OF THE MANAGEMENT BOARD OF THE FUNDAMENTAL RIGHTS AGENCY (FRA) ON SECURITY RULES AND RULES ON PROTECTING RESTREINT UE/EU RESTRICTED INFORMATION IN FRA

THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

HAVING REGARD to:

Having regard to Council Regulation (EC) No 168/2007 of 15 February 2007 FRA establishing a European Union Agency for Fundamental Rights (hereinafter "FRA")

WHEREAS:

FRA is requested by its stakeholders to undertake operational work that requires FRA to handle RESTREINT UE/EU RESTRICTED information.

Whereas the Commission has adopted Decision (EU, Euratom) No 2015/443 of 13 March 2015,

Whereas the objective of security within FRA is to enable FRA 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 timely delivery of security.

Within FRA, physical security aimed at protecting classified information is the application of physical and technical protective measures intended to prevent unauthorised access to EU classified information.

Whereas FRA should define sensitive non-classified information and the way it should be handled.

Whereas therefore there is a need for FRA to establish its rules on security and to update its rules on handling RESTREINT UE/EU RESTRICTED information.

HAS DECIDED AS FOLLOWS:

CHAPTER 1

GENERAL PROVISIONS

Article 1
Subject matter

1. This decision sets out the objectives, basic principles, organisation and responsibilities regarding security at FRA as well as the basic principles and minimum standards of security for protecting RESTREINT UE/EU RESTRICTED information.

2. This decision shall apply to all FRA's units and in all FRA's premises.

3. Notwithstanding any specific indications concerning particular groups of staff, this decision shall apply to all FRA's staff under the scope of the Staff Regulations of Officials of the European Union (the 'Staff Regulations') and of the Conditions of Employment of Other Servants of the European Union (the 'CEOS')[1], to national experts seconded to FRA (SNEs), to service providers and their staff, to trainees and to any individual with access to FRA's buildings or other assets, or to information handled by FRA.

4. The provisions of this decision shall be without prejudice to FRA's decision on the security of communication and information systems in FRA.

Article 2
Definitions

For the purposes of this decision, the following definitions apply:

(1) 'Accreditation' means the formal authorisation and approval granted to a communication and information system by the Security Accreditation Authority to process RESTREINT UE/EU RESTRICTED information in its operational environment, following the formal validation of the Security Plan and its correct implementation.
(2) 'Accreditation Process' means the necessary steps and tasks required prior to the accreditation by the Security Accreditation Authority. These steps and tasks shall be specified in an Accreditation Process Standard.
(3) 'Assets' means all movable and immovable property and possessions of FRA.
(4) 'FRA's unit' means a unit, group or section of FRA.
(5) '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. This definition includes business applications, shared IT services, outsources systems, and end-user devices.
(6) '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 FRA regardless of its origin.

---

[1] Laid down by 14.6.62 OFFICIAL JOURNAL OF THE EUROPEAN COMMUNITIES 1385/62, Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community.

(7) 'Cryptographic (Crypto) material' means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material.
(8) 'Data' means information in a form that allows it to be communicated, recorded, processed or destroyed.
(9) 'Declassification' means the removal of any security classification.
(10) 'Defence in depth' means the application of a range of security measures organised as multiple layers of defence.
(11) 'Document' means any recorded information regardless of its physical form or characteristics.
(12) 'Handling' of RESTREINT UE/EU RESTRICTED information means all possible actions to which the information may be subject throughout its life-cycle. It comprises its creation, recording, processing, carriage, declassification and destruction. In relation to Communication and Information Systems, it also comprises its collection, display, transmission and storage.
(13) 'Holder' means a duly authorised individual with an established need-to-know who is in possession of an item of RESTREINT UE/EU RESTRICTED information and is accordingly responsible for protecting it.
(14) 'Implementing rules' means any set of rules or security notices adopted in accordance with Article 65.
(15) 'Material' means any medium or data carrier.
(16) 'Originator' means the Union institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the Union's structures.
(17) 'Personal data' means personal data as defined in Article 3(1) of Regulation (EU) No 2018/1725[2] of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC
(18) 'Premises' shall mean any immovable or assimilated property and possessions of FRA.
(19) 'Prevention of risk' shall mean security measures that can reasonably be expected to impede, delay or stop a risk to security.
(20) 'Residual risk' means the risk which remains after security measures have been implemented, given that not all threats are countered and not all vulnerabilities can be eliminated.
(21) 'Risk' means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact.
(22) 'Risk acceptance' is the decision to agree to the further existence of a residual risk after risk treatment.
(23) 'Risk assessment' consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact.
(24) 'Risk communication' consists of developing awareness of risks among CIS user communities, informing approval authorities of such risks and reporting them to operating authorities.
(25) 'Risk to security' means the combination of the threat level, the level of vulnerability and the possible impact of an event.
(26) 'Risk treatment' consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk.

---

[2] OJ L 295, 21.11.2018, p39.

(27) 'Security Group' means a group advising the Director, where appropriate, on matters relating to its internal security policy and more particularly on the protection of RESTREINT UE/EU RESTRICTED information.

(28) 'Security in FRA' means the security of persons, assets and information in FRA, 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 FRA's operations.

(29) 'Security measure' means any measure taken in accordance with this decision for the purposes of controlling risks to security.

(30) 'Security Officer' means the officer with general responsibility for security in FRA under the authority and responsibility of the Director.

(31) 'Security risk management process' means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of any of the systems it uses. It covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication.

(32) 'Staff Regulations' means the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community, as laid down by Regulation No 31 (EEC), 11 (EAEC).

(33) 'Threat' means a potential cause of an unwanted incident which may result in harm to an organisation or any of the systems it uses; such threats may be accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods.

(34) 'Threat to security' means an event or agent that can reasonably be expected to adversely affect security if not responded to and controlled. An 'Immediate threat to security' means a threat to security which occurs with no or with extremely short advance warning; and a '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 FRA.

(35) 'Vulnerability' means a weakness of any nature that can be exploited by one or more threats. A vulnerability may be an omission or it may relate to a weakness in controls in terms of their strength, completeness or consistency and may be of a technical, procedural, physical, organisational or operational nature.

CHAPTER 2

PRINCIPLES

Article 3
Principles for security in FRA

1. In implementing this decision, FRA 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 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 65(2) providing guidance in this respect shall be issued.

2. Security in FRA 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.

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. FRA's units shall ensure that security issues are taken into account from the start of the development and implementation of FRA's policies, decisions, programmes, projects and activities for which they are responsible.

6. FRA shall, where appropriate, seek cooperation with the competent authorities of the host state, of Member States 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 and 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, given their current duties, may be entrusted with the power to take one or several of the following measures:

   (a) Conduct security inquiries as referred to in Article 13;
   (b) 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 persons 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, FRA 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 transmitter information on an individual to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Regulation (EU) 2016/679 of the European Parliament[3], in accordance with Article 9 of Regulation (EU) No 2018/1725;
   (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:
      i. the envisaged measures against the individual posing the threat to security cannot be taken or are not likely to be effective;
      ii. FRA cannot control the threat to security by its own actions or cannot do so in a timely manner;

---

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the European Union, L 119, 4 May 2016)

iii. the measure does not constitute a disproportionate danger for the other individual and his rights.

2. The Security Officer 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 FRA, taking into account security and safety requirements.

2. In case of major risks to security, the Security Group shall provide appropriate security measures for FRA's staff and 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, FRA may order the evacuation or lockdown (invacuation) of its premises.

4. Victims of accidents or attacks within FRA's premises shall receive assistance.

5. In order to prevent and control risks to security, staff duly mandated for the specific task may carry out background checks of persons falling under the scope of this decision, so as to determine whether giving such persons access to FRA's premises or information presents a threat to security. For that purpose, and in compliance with Regulation (EU) No 2018/1725 and the provisions referred to under Article 3, the mandated staff concerned may:

(a) use any source of information available to FRA, taking into account the reliability of the source of information;
(b) access the personnel file or data FRA 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 FRA 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 FRA's 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 66(2) hereunder and other information sources.

4. Physical security shall include:

- an access policy applicable to any person or vehicle requiring access to FRA's 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 FRA's 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 FRA's premises.

Article 9
Security measures regarding information

1. Security of information covers all information handled by FRA.

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 to:

(a) 'RESTREINT UE/EU RESTRICTED information' as defined in Article 21;
(b) 'Sensitive non-classified information' as defined in Article 18.

6. Any individual who is responsible for compromising or losing RESTREINT UE/EU RESTRICTED 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 used by FRA shall comply with FRA's Information Systems Security Policy, as set out in FRA's policies on[4] the security of communication and information systems in FRA, its implementing rules and corresponding security standards.

2. FRA's services which own, manage or operate CIS shall only allow 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 Commission Decision 2017/46 of 10 January 2017[5] on the security of communication and information systems in the European Commission, its implementing rules and corresponding security standards. FRA 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 Security Officer shall in particular be responsible for conducting forensic technical analysis in cooperation with the competent units at FRA 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 security in FRA 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 FRA's premises, escorting persons from FRA's premises, banning persons from the FRA'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 the removal, seizure and disposal of objects;
   (d) searching of FRA's premises, including of offices, within such premises;
   (e) searching of CIS and equipment, telephone and telecommunications traffic data, log files, user accounts, etc.;

---

4 PO.ICTF.007-01 ICT Security and Data Management policy and PO.ICT.001-03 ICT Policy

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

(f) other specific security measures with similar effect in order to prevent or control risks to security, in particular in the context of FRA's rights as an employer in accordance with the applicable national laws;
(g) interview those who could provide useful information with regard to the inquiry.

2. Under exceptional circumstances, staff members of the Security Group, 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 request the Director to confirm the measures taken and authorise 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 (EUC) No 2018/1725, and to allow 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), FRA 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 FRA, including suspected criminal offences;
(b) in case of potential leakage, mishandling or compromise of sensitive non-classified information, RESTREINT UE/EU RESTRICTED;
(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 who will also be the recipient of the inquiry report.

3. 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.

4. 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 FRA's premises or involving persons referred to in Article 1(3) either as the victim or the perpetrator of such offences.

5. The Security Officer 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 Security Officer may, where appropriate or required, provide support to the authorities of the host Member State or any other Member State concerned.

6. In the case of serious cyber-incidents, the IT unit shall collaborate closely with the Security Officer to provide support on all technical matters. The Director shall decide, in consultation with the Head of the Corporate Services Unit, when it is appropriate to inform the competent authorities of the host country or any other Member State concerned. The incident coordination services of the 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.

7. Security inquiries shall be documented in accordance with FRA's procedures.

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

1. Where the Security Group conducts security inquiries, as referred to in Article 13, and if these enquiries fall within the competences of the European Anti-Fraud Office (OLAF), it shall liaise with OLAF at once with a view, in particular, not to compromise later steps by OLAF. Where appropriate, the Director shall invite OLAF 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 as laid down in the rules governing this body. The Security Group may be requested to provide technical assistance for inquiries initiated by OLAF.

3. The Security Officer may be asked to assist OLAF's agents when they access the FRA's 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[6], in order to facilitate their tasks.

4. Where a case may fall within the competence of both the Security Group and OLAF, the Security Officer shall without delay report to the Director who 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.

---

[6] 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).

Article 15
Alert states and management of crisis situations

1. The Director shall be responsible for putting in place appropriate alert state measures in anticipation of or in response to threats and incidents affecting security at FRA, 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 state levels shall be defined in close cooperation with the competent services of other Union institutions, agencies and bodies, and of the Member State hosting FRA's premises.

3. The Security Group shall be the contact point for alert states and management of crisis situations.

CHAPTER 4

ORGANISATION

Article 16
General responsibilities of FRA's services

1. The security responsibilities of FRA referred to in this decision shall be exercised by the Security Officer under the authority and responsibility of the Director.

2. The specific arrangements as regards cyber-security are defined in FRA's policies on the security of communication and information systems in FRA.

3. The responsibilities for implementing this decision and its implementing rules and for day-to-day compliance may be delegated to other units at FRA.

Article 17
Security Officer and Security Group

1. FRA shall appoint a Security Officer, who shall act as the principal point of contact on all matters related to security in FRA. The Security Officer shall be an official or a temporary agent.
2. As the main point of contact on security within FRA, the Security Officer shall, at regular intervals, report to the Director and to his/her hierarchy on security issues involving the units and, immediately, on any security incidents, including those where RESTREINT UE/EU RESTRICTED or sensitive non-classified information may have been compromised.
3. For matters related to the security of communication and information systems, the Security Officer shall liaise with the Local Informatics Security Officer of FRA, whose role and responsibilities are laid down in the Decision concerning the security of communication and information systems in FRA.
4. The Security Officer should liaise, where applicable, with the police and security authorities of Union institutions.
5. The Security Officer may be assigned specific tasks in cases of major or immediate risks to security or of emergencies at the request of the Director.
6. The responsibilities of the Security Officer shall be without prejudice to the role and responsibilities assigned to the Local Informatics Security Officer or any other function implying security or safety-related responsibilities. The Security Officer 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 FRA.
7. The Security Officer shall have direct access to the Director, while informing his direct hierarchy.
8. FRA shall establish a Security Group, who shall advise the Director, where appropriate, on matters relating to its internal security policy and more particularly on protection of RESTREINT UE/EU RESTRICTED information.
9. The Security Group is recommended to consist of the Head of Corporate Services Unit, the Security Officer and the Local Informatics Security Officer.
10. Where appropriate the Security Group may involve any other function implying security or safety-related responsibilities including security inquiries.
11. Security inquiries shall be conducted only by dedicated members of staff of the Security Group, duly mandated in accordance with Article 5

CHAPTER 5

SENSITIVE NON-CLASSIFIED INFORMATION

Article 18
Definition of sensitive non-classified information

'Sensitive non-classified information' is understood as all information or material restricted to a limited number of persons (on a need-to-know or need for access basis), whereby its disclosure to non-authorised persons would cause a moderate level of harm to FRA, EU institutions, Member States or bodies and agencies for which FRA works, but not to such a serious level as to merit being classified as RESTREINT UE/EU RESTRICTED classification within the meaning of Article 21. FRA must protect this information or material 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[7] of the European Parliament and of the Council 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 (EU) No 2018/1725.

Article 19
Protection, handling and storage of sensitive non-classified information

1. Sensitive non-classified information' must be protected by appropriate security measures. To this end, the Management Board requests FRA's Director to establish the appropriate implementing rules for protecting sensitive non-classified information.

2. 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 Security Officer. When handled or stored on Communication and Information Systems, such information shall be protected in compliance with FRA's decision on the security of communication and information systems in FRA, its implementing rules and corresponding standards.

3. If it is necessary for FRA to exchange sensitive non-classified information with a third party outside the Agency, a Memorandum of Understanding shall be drawn up between the FRA and the external party. The Memorandum shall set out the handling instructions for all such information exchanged between them. The Commission shall be consulted prior to the conclusion of any such MoUs. Each entity shall remain responsible for compliance by its own staff handling the information exchanged.

---

7 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.

CHAPTER 6

CLASSIFICATION AND MARKINGS

Article 20
Authorisation

The Management Board hereby decides to authorise FRA to handle classified information up to the level of RESTREINT UE/EU RESTRICTED.

Article 21
Definition of RESTREINT UE/EU RESTRICTED information

1. RESTREINT UE/EU RESTRICTED information means information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

Article 22
Classification and markings

1. Information shall be classified where it requires protection with regard to its confidentiality in accordance with Article 21.

2. The originator of a document shall be responsible for classifying it in accordance with the relevant implementing rules, standards and guidelines regarding classification, and for the initial dissemination of the information.

3. Classifying a document shall involve an assessment and a decision by the originator as to whether the disclosure of the document to unauthorised persons would cause a degree of prejudice to the interests of the European Union or of one or more of the Member States. If drafters are in doubt whether the document they are drafting warrants a RESTREINT UE/EU RESTRICTED marking they should consult the Director or Head of Unit responsible.

4. While not an exhaustive list, a document shall be classified as at least RESTREINT UE/EU RESTRICTED if its unauthorised disclosure could, for example:

   (a) adversely affect diplomatic relations;

   (b) cause substantial distress to individuals;

   (c) make it more difficult to maintain the operational effectiveness or security of Member States' or other contributors' deployed personnel;

   (d) breach undertakings to maintain the confidence of information provided by third parties;

   (e) prejudice the investigation of or facilitate crime;

   (f) disadvantage EU or Member States in commercial or policy negotiations with others;

(g) impede the effective development or operation of EU policies;

(h) undermine the proper management of the EU and its missions in general; or

(i) lead to the discovery of information classified at a higher level.

5. Originators may decide to attribute a standard classification level to categories of information which they create on a regular basis. However, they shall ensure that in so doing they do not overclassify or underclassify individual pieces of information.6. The security classification marking "RESTREINT UE/EU RESTRICTED" shall be clearly and correctly indicated, regardless of whether the classified information is on paper, oral, electronic or in any other form. The marking shall be in upper case, with no spaces either side of the forward slash, in both languages (French first) and shall never be translated.

7. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may or may not require classification and shall be marked accordingly, including when stored in electronic form.

8. The complete document or file shall be classified if it contains any classified components.

9. In order to enable originator control to be applied correctly, originators of RESTREINT UE/EU RESTRICTED documents shall, to the extent possible, keep a record of any classified sources used for producing the classified document, including if the sources are originally from EU Member States, international organisations or third states.

Article 23
Other markings

In addition to the security classification marking, the document may bear additional markings, such as:

(a) an identifier to designate the originator;
(b) any caveats, code-words or acronyms specifying the field of activity to which the document relates, a particular distribution on a need-to-know basis or restrictions on use;
(c) releasability markings;
(d) where applicable, the date or specific event after which it may be declassified.

Article 24
Abbreviated classification marking

1. A standardised abbreviated classification marking may be used to indicate the classification level of individual paragraphs of a text. The abbreviation may be used where the full classification marking cannot be inserted, for example on a small portable device. The abbreviation shall not replace the full classification marking in the header or footer of the document.

2. The following standard abbreviation may be used within RESTREINT UE/EU RESTRICTED documents to indicate the classification level of sections or blocks of text of less than a single page:

R-UE/EU-R

Article 25
Classification management

1. All FRA's units shall ensure that any classified information they create is appropriately classified, clearly identified as RESTREINT UE/EU RESTRICTED and retains its classification level for only as long as necessary.

2. Whenever possible, any indications for declassification shall be affixed on the first page of the document at the time it is created. For example:

RESTREINT UE/EU RESTRICTED
until [dd.mm.yyyy]

3. Without prejudice to Article 60 below, EUCI shall not be declassified nor shall the security classification marking be removed without the prior written consent of the originator.

Article 26
Protection of classified information

1. RESTREINT UE/EU RESTRICTED information shall be protected in accordance with this decision and its implementing rules.

2. The holder of any RESTREINT UE/EU RESTRICTED information shall be responsible for protecting it, in accordance with this decision and its implementing rules, according to the rules laid out in Chapter 9 below.

Article 27
Security risk management

1. Security measures for protecting RESTREINT UE/EU RESTRICTED information throughout its life-cycle shall be commensurate in particular with its security classification, the form and the volume of the information or material, the location and construction of facilities housing the classified information and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.

2. Contingency plans shall take account of the need to protect RESTREINT UE/EU RESTRICTED information during emergency situations in order to prevent unauthorised access, disclosure or loss of integrity or availability.

3. Preventive and recovery measures to minimise the impact of major failures or incidents on the handling and storage of RESTREINT UE/EU RESTRICTED information shall be included in all services' business continuity plans.

Article 28
Implementation of this decision

1. Where necessary, implementing rules to supplement or support this decision shall be adopted in accordance with Article 65below.

2. FRA's units shall take all the necessary measures falling under their responsibility in order to ensure that, when handling or storing RESTREINT UE/EU RESTRICTED or sensitive non-classified information, this decision and the relevant implementing rules are applied.

3. Within FRA, the Security Officer shall have the following overall responsibilities for protecting RESTREINT UE/EU RESTRICTED information in accordance with this decision, in close cooperation with the Director:

   (a) contributing to security training and awareness briefings addressing the specific needs of staff, contractors and other individuals working under the authority of FRA;
   (b) reporting on breaches of security and compromise of RESTREINT UE/EU RESTRICTED information;
   (c) holding spare keys;
   (d) assuming other tasks related to the protection of RESTREINT UE/EU RESTRICTED information or defined by the implementing rules.

Article 29
Breaches of security and compromise of RESTREINT UE/EU RESTRICTED information

1. A breach of security occurs as the result of an act or omission by an individual which is contrary to the security rules laid down in this decision and its implementing rules.

2. Compromise of RESTREINT UE/EU RESTRICTED information occurs when, as a result of a breach of security, it has wholly or in part been disclosed to unauthorised persons.

3. Any breach or suspected breach of security shall be reported immediately to the Security Officer.

4. Where it is known or where there are reasonable grounds to assume that RESTREINT UE/EU RESTRICTED information has been compromised or lost, a security inquiry shall be conducted in accordance with Article 13.

5. All appropriate measures shall be taken to:

   (a) inform the originator;
   (b) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts;
   (c) assess the potential damage caused to the interests of FRA, the Union or one or more of the Member States;
   (d) take appropriate measures to prevent a recurrence; and
   (e) notify the appropriate authorities of the action taken.

6. Any individual who is responsible for a breach of the security rules laid down in this decision may be liable to disciplinary action in accordance with the Staff Regulations. Any individual who is responsible for compromising or losing RESTREINT UE/EU

RESTRICTED information shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

CHAPTER 7

PERSONNEL SECURITY

Article 30
Basic Principles

1. An individual shall only be granted access to RESTREINT UE/EU RESTRICTED information after:

(1) his need-to-know has been determined;
(2) he has been briefed on the security rules for protecting RESTREINT UE/EU RESTRICTED information and the relevant security standards and guidelines, and has acknowledged his responsibilities with regard to protecting such information.

Article 31
Security briefings

1. After having participated in the security briefing organised by the Security Officer, all individuals shall acknowledge in writing that they have understood their obligations in respect of protecting RESTREINT UE/EU RESTRICTED information and the consequences if it is compromised. A record of such a written acknowledgement shall be kept by the Security Officer.

2. All individuals who are required to handle RESTREINT UE/EU RESTRICTED information, shall initially be made aware, and periodically briefed on the threats to security and must report immediately to the Security Officer any approach or activity that they consider suspicious or unusual.

3. All individuals who cease to be employed in duties requiring access to RESTREINT UE/EU RESTRICTED information shall be made aware of, and where appropriate acknowledge in writing, their obligations, in accordance with Article 17 (2) of the Staff Regulations, in respect of the continued protection of classified information.

Article 32
Potential Access to RESTREINT UE/EU RESTRICTED information

Couriers, guards and escorts shall be briefed on security procedures for protecting RESTREINT UE/EU RESTRICTED information and be instructed on their duties for protecting such information entrusted to them.

CHAPTER 8

PHYSICAL SECURITY AIMED AT PROTECTING CLASSIFIED INFORMATION

Article 33
Basic principles

1. Physical security measures shall be designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions and to allow for segregation of personnel in their access to RESTREINT UE/EU RESTRICTED information on a need-to-know basis. Such measures shall be determined based on a risk management process, in accordance with this decision and its implementing rules.

2. In particular, physical security measures shall be designed to prevent unauthorised access to RESTREINT UE/EU RESTRICTED information by:

   (a) ensuring that RESTREINT UE/EU RESTRICTED information is handled and stored in an appropriate manner;
   (b) allowing for segregation of personnel in terms of access to RESTREINT UE/EU RESTRICTED information on the basis of their need-to-know;
   (c) deterring, impeding and detecting unauthorised actions; and
   (d) denying or delaying surreptitious or forced entry by intruders.

3. Physical security measures shall be put in place for all premises, buildings, offices, rooms and other areas in which RESTREINT UE/EU RESTRICTED information is handled or stored, including areas housing communication and information systems as referred to in Chapter 11.

Article 34
Physical security requirements and measures

1. Physical security measures shall be selected on the basis of a threat assessment made by the Security Group, where appropriate in consultation with other units at FRA, Union institutions, agencies or bodies and/or competent authorities in the Member States. FRA shall apply a risk management process for protecting RESTREINT UE/EU RESTRICTED information on its premises to ensure that a commensurate level of physical protection is afforded against the assessed risk. The risk management process shall take account of all relevant factors, in particular:

   (a) the classification level of the information;
   (b) the form and volume of the RESTREINT UE/EU RESTRICTED information, bearing in mind that large quantities or a compilation of classified information may require more stringent protective measures to be applied;
   (c) the surrounding environment and structure of the buildings or areas housing RESTREINT UE/EU RESTRICTED information; and
   (d) the assessed threat from intelligence services which target the Union, its institutions, bodies or agencies, or the Member States and from sabotage, terrorist, subversive or other criminal activities.

2. The Security Group, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. To that effect, the Security Group shall develop minimum standards, norms and criteria which shall be defined in the implementing rules.

3. The Security Group Officer is authorised to conduct entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of RESTREINT UE/EU RESTRICTED information from premises or buildings.

4. When RESTREINT UE/EU RESTRICTED information is at risk of being overlooked, even accidentally, FRA's units concerned shall take the appropriate measures, as defined by the Security Group Officer, to counter this risk.

5. For new facilities, physical security requirements and their functional specifications shall be defined in consent with the Security Group Officer as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented in accordance with the minimum standards, norms and criteria set out in the implementing rules.

Article 35
Equipment for the physical protection of RESTREINT UE/EU RESTRICTED information

1. Physically protected areas shall be established and designated as Administrative Areas for the physical protection of RESTREINT UE/EU RESTRICTED information.

2. The Security Group Officer shall establish that an area meets the requirements to be designated as an Administrative Area.

3. For Administrative Areas:

   (a) a visibly defined perimeter shall be established which allows individuals and, where possible, vehicles to be checked;
   (b) unescorted access shall be granted only to individuals who are duly authorised by the Security Officer; and
   (c) all other individuals shall be escorted at all times or be subject to equivalent controls.

Article 36
Physical protective measures for handling and storing RESTREINT UE/EU RESTRICTED information

1. EUCI which is classified RESTREINT UE/EU RESTRICTED may be handled:

   (a) in an Administrative Area provided the it is protected from access by unauthorised individuals, or
   (b) outside an Administrative Area temporarily, and only for the time necessary, provided the holder carries it in accordance with Articles 41 and 42 and has undertaken to comply with compensatory measures, set out in the implementing measures, to ensure that the RESTREINT UE/EU RESTRICTED information is protected from access by unauthorised persons.

2. When handling RESTREINT UE/EU RESTRICTED information, the holder shall comply with at least the following:

   - The documents shall be stowed in appropriate locked furniture when they are not being read or discussed.
   - The doors to the room shall be closed while the document is being read or discussed.

- Screens displaying RESTREINT UE/EU RESTRICTED information shall be permanently turned away from windows and doors to prevent overlooking.
- The details of the document shall not be discussed over the phone on a non-secured line or in an unencrypted e-mail.
- The document shall not be photocopied or scanned on non-accredited equipment.
- The holder shall not throw the classified document away but shall return it for storage in an Administrative Area, or for destruction in an approved shredder.

3. RESTREINT UE/EU RESTRICTED information shall be stored in suitable locked office furniture in an Administrative Area.

Article 37
Management of keys and any combinations used for protecting EUCI

1. Procedures for managing keys and any combination settings for offices, rooms, and security containers shall be laid down in the implementing rules according to Article 65below. Such procedures shall be intended to guard against unauthorised access.

2. Where applicable, combination settings shall be committed to memory by the smallest possible number of individuals needing to know them. Combination settings for security containers storing EUCI shall be changed:

(a) on receipt of a new container;
(b) whenever there is a change in personnel knowing the combination;
(c) whenever a compromise has occurred or is suspected;
(d) when a lock has undergone maintenance or repair; and
(e) at least every 12 months.

CHAPTER 9

MANAGEMENT OF EU CLASSIFIED INFORMATION

Article 38
Basic principles

1. All EUCI documents should be managed in compliance with FRA's policy on document management and consequently should be recorded, filed, preserved and finally eliminated, sampled or transferred to the Historical Archives in accordance with the common Commission-level retention list for European Commission files, applied by analogy.

2. FRA's units and premises where EUCI is handled or stored shall be subject to regular inspection by the Security Officer.

3. EUCI shall be conveyed between services and premises outside physically protected areas as follows:

   (a) as a general rule, EUCI shall be transmitted by electronic means protected by cryptographic products approved in accordance with Chapter 11;
   (b) when the means referred to in point (a) are not used, EUCI shall be carried either:
      (i) on electronic media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products approved in accordance with Chapter 11; or
      (ii) in all other cases, as prescribed in the implementing rules.

Article 39
Creation of EUCI

1. As a general rule, RESTREINT UE/EU RESTRICTED documents shall be created using electronic means. When creating an EU classified document:

   (a) each page shall be marked clearly with the classification level;
   (b) each page shall be numbered;
   (c) the document shall bear a reference number and a subject, which is not itself classified information, unless it is marked as such;
   (d) the document shall have a date on it.

Article 40
Copying and translating EU classified documents

1. RESTREINT UE/EU RESTRICTED information may be copied or translated on instruction from the holder.

2. The security measures applicable to the original document shall apply to copies and translations thereof. Extracts shall be classified at the same level as the original full document, unless the originator has explicitly specified otherwise.

Article 41
Carriage of EUCI

1. As a general rule, RESTREINT UE/EU RESTRICTED information that needs to be conveyed shall be transmitted electronically by duly accredited means and/or protected by approved cryptographic products. However, depending on the means available and/or the particular circumstances, RESTREINT UE/EU RESTRICTED information may be physically carried by hand.

2. Staff may carry RESTREINT UE/EU RESTRICTED information in the form of hard copy documents or removable electronic media, such as USB sticks or CD-ROMs. Removable storage media shall be marked with the appropriate classification marking. The use of removable storage media to transfer RESTREINT UE/EU RESTRICTED information shall be given preference to sending physical documents.

3. Only USB sticks provided by FRA shall be used. Personal USB sticks or those given freely at conferences, seminars etc. shall not be used for transferring classified information. RESTREINT UE/EU RESTRICTED information on removable electronic media that is not protected by an encryption product that has been approved by the FRA Security Authority shall be handled in the same manner as hard copy. When EUCI is carried on electronic media, the protective measures may be supplemented by appropriate technical countermeasures so as to minimise the risk of loss or compromise.

4. A consignment may contain more than one piece of RESTREINT UE/EU RESTRICTED information, provided the need-to-know principle is respected. Only the classified documents to be released shall be stored on the media. In this context, all the classified information on a single USB stick, for instance, would have to be intended for the same recipient. The sender shall bear in mind that large amounts of classified information stored on such devices may warrant a higher classification level.

5. EUCI shall be carried in such a way as to protect it from unauthorised disclosure during its carriage.

6. Carriage of EUCI shall be subject to the protective measures, which shall:

- be commensurate with the level of classification of the EUCI carried, and
- be adapted to the specific conditions of its carriage, in particular depending on whether EUCI is carried:
  - within FRA's building,
  - within the Union, and
  - be adapted to the nature and form of the EUCI.

7. These protective measures shall be laid down in detail in the implementing rules.

8. The implementing rules shall include provisions commensurate with the level of EUCI, regarding:

— the type of carriage, such as hand carriage, carriage by diplomatic courier, carriage by postal services or commercial courier services,
— packaging of EUCI,
— technical countermeasures for EUCI carried on electronic media,
— any other procedural, physical or electronic measure,
— use of security personnel.

9. The packaging used shall ensure that the contents are covered from view. As a rule, outside a building or group of self-contained FRA buildings RESTREINT UE/EU RESTRICTED information shall be carried in opaque packaging, such as envelopes, opaque folders or a briefcase. The outside of the packaging shall not bear any indication of the nature/classification level of its contents. If used, the inner layer of packaging shall be marked as RESTREINT UE/EU RESTRICTED. Both layers shall state the intended recipient's name, job title and address, as well as a return address in case delivery cannot be made.

10. Staff or couriers hand-carrying RESTREINT UE/EU RESTRICTED information shall report any security incidents for subsequent investigation.

Article 42
Carriage of RESTREINT UE/EU RESTRICTED information within the EU

1. RESTREINT UE/EU RESTRICTED information may be hand carried by FRA staff anywhere within the EU provided they comply with the following instructions:

(a) the envelope/packaging used must be opaque and bear no indication of the classified nature of its contents;

(b) the RESTREINT UE/EU RESTRICTED information must not leave the possession of the bearer; and

(c) the envelope/package must not be opened *en route* and the information must not be read in public places.

2. Alternatively, FRA staff wishing to send RESTREINT UE/EU RESTRICTED information to other locations in the EU may arrange for it to be conveyed by one of the following means:

- national postal services that track the consignment or certain commercial courier services (see below) and guarantee personal hand carriage, provided that they meet the requirements stipulated below on .
- government or diplomatic courier/pouch, as appropriate.

Article 43
Carriage of RESTREINT UE/EU RESTRICTED information from or to the territory of a third state

1. Information classified RESTREINT UE/EU RESTRICTED may be hand-carried by staff from the territory of the EU to the territory of a third state.

2. Alternatively, the document may be sent via:

- carriage by postal services that track the consignment or commercial courier services that guarantee personal hand carriage; or

- carriage by diplomatic courier, as appropriate.

3. When hand-carrying either paper-based information or encrypted removable data storage media classified as RESTREINT UE/EU RESTRICTED, staff shall comply with the following additional measures:

   - when travelling by public transport the classified information shall be placed in a briefcase or bag that is kept in the bearer's personal custody. It shall not be consigned to a baggage hold;
   - the inner package shall bear an official seal so as to indicate that it is an official consignment and should not undergo security scrutiny; and
   - the bearer should carry a courier certificate.

Article 44

Transport of RESTREINT UE/EU RESTRICTED documents by commercial couriers

1. For the purposes of this Decision, 'commercial couriers' include national postal services, privatised national postal services and commercial courier companies that offer a service where information is delivered for a fee and is either personally hand carried or tracked.

2. The sanctions applicable to the company in the case of a breach of security shall be specified in the contract.

3. Courier companies may use the services of a sub-contractor, however the responsibility for fulfilling the requirements set out in these implementing rules shall remain with the courier company.

4. When classified consignments are being prepared the sender shall bear in mind that commercial courier services might deliver the RESTREINT UE/EU RESTRICTED consignments to the intended recipient, a duly authorised substitute, the registry control officer or his/her duly authorised substitute or a receptionist. To mitigate the risk that the consignment may not reach the intended recipient on both the outer and inner layers of packaging of the consignment a return address shall therefore be included.

5. Services offered by commercial couriers providing electronic transmission of registered delivery documents shall not be permitted for RESTREINT-UE/EU-RESTRICTED information.

Article 45

Other specific handling conditions

1. Any carriage conditions set out in an Administrative Arrangement shall be complied with. If in doubt, staff shall consult the Security Officer who may consult the Security Directorate in the Directorate-General for Human Resources and Security.

2. RESTREINT UE/EU RESTRICTED information contained in hand-carried encrypted media that has been approved needs to be packaged in an opaque envelope for addressing purposes, and also as the medium bears an explicit security classification marking. The electronic medium may require additional physical protection measures.

CHAPTER 10

CLASSIFIED MEETINGS

Article 46
Preparing for a RESTREINT UE/EU RESTRICTED meeting

1. As a general rule agendas should be not classified. If the agenda of a meeting quotes classified documents, the agenda itself shall not automatically be classified. Agenda items shall be worded in a way that avoids jeopardising the protection of the EU or one or more of the Member States' interests.
2. RESTREINT UE/EU RESTRICTED items should be grouped consecutively on the agenda in order to facilitate the smooth functioning of the meeting, as only persons with a need-to-know may be present during discussions of classified items.
3. If electronic files containing RESTREINT UE/EU RESTRICTED information are to be attached to the agenda, it is mandatory to protect them with an approved cryptographic product.
4. Meeting organisers shall remind participants that any comments sent in on a RESTREINT UE/EU RESTRICTED agenda item must not be sent through ordinary open e-mails, or through other means that have not been duly accredited.
5. The invitation itself shall forewarn the participants that the meeting will discuss classified topics, and that corresponding security measures will apply.
6. Meeting organisers shall prepare the complete list of external participants prior to the meeting.

Article 47
Electronic equipment in a RESTREINT UE/EU RESTRICTED meeting room

1. Any presentation given by electronic means that displays RESTRICTED EU/EU RESTRICTED information may only be made using an accredited IT system.
2. The use of wireless microphones in RESTREINT UE/EU RESTRICTED meetings is prohibited.

Article 48
Portable electronic devices inside a RESTREINT UE/EU RESTRICTED meeting

The invitation or note on the agenda itself shall remind participants that electronic devices shall be switched off during the discussion of RESTREINT UE/EU RESTRICTED items.

Article 49
RESTREINT UE/EU RESTRICTED documents in the meeting

1. Only the necessary number of documents shall be given to participants and interpreters, as appropriate, at the start of the meeting.
2. At the end of the meeting, the delegates shall be reminded not to leave any classified documents lying unattended in the room.
3. RESTREINT UE/EU RESTRICTED documents not taken away by the participants at the end of the meeting shall be collected by the meeting organisers and shredded in appropriate shredders.

Article 50
Procedures to be followed during a RESTREINT UE/EU RESTRICTED meeting

1. At the start of the classified discussion, the Chair shall remind the meeting that it is moving into classified mode. The doors and blinds shall be closed, and the loudspeakers and any portable electronic devices shall be switched off.

2. If RESTREINT UE/EU RESTRICTED documents are to be left unattended while the meeting breaks, the room shall be locked and guarded.

3. The list of attendants and an outline of any classified information released orally to third states or international organisations shall be noted down during the meeting in order to be recorded in the outcome of proceedings.

Article 51
Interpreters and translators

Only interpreters and translators under the scope of the Staff Regulations and of the Conditions of Employment of other servants of the European Union or who have a contractual link to FRA shall have access to RESTREINT UE/EU RESTRICTED information.

CHAPTER 11

PROTECTION OF EU CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS

Article 52
Basic principles of Information Assurance

1. Information Assurance in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

2. Effective Information Assurance shall ensure appropriate levels of:

Authenticity: the guarantee that information is genuine and from bona fide sources;
Availability: the property of being accessible and usable upon request by an authorised entity;
Confidentiality: the property that information is not disclosed to unauthorised individuals, entities or processes;
Integrity: the property of safeguarding the accuracy and completeness of assets and information;
Non-repudiation: the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.

3. Information Assurance shall be based on a risk management process.

Article 53
CIS handling EUCI

1. CIS shall handle RESTREINT UE/EU RESTRICTED information in accordance with the concept of Information Assurance.

2. For CIS handling RESTREINT UE/EU RESTRICTED information, compliance with FRA's information systems security policy, as referred to in the policies on the security of communication and information systems in FRA, implies that:

(a) the Plan-Do-Check-Act approach shall be applied for the implementation of the information systems security policy during the full life-cycle of the information system;
(b) the security needs must be identified through a business impact assessment;
(c) the information system and the data therein must undergo a formal asset classification;
(d) all mandatory security measures as determined by the policy on the security of information systems must be implemented;
(e) a risk management process must be applied, consisting of the following steps: threat and vulnerability identification, risk assessment, risk treatment, risk acceptance and risk communication;
(f) a security plan, including the Security Policy and the Security Operating Procedures, is defined, implemented, checked and reviewed.

3. All staff involved in the design, development, testing, operation, management or usage of CIS handling RESTREINT UE/EU RESTRICTED information shall notify to the Security Accreditation Authority all potential security weaknesses, incidents, breaches of security or compromise which may have an impact on the protection of the CIS and/or the RESTREINT UE/EU RESTRICTED information therein. The Director shall act as FRA's Security Accreditation Authority.

4. Where the protection of RESTREINT UE/EU RESTRICTED information is provided by cryptographic products, such products shall be approved as follows:

   (a) preference shall be given to products which have been approved by the Council or by the Secretary-General of the Council in its function as crypto approval authority of the Council, upon recommendation by the Commission's Security Expert Group;
   (b) where warranted on specific operational grounds, FRA's Crypto Approval Authority may, upon recommendation by the FRA Security Authority, waive the requirements referred to under a) and grant an interim approval for a specific period.

5. During transmission, processing and storage of RESTREINT UE/EU RESTRICTED information by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or in specific technical configurations after approval by the Crypto Approval Authority.

6. FRA's Security Group shall assume the following functions:

   - Information Assurance Authority,
   - Crypto Approval Authority,
   - Crypto Distribution Authority,

7. The Director shall appoint for each system the Information Assurance Operational Authority.

8. The responsibilities of the functions described in paragraphs 6 and 7 will be defined in the implementing rules.

Article 54
Accreditation of CIS handling RESTREINT UE/EU RESTRICTED information

1. All CIS handling RESTREINT UE/EU RESTRICTED information shall undergo an accreditation process, based upon the principles of Information Assurance, whose level of detail must be commensurate with the level of protection required.

2. The accreditation process shall include the formal validation by FRA's Security Accreditation Authority of the Security Plan for the CIS concerned in order to obtain assurance that:

   (a) the risk management process, as referenced in Article 53(2), has been properly carried out;
   (b) the Director has knowingly accepted the residual risk; and
   (c) a sufficient level of protection of the CIS, and of the EUCI handled in it, has been achieved in accordance with this decision.

3. The accreditation process shall consist of a series of tasks to be assumed by the parties involved. The responsibility for the preparation of the accreditation files and documentation shall rest entirely upon the CIS System Owner.

4. The accreditation shall be the responsibility of FRA's Security Accreditation Authority, who, at any moment in the life cycle of the CIS, shall have the right to:

   (a) require that an accreditation process be applied;
   (b) audit or inspect the CIS;
   (c) where conditions for operations are no longer satisfied, require the definition and effective implementation of a security improvement plan within a well-defined timescale, potentially withdrawing permission to operate the CIS until conditions for operations are again satisfied.

5. The accreditation process shall be established in a standard on the accreditation process for CIS handling EUCI, which shall be adopted in accordance with FRA's decision on the security of communication and information systems in FRA.

Article 55
Emergency circumstances

1. Notwithstanding the provisions of this Chapter, the specific procedures described below may be applied in an emergency, such as during impending or actual crisis, conflict, war situations or in exceptional operational circumstances.

2. RESTREINT UE/EU RESTRICTED information may be transmitted without encryption with the consent of the competent authority if any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and if:

   (a) the sender and recipient do not have the required encryption facility; and
   (b) the classified material cannot be conveyed in time by other means.

3. Classified information transmitted under the circumstances set out in paragraph 1 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.

4. A subsequent report shall be made to the competent authority.

CHAPTER 12

EXCHANGE OF CLASSIFIED INFORMATION WITH UNION INSTITUTIONS, AGENCIES, BODIES AND OFFICES, WITH MEMBER STATES AND WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

Article 56
Basic principles

1. Where FRA determines that there is a need to exchange classified information with the authorities of third States or international organisations, FRA shall establish corresponding working arrangements with the counterpart authorities of the third State or international organisation concerned. Such working arrangements may be concluded only with the authorisation of the Management Board after having consulted the Commission. They shall not be binding on the Union or on the Member States.
2. Working arrangements involving access to RESTREINT UE/EU RESTRICTED information may only be concluded with the relevant units of third countries or international organisations with which the European Commission already has an Administrative Arrangement or Security of Information Agreement within the meaning of Chapter 7 of Commission Decision 2015/444.
3. Where FRA or one of its units determines there is an exceptional need in the context of a Union political or legal framework to release RESTREINT UE/EU RESTRICTED to a third State or international organisation but no such working arrangements are in place, the FRA Security Officer shall consult the Commission, in accordance with Article 59.
4. RESTREINT UE/EU RESTRICTED information may only be shared with a Union institution, agency, body or office, which has equivalent basic principles and minimum standards for protecting RESTREINT UE/EU RESTRICTED information in place and if there is an appropriate legal or administrative framework.
5. The decision to release RESTREINT UE/EU RESTRICTED information originating in FRA shall be taken by the FRA department, as originator of this RESTREINT UE/EU RESTRICTED information, on a case-by-case basis, according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the Union. If the originator of the classified information for which release is desired, or of the source material it may contain, is not FRA, the FRA department which holds this classified information, shall first seek the originator's written consent to release. If the originator cannot be established, the FRA department, which holds this classified information, shall assume the former's responsibility after consulting the Commission.

Article 57
Sharing of RESTREINT UE/EU RESTRICTED information with Union institutions, agencies, bodies and offices

1. The conditions under which FRA may share RESTREINT UE/EU RESTRICTED information with the European Commission shall be set out in an administrative arrangement within the meaning of Article 51 of Commission Decision (EU, Euratom) 2015/444. Equivalence of FRA's rules and procedures for protecting RESTREINT UE/EU RESTRICTED information shall be established by means of an assessment visit.

2. Before entering into an administrative arrangement for sharing RESTREINT UE/EU RESTRICTED information with any other Union Institution, agency, body or office, FRA shall seek assurance that the Union Institution, agency, body or office concerned:
   (a) has a regulatory framework for the protection of EUCI in place, which lays down basic principles and minimum standards equivalent to those laid down in this Decision and its implementing rules;
   (b) applies security standards and guidelines regarding personnel security, physical security, management of RESTREINT UE/EU RESTRICTED information and security of Communication and Information Systems (CIS), which guarantee an equivalent level of protection of RESTREINT UE/EU RESTRICTED information as that afforded in FRA.
   (c) marks classified information, which it creates, as RESTREINT UE/EU RESTRICTED information.

3. The Head of Corporate Services Unit shall, in close cooperation with the Directorate-General Human Resources and Security of the Commission, be the lead service within FRA for the conclusion of administrative arrangements for sharing EUCI with Union institutions, agencies, bodies or offices.

4. Administrative arrangements shall as a general rule take the form of an Exchange of Letters, signed by the Executive Director on behalf of FRA.

5. Before entering into an administrative arrangement on sharing RESTREINT UE/EU RESTRICTED information, the FRA Security Officer shall ensure that an assessment visit has been conducted aimed at assessing the regulatory framework for protecting RESTREINT UE/EU RESTRICTED information and ascertaining the effectiveness of measures implemented for protecting it. The administrative arrangement shall enter into force, and RESTREINT UE/EU RESTRICTED information shall be shared, only if the outcome of this assessment visit is satisfactory and the recommendations made further to the visit have been complied with. Regular follow-up assessment visits shall be conducted to verify that the administrative arrangement is complied with and the security measures in place continue to meet the basic principles and minimum standards agreed.

6. The Director shall be informed of the process of concluding administrative arrangements pursuant to paragraph 3.

Article 58
Sharing of RESTREINT UE/EU RESTRICTED information with Member States

1. RESTREINT UE/EU RESTRICTED information may be shared with Member States provided that they protect that information in accordance with the requirements applicable to classified information bearing a national security classification at the equivalent level as set out in the table of equivalence of security classifications contained in Annex to the intergovernmental Agreement[8] between Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union.

2. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the European Union, FRA shall protect that information in accordance with the requirements applicable to RESTREINT

[8] OJ C 202, 8.7.2011, p. 13.

UE/EU RESTRICTED information as set out in the table of equivalence of security classifications contained in Annex I of Commission Decision (EU, Euratom) 2015/444.

Article 59
Exceptional *ad hoc* release of RESTREINT UE/EU RESTRICTED information

1. In the absence of working arrangements with the authorities of the third State or international organisation concerned, and in the absence of administrative arrangements with Union institutions, agencies, bodies and offices, RESTREINT UE/EU RESTRICTED information may be released under the exceptional *ad hoc* release procedure. The Decision to release shall be taken, after consultation of the Security Directorate of the Commission, by the Director on the basis of a proposal by the FRA Security Group.

2. Following the Director's decision to release the RESTREINT UE/EU RESTRICTED information and subject to prior written consent of the originator, including the originators of source material it may contain, FRA shall forward the information concerned. The information shall bear a releasability marking indicating the authorities of the third State, international organisation, Union institution, agency, body or office to which it is being released. Prior to or upon actual release, the third party in question shall undertake in writing to protect the RESTREINT UE/EU RESTRICTED information it receives in accordance with the basic principles and minimum standards set out in this Decision.

CHAPTER 13

END OF LIFE FOR RESTREINT UE/EU RESTRICTED INFORMATION

Article 60
Declassification of RESTREINT UE/EU RESTRICTED information

1. At the time of its creation, the originator shall indicate, where possible, whether RESTREINT UE/EU RESTRICTED information can be declassified on a given date or following a specific event.

2. Each department at FRA shall regularly review RESTREINT UE/EU RESTRICTED information for which it is the originator to ascertain whether the classification level still applies. Such a review shall not be necessary where the originator has indicated from the outset that the information will automatically be declassified and the information has been marked accordingly.

3. When review of the document results in a decision to declassify, consideration shall be given as to whether the document should be made public or bear a sensitive non-classified information distribution marking within the meaning of Article 9 of Commission Decision (EU, Euratom) 2015/443.

4. Information classified RESTREINT UE/EU RESTRICTED having originated in FRA will be considered to be automatically declassified after thirty years, in accordance with Regulation (EEC, Euratom) No 354/83 as amended by Council Regulations (EC, Euratom) No 1700/2003 and 496/2015[9].

Article 61
How to indicate that a document has been declassified

1. The original classification marking at the top and bottom of every page shall be visibly crossed out (not removed) either using the "strikethrough" functionality for electronic formats, or manually for print-outs.

2. The first (cover) page shall be stamped as declassified and completed with the reference of the authority responsible for declassifying.

3. The original recipients of RESTREINT UE/EU RESTRICTED information shall receive a copy of the declassified document for information. These initial recipients shall be responsible for informing any subsequent addressees to whom they have sent or copied the original RESTREINT UE/EU RESTRICTED information.

4. The declassified document will be archived following the provision of the FRA's document management and archiving policies.

5. All translations of classified information shall be subject to the same declassification procedures as the original language version.

---

[9] Council Regulation (EC, Euratom) No 1700/2003 of 22 September 2003 amending Regulation (EEC, Euratom) No 354/83 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community (OJ L 243, 27.9.2003, p.1).

Article 62

Partial declassification of RESTREINT UE/EU RESTRICTED information

1. Partial declassification shall also be possible (e.g. annexes, a few paragraphs). The procedure shall be identical to that of full declassification.

2. Upon partial declassification ("sanitising") of RESTREINT UE/EU RESTRICTED information, a declassified extract shall be produced.

3. The omitted text representing the non-declassified parts shall be replaced by:

PART NOT TO BE DECLASSIFIED

either in the body of the text itself (if the non-declassified part is a part of a paragraph), or as a paragraph (if the non-declassified part is a specific paragraph or more than one paragraph).

3. Specific mention shall be made in the text if a complete annex cannot be declassified and has hence been withheld from the extract.

Article 63

Destruction of RESTREINT U/EU RESTRICTED information

1. EU classified documents which are no longer required may be destroyed, taking account of regulations on archives and of FRA's rules and regulations on document management and archiving which follow the common Commission-level retention list for European Commission files, applied by analogy..
2. Documents classified as RESTREINT UE/EU RESTRICTED shall be destroyed by methods which shall be defined in the implementing rules and which shall meet relevant EU or equivalent standards.
3. Computer storage media used for RESTREINT UE/EU RESTRICTED information shall be destroyed in accordance with the procedures laid down in the implementing rules.
4. The Security Officer shall prepare plans based on local conditions for the safeguarding of EU classified material in a crisis including if necessary emergency invacuation, evacuation and evacuation plans. He shall promulgate instructions deemed necessary to prevent RESTREINT UE/EU RESTRICTED information from falling into unauthorised hands.
5. In the event of an emergency, if there is an imminent risk of unauthorised disclosure, RESTREINT UE/EU RESTRICTED information shall be destroyed by the holder in such a way that it cannot be reconstructed in whole or in part. The originator shall be informed of the emergency destruction of the RESTREINT UE/EU RESTRICTED information.

CHAPTER 14

FINAL PROVISIONS

Article 64
Classified information created before the entry into force of this decision

1. All classified information held by FRA before entry into force of this decision shall:

   (a) if created by FRA, continue to be considered to have been reclassified RESTREINT UE/EU RESTRICTED by default, unless its author had decided to declassify it and had informed all addressees of the document concerned;
   (b) if created by authors outside FRA, retain its original classification and thus be treated as RESTREINT UE/EU RESTRICTED information, unless the author agrees to declassification of the information.

Article 65
Implementing rules and security notices

1. As necessary, the adoption of the implementing rules for this decision will be the subject of a decision of the Director.

2. The Director may develop security notices setting out security guidelines and best practices within the scope of this decision and its implementing rules.

Article 66
Processing of personal data

1. FRA shall process personal data needed for implementing this decision in accordance with Regulation (EU) No 2018/1725.

2. Notwithstanding the measures already in place at the time of adoption of this decision and notified to the European Data Protection Supervisor, 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 12, which shall lay down appropriate safeguards for data subjects.

3. The Director shall be responsible for the security of any processing of personal data undertaken in the context of this decision.

Article 67
Transparency

This decision and its implementing rules shall be brought to the attention of FRA's staff and to all individuals to whom they apply.

Article 68

This decision shall enter into force on the date of its adoption. It repeals Director's decision ADMIN/012/2015 of 13/11/2015 on security provisions regarding the protection of EU Classified Information

Done at Vienna, on 17.05.2019

For the European Union Agency for Fundamental Rights

Sirpa Rautio
Chairperson of the Management Board