IV

(Notices)

NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

EUROPEAN PARLIAMENT

DECISION OF THE BUREAU OF THE EUROPEAN PARLIAMENT

of 6 June 2011

concerning the rules governing the treatment of confidential information by the European Parliament

(2011/C 190/02)

THE BUREAU OF THE EUROPEAN PARLIAMENT,

Having regard to Rule 23(12) of the Rules of Procedure of the European Parliament,

Whereas:

(1) In the light of the Framework Agreement on relations between the European Parliament and the European Commission [1] signed on 20 October 2010 ('the Framework Agreement'), it is necessary to revise the Bureau Decision of 13 November 2006 on the rules governing the administrative processing of confidential documents.

(2) The Lisbon Treaty assigns new tasks to the European Parliament and, in order to develop Parliament's activities in those areas which require a degree of confidentiality, it is necessary to lay down basic principles, minimum standards of security and appropriate procedures for the treatment by the European Parliament of confidential, including classified, information.

(3) The rules laid down in this Decision aim at ensuring equivalent standards of protection and compatibility with the rules adopted by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States, in order to facilitate the smooth functioning of the decision-making process of the European Union.

(4) The provisions of this Decision are without prejudice to Article 15 of the Treaty on the Functioning of the European Union (TFEU) and to 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 [2].

(5) The provisions of this Decision are without prejudice to Article 16 of the TFEU and to 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 [3],

HAS ADOPTED THIS DECISION:

Article 1

Objective

This Decision governs the creation, reception, forwarding and storage of confidential information by the European Parliament with a view to the appropriate protection of its confidential nature. It implements, in particular, Annex 2 to the Framework Agreement.

[1] OJ L 304, 20.11.2010, p. 47.

[2] OJ L 145, 31.5.2001, p. 43.

[3] OJ L 8, 12.1.2001, p. 1.

Article 2

Definitions

For the purposes of this Decision:

(a) 'information' means any written or oral information, whatever the medium and whoever the author may be;

(b) 'confidential information' means 'EU classified information' (EUCI), and non-classified 'other confidential information';

(c) 'EU classified information' (EUCI) means any information and material, classified as 'TRÈS SECRET UE/EU TOP SECRET', 'SECRET UE/EU SECRET', 'CONFIDENTIEL UE/EU CONFIDENTIAL' or 'RESTREINT UE/EU RESTRICTED', unauthorised disclosure of which could cause varying degrees of prejudice to EU interests, or to those of one or more of its Member States, whether such information originates within the institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or is received from Member States, third States or international organisations. In this regard:

— 'TRÈS SECRET UE/EU TOP SECRET' is the classification for information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the Union or of one or more of the Member States,

— 'SECRET UE/EU SECRET' is the classification for information and material the unauthorised disclosure of which could seriously harm the essential interests of the Union or of one or more of the Member States,

— 'CONFIDENTIEL UE/EU CONFIDENTIAL' is the classification for information and material the unauthorised disclosure of which could harm the essential interests of the Union or of one or more of the Member States,

— 'RESTREINT UE/EU RESTRICTED' is the classification for information and material the unauthorised disclosure of which could be disadvantageous to the interests of the Union or of one or more of the Member States;

(d) 'other confidential information' means any other non-classified confidential information, including information covered by data protection rules or by the obligation of professional secrecy, created in the European Parliament or forwarded by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States to the European Parliament;

(e) 'document' means any recorded information regardless of its physical form or characteristics;

(f) 'material' means any document or item of machinery or equipment, either manufactured or in the process of manufacture;

(g) 'need to know' means the need of a person to have access to confidential information in order to be able to perform an official function or a task;

(h) 'authorisation' means a decision (clearance decision), adopted by the President if it concerns Members of the European Parliament and by the Secretary-General if it concerns officials of the European Parliament and other Parliament employees working for political groups, to grant an individual access to EUCI up to a specific level, on the basis of a positive result of a security screening (vetting) carried out by a national authority under national law and pursuant to the provisions laid down in Annex I, part 2;

(i) 'downgrading' means a reduction in the level of classification;

(j) 'declassification' means the removal of any classification;

(k) 'originator' means the duly authorised author of EUCI or of any other confidential information;

(l) 'security notices' mean technical implementing measures as laid down in Annex II [1].

Article 3

Basic principles and minimum standards

1. The treatment of confidential information by the European Parliament shall follow the basic principles and minimum standards laid down Annex I, part 1.

2. The European Parliament shall set up an information security management system (ISMS) in accordance with those basic principles and minimum standards which shall aim at facilitating Parliamentary and administrative work, while ensuring the protection of any confidential information processed by the European Parliament, in full respect of the rules established by the originator of such information as laid down in the security notices.

The processing of confidential information by means of automated information systems (IS) of the European Parliament shall be implemented in accordance with the concept of information assurance (IA) and laid down in the security notices.

[1] Annex to be adopted.

3. Members of the European Parliament may consult classified information up to and including the level of 'CONFIDENTIEL UE/EU CONFIDENTIAL' without security clearance. For information classified as 'CONFIDENTIEL UE/EU CONFIDENTIAL', they shall sign a solemn declaration that they will not disclose the contents of that information to third persons. Information classified above the level of 'CONFIDENTIEL UE/EU CONFIDENTIAL' shall be made available only to Members who hold the appropriate level of security clearance.

4. Officials of the European Parliament and other Parliament employees working for political groups may consult confidential information if they have an established 'need to know', and may consult classified information above the level of 'RESTREINT UE/EU RESTRICTED' if they hold the appropriate level of security clearance.

Article 4

Creation of confidential information and administrative handling by the European Parliament

1. The President of the European Parliament, the chairs of the parliamentary committees concerned and the Secretary-General and/or any person duly authorised by him or her in writing may originate confidential information and/or classify information as laid down in the security notices.

2. When creating classified information, the originator shall apply the appropriate level of classification in line with the international standards and definitions set out in Annex I. The originator shall also determine, as a general rule, the addressees who are to be authorised to consult the information commensurate to the level of classification. This information shall be communicated to the Confidential Information Service (CIS) when the document is deposited with the CIS.

3. Confidential information covered by professional secrecy shall be dealt with in accordance with the handling instructions defined in the security notices.

Article 5

Reception of confidential information by the European Parliament

1. Confidential information received by the European Parliament shall be communicated as follows:

— EUCI classified as 'RESTREINT UE/EU RESTRICTED' and other confidential information to the secretariat of the parliamentary body/office-holder who submitted the request therefor,

— EUCI classified as 'CONFIDENTIEL UE/EU CONFIDENTIAL' and above to the CIS.

2. The registration, storage and traceability of confidential information shall be assured either by the secretariat of the parliamentary body/office-holder which received the information or by the CIS.

3. In the case of confidential information communicated by the Commission pursuant to the Framework Agreement, the agreed arrangements within the meaning of point 3.2 of Annex 2 to the Framework Agreement (laid down by common accord and concerning addressees, consultation procedure, i.e. secure reading room and meetings in camera, or other matters) designed to preserve the confidentiality of the information shall be deposited together with the confidential information at the secretariat of the parliamentary body/office holder or at the CIS when the information is classified as 'CONFIDENTIEL UE/EU CONFIDENTIAL' or above.

4. The arrangements referred to in paragraph 3 may also be applied *mutatis mutandis* for the communication of confidential information by other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or by Member States.

5. EUCI classified as 'TRÈS SECRET UE/EU TOP SECRET' shall be transmitted to the European Parliament subject to further arrangements, to be agreed between the parliamentary body/office holder who submitted the request for the information and the EU institution or the Member State by whom it is communicated. An oversight committee shall be set up by the Conference of Presidents. It shall aim at ensuring a level of protection commensurate with that level of classification.

Article 6

Communication of EUCI by the European Parliament to third parties

The European Parliament may, subject to the originator's consent, forward EUCI to other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties or to Member States on the condition that they ensure that, when EUCI is handled, rules equivalent to those laid down in this Decision are respected within their services and premises.

Article 7

Storage and consultation of confidential information in secured areas (secure reading rooms)

1. Secure reading rooms shall provide for secure storage and shall not contain photocopying machines, telephones, fax facilities, scanners or any other technical equipment for the reproduction or transmission of documents.

2. The following conditions shall govern access to a secure reading room:

(a) only the following persons shall have access:

— Members of the European Parliament, officials of the European Parliament and other Parliament employees working for political groups, duly identified in accordance with the arrangements referred to in Article 4(2) or Article 5(3) and (4),

— the European Parliament's officials responsible for managing the CIS,

— as necessary, the European Parliament's officials responsible for security and fire safety.

Cleaning of the secured area shall only occur in the presence of and under close surveillance of an official working in the CIS;

(b) each person wishing to access the confidential information shall communicate in advance his or her name to the CIS. The CIS shall check the identity of each person who submits an application to consult that information and verify, where relevant, consult it in accordance with the arrangements referred to in Article 4(2) or Article 5(3) and (4);

(c) the CIS shall be empowered to deny access to the room to any person not authorised to enter it pursuant to points (a) and (b). Any objection challenging the decision by the CIS shall be submitted to the President, in the case of Members of the European Parliament, and to the Secretary-General, in other cases.

3. The following conditions shall govern the consultation of confidential information in the secure reading room:

(a) persons who are authorised to consult the information and who have submitted the application referred to in point (b) of paragraph 2 shall present themselves to the CIS.

Save in exceptional circumstances (e.g. where numerous requests for consultation are submitted in a short period of time), only one person at a time shall be authorised to consult confidential information in the secure reading room, in the presence of an official of the CIS.

That official shall inform the person thus authorised of his/her obligations and, in particular, shall ask him/her to sign a solemn declaration undertaking not to disclose the content of the information to any third person;

(b) during the consultation process, contact with the exterior (including by means of telephones or other technologies), the taking of notes and the photocopying or photographing of the confidential information consulted shall be prohibited;

(c) before authorising a person to leave the secure reading room, the official of the CIS referred to in point (a) shall check that the confidential information consulted is still present, intact and complete.

4. In the event of a breach of the rules set out above, the official responsible for the CIS shall inform the Secretary-General, who shall refer the matter to the President, should the perpetrator be a Member of the European Parliament.

Article 8

Minimum standards for other consultation of confidential information

1. As regards the administrative processing of confidential information at a meeting in camera, the secretariat of the parliamentary body/office holder responsible for the meeting shall ensure that:

— only the persons designated to participate in the meeting and holding the necessary level of security clearance are allowed to enter the meeting room,

— all documents are numbered, distributed at the beginning of the meeting and collected again at the end, and that no notes of those documents and no photocopies or photographs thereof are taken,

— the minutes of the meeting make no mention of the content of the discussion of the information considered under the confidential procedure,

— confidential information provided orally to recipients in the European Parliament is subject to the equivalent level of protection as that applied to confidential information in written form. This may include a solemn declaration by the recipients of that information not to divulge its contents to any third person.

2. The following rules shall apply to the administrative processing of confidential information by the secretariat of the parliamentary body/office holder outside the meeting in camera:

— the hard copy documents shall be handed over in person to the head of the secretariat, who shall register them and provide an acknowledgement of receipt,

— such documents shall be kept in a locked location, under the responsibility of the secretariat, when they are not actually being used,

— without prejudice to the administrative processing of confidential information at a meeting in camera as provided for in paragraph 1, in no case may they be duplicated, saved on another medium, or transmitted to any person,

— access to such documents shall be restricted to the addressees thereof and shall, in accordance with the arrangements referred to in Article 4(2) or Article 5(3) or (4), be under the supervision of the secretariat,

— the secretariat shall keep a record of the persons who have consulted the documents, and of the date and time of such consultation. That record shall be transmitted to the CIS in view of the establishment of the annual report referred to in Article 12.

Article 9

Archiving of confidential information

1. Secure archiving facilities shall be provided on the European Parliament's premises.

Confidential information definitively deposited with the CIS or the secretariat of the parliamentary body/office-holder shall be transferred to the secure archive in the CIS six months after they were last consulted and, at the latest, one year after they were deposited.

2. The CIS shall be responsible for managing the secure archives, in accordance with standard archiving criteria.

3. Confidential information held in the secure archives may be consulted subject to the following conditions:

— only those persons identified by name or by office in the accompanying document drawn up when the confidential information was deposited shall be authorised to consult that information,

— the application to consult confidential information must be submitted to the CIS, which shall transfer the document in question to the secure reading room,

— the procedures and conditions governing the consultation of confidential information set out in Article 7 shall apply.

Article 10

Downgrading and declassification of EUCI

1. EUCI may be downgraded or declassified only with the permission of the originator, and, if necessary, after discussion with other interested parties. Downgrading or declassification shall be confirmed in writing. The originator shall be responsible for informing its addressees of the change, and they in turn shall be responsible for informing any subsequent addressees to whom they have sent or copied the document, of the change. If possible, originators shall specify on classified documents a date, period or event when the contents may be downgraded or declassified. Otherwise, they shall keep the documents under review every five years, at the latest, in order to ensure that the original classification is necessary.

2. Declassification of documents held in the secure archives will take place at the latest after 30 years pursuant to the provisions of Council Regulation (EEC, Euratom) No 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community [1]. Declassification will be effected by the originator of the classified information or the service currently responsible in accordance with Annex I, Part 1, Section 10.

Article 11

Breaches of confidentiality

1. Breaches of confidentiality in general, and of this Decision in particular, shall in the case of Members of the European Parliament entail the application of the relevant provisions concerning penalties set out in the European Parliament's Rules of Procedure.

2. Breaches committed by staff shall lead to the application of the procedures and penalties provided for by, respectively, the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union, laid down in Regulation (EEC, Euratom, ECSC) No 259/68 [2] ('the Staff Regulations').

3. The President and the Secretary-General shall organise any necessary investigations.

Article 12

Adaptation of this Decision and its implementing rules and annual reporting on the application of this Decision

1. The Secretary-General shall propose any necessary adaptation of this Decision and the annexes implementing it and shall forward those proposals to the Bureau for decision.

2. The Secretary-General shall submit an annual report to the Bureau on the application of this Decision.

[1] OJ L 43, 15.2.1983, p. 1.
[2] OJ L 56, 4.3.1968, p. 1.

Article 13

Transitional and final provisions

1. Confidential information existing in the CIS or in the archives before the application of this Decision shall be classified 'RESTREINT UE/EU RESTRICTED' by default unless its originator decides either not to classify it or to classify it at a higher classification level or with a marking within one year from the date of entry into force of this Decision.

2. If its originator decides to give such confidential information a higher classification level, it shall be classified at the lowest possible level by the originator or its delegates, in liaison with the CIS and in accordance with the criteria laid down in the Annex I.

3. The Decision of the Bureau of 13 November 2006 on the rules governing the administrative processing of confidential documents is repealed.

4. The Decision of the Bureau of 24 October 2005 mandating the Secretary-General to set up a declassification committee and to adopt decisions on the issue of declassification is repealed.

Article 14

Entry into force

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

2. It shall apply from 1 July 2011.

ANNEX I

PART 1

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY FOR THE PROTECTION OF CONFIDENTIAL INFORMATION

1. **Introduction**

These provisions lay down the basic principles and minimum standards of security to be complied with by the European Parliament in all its places of employment, as well as by all recipients of EUCI and other confidential information, so that security is safeguarded and all persons concerned may be assured that a common standard of protection is established. They are supplemented by rules governing the treatment of confidential information by parliamentary committees and other parliamentary bodies/office-holders.

2. **General principles**

The European Parliament's security policy forms an integral part of its general internal management policy and is thus based on the principles governing that general policy. Those principles include legality, transparency, accountability, and subsidiarity and proportionality.

The principle of legality entails the need to remain strictly within the legal framework in the execution of security functions, and to conform to the applicable legal requirements. It also means that responsibilities in the security domain must be based on proper legal provisions. The provisions of the Staff Regulations, in particular Article 17 thereof on the obligation of staff to refrain from any unauthorised disclosure of information received in the line of duty and Title VI thereof on disciplinary measures, are fully applicable. Finally, it means that breaches of security within the responsibility of the European Parliament must be dealt with in a manner consistent with the European Parliament's policy on disciplinary measures.

The principle of transparency entails the need for clarity regarding all security rules and provisions, for a balance to be struck between the different services and the different domains (physical security as compared to the protection of information, etc.), and for a consistent and structured security awareness policy. It also means that clear written guidelines are necessary for the implementation of security measures.

The principle of accountability means that responsibilities in the field of security will be clearly defined. Moreover, it entails the need regularly to monitor whether those responsibilities have been properly fulfilled.

The principle of subsidiarity means that security shall be organised at the lowest possible level and as closely as possible to the European Parliament's Directorates-General and services. The principle of proportionality means that security activities shall be strictly limited to what is absolutely necessary and that security measures shall be proportional to the interests to be protected and to the actual or potential threat to those interests, so as to enable them to be defended in a way which causes the least possible disruption.

3. **Foundations of information security**

The foundations of sound information security are:

(a) within the European Parliament, an INFOSEC (information security) assurance service responsible for working with the security authority concerned to provide information and advice on technical threats to security and the means of protecting against them;

(b) close cooperation between the European Parliament's responsible services and the security services of the other EU institutions.

4. **Principles of information security**

4.1. *Objectives*

The principle objectives of information security are as follows:

(a) to safeguard EUCI and other confidential information against espionage, compromise or unauthorised disclosure;

(b) to safeguard EUCI handled in communications and information systems and networks against threats to its confidentiality, integrity and availability;

(c) to safeguard European Parliament premises housing EUCI against sabotage and malicious wilful damage;

(d) in the event of a security failure, to assess the damage caused, limit its consequences, conduct security investigations and adopt the necessary remedial measures.

4.2. *Classification*

4.2.1. Where confidentiality is concerned, care and experience are needed in the selection of the information and material to be protected and the assessment of the degree of protection required. It is fundamental that the degree of protection should correspond to the sensitivity, in terms of security, of the individual item of information or material to be safeguarded. In order to ensure the smooth flow of information, both over-classification and under-classification shall be avoided.

4.2.2. The classification system is the instrument by which effect is given to the principles set out in this section; a similar system of classification shall be followed in planning and organising ways to counter espionage, sabotage, terrorism and other threats, so that the maximum protection is afforded to the most important premises housing EUCI and to the most sensitive points within them.

4.2.3. Responsibility for classifying information lies solely with the originator of the information concerned.

4.2.4. The level of classification may solely be based on the content of that information.

4.2.5. Where a number of items of information are grouped together, the classification level to be applied to the whole must at least be as high as the highest classification applied individually to those items. A collection of information may however be given a higher classification than its constituent parts.

4.2.6. Classifications shall be assigned only when necessary and for as long as necessary.

4.3. *Aims of security measures*

The security measures shall:

(a) extend to all persons having access to EUCI, EUCI-carrying media, and other confidential information, as well as all premises containing such information and important installations;

(b) be designed to detect persons whose position might jeopardise the security of such information and of important installations housing such information, and provide for their exclusion or removal;

(c) prevent any unauthorised person from having access to such information or to installations containing it;

(d) ensure that such information is disseminated solely on the basis of the need-to-know principle that is fundamental to all aspects of security;

(e) ensure the integrity (i.e. prevent corruption, unauthorised alteration or unauthorised deletion) and the availability (to those needing and authorised to have access thereto) of all confidential information, whether classified or not classified, and especially where it is stored, processed or transmitted in electromagnetic form.

5. **Common minimum standards**

The European Parliament shall ensure that common minimum standards of security are observed by all recipients of EUCI, both inside the institution and under its competence, namely all its services and contractors, so that such information can be passed on in the confidence that it will be handled with equal care. Such minimum standards shall include criteria for the security clearance of officials of the European Parliament and other Parliament employees working for political groups, and procedures for the protection of confidential information.

The European Parliament shall allow outside bodies access to such information only on condition that they ensure that it is handled in accordance with provisions that are at least strictly equivalent to these common minimum standards.

Such common minimum standards shall also be applied when, pursuant to a contract or grant, the European Parliament entrusts to industrial or other entities tasks involving confidential information.

6. **Security for officials of the European Parliament and other Parliament employees working for political groups**

6.1. *Security instructions for officials of the European Parliament and other Parliament employees working for political groups*

Officials of the European Parliament and other Parliament employees working for political groups in positions where they could have access to EUCI shall be given thorough instructions, both on taking up their assignment and at regular intervals thereafter, in the need for security and the procedures for achieving it. Such persons shall be required to certify in writing that they have read and fully understand the applicable security provisions.

6.2. *Management responsibilities*

Managers shall have the duty of knowing those of their staff who are engaged in work on classified information or who have access to secure communication or information systems, and to record and report any incidents or apparent vulnerabilities which are likely to affect security.

6.3. *Security status of officials of the European Parliament and other Parliament employees working for political groups*

Procedures shall be established to ensure that, when adverse information becomes known concerning an official of the European Parliament or other Parliament employee working for a political group, steps are taken to determine whether that individual's work brings him or her into contact with classified information or whether he or she has access to secure communication or information systems, and that the European Parliament's responsible service is informed. If it is established that such an individual constitutes a security risk, he or she shall be barred or removed from assignments where he or she might endanger security.

7. **Physical security**

'Physical security' means the application of physical and technical protective measures to prevent unauthorised access to EUCI.

7.1. *Need for protection*

The degree of physical security measures to be applied to ensure the protection of EUCI shall be proportional to the classification and volume of, and the threat to, the information and material held. All holders of EUCI shall follow uniform practices regarding classification of such information and must meet common standards of protection regarding the custody, transmission and disposal of information and material requiring protection.

7.2. *Checking*

Before leaving areas containing EUCI unattended, persons having custody thereof shall ensure that it is securely stored and that all security devices have been activated (locks, alarms, etc.). Further independent checks shall be carried out after working hours.

7.3. *Security of buildings*

Buildings housing EUCI or secure communication and information systems shall be protected against unauthorised access.

The nature of the protection afforded to EUCI, e.g. barring of windows, locks for doors, guards at entrances, automated access control systems, security checks and patrols, alarm systems, intrusion detection systems and guard dogs, shall depend on:

(a) the classification, volume and location within the building of the information and material to be protected;

(b) the quality of the security containers for the information and material concerned; and

(c) the physical nature and location of the building.

The nature of the protection afforded to communication and information systems shall depend on an assessment of the value of the assets at stake and of the potential damage if security were to be compromised, on the physical nature and location of the building in which the system is housed, and on the location of that system within the building.

7.4. *Contingency plans*

Detailed plans shall be prepared in advance for the protection of classified information during an emergency.

8. **Security designators, markings, affixing and classification management**

8.1. *Security designators*

No classifications other than those defined in Article 2(c) of this Decision are permitted.

An agreed security designator may be used to set limits to the validity of a classification (for classified information signifying automatic downgrading or declassification). That designator shall either be 'UNTIL … (time/date)' or 'UNTIL … (event)'.

Additional security designators such as CRYPTO or any other EU-recognised security designator shall apply where there is a need for limited distribution and special handling in addition to that designated by the security classification.

Security designators shall only be used in combination with a classification.

8.2. *Markings*

A marking may be used to specify the field covered by a given document or a particular distribution on a need-to-know basis, or (for non-classified information) to signify the end of an embargo.

A marking is not a classification and must not be used in lieu of one.

8.3. *Affixing of classifications and of security designators*

Classifications shall be affixed as follows:

(a) on documents classified as 'RESTREINT UE/EU RESTRICTED', by mechanical or electronic means;

(b) on documents classified as 'CONFIDENTIEL UE/EU CONFIDENTIAL', by mechanical means or by hand or by printing on pre-stamped, registered paper;

(c) on documents classified as 'SECRET UE/EU SECRET' and 'TRÈS SECRET UE/EU TOP SECRET', by mechanical means or by hand.

Security designators shall be affixed directly under the classification, by the same means as those used for affixing classifications.

8.4. *Classification management*

8.4.1. General

Information shall be classified only when necessary. The classification shall be clearly and correctly indicated, and shall be maintained only as long as the information requires protection.

The responsibility for classifying information and for any subsequent downgrading or declassification rests solely with the originator.

Officials of the European Parliament shall classify, downgrade or declassify information on instructions from or pursuant to a delegation from the Secretary-General.

The detailed procedures for the treatment of classified documents shall be so framed as to ensure that they are afforded protection appropriate to the information which they contain.

The number of persons authorised to originate 'TRÈS SECRET UE/EU TOP SECRET' documents shall be kept to a minimum, and their names shall be kept on a list drawn up by the CIS.

8.4.2. Application of classification

The classification of a document shall be determined by the level of sensitivity of its contents in accordance with the definitions contained in Article 2(c). It is important that classification be correctly and sparingly used, especially as regards the 'TRÈS SECRET UE/EU TOP SECRET' classification.

The classification of a letter or note containing enclosures shall be as high as the highest classification granted to one of its enclosures. The originator shall indicate clearly the level at which the letter or note should be classified when detached from its enclosures.

The originator of a document that is to be given a classification shall bear in mind the rules set out above and shall curb any tendency to over- or under-classify.

Individual pages, paragraphs, sections, annexes, appendices, attachments and enclosures of a given document may require different classifications and shall be classified accordingly. The classification of the document as a whole shall be that of its most highly classified part.

9. **Inspections**

Periodic inspections of the security arrangements for the protection of EUCI shall be carried out by the European Parliament's directorate responsible for security, which may be assisted in this task by the CIS.

The European Parliament's directorate responsible for security and the security services of other institutions, bodies, offices and agencies established by virtue or on the basis of the Treaties holding EUCI may also agree to carry out peer evaluations of the security arrangements for the protection of EUCI.

10. **Declassification procedure**

10.1. The CIS will examine EUCI and will make proposals on a declassification to the originator of a document by no later than the 25th year following the date of its creation. Documents not declassified at the first examination shall be re-examined periodically and at least every five years.

10.2. In addition to being applied to documents actually located in the secure archives and duly classified, the declassification process may also cover other confidential information existing in either the secure archives or the European Parliament Archive and Documentation Centre (CARDOC).

10.3. On behalf of the originator, the CIS will be responsible for informing the addressees of the document of the change to the classification, and they in turn shall be responsible for informing any subsequent addressees to whom they have sent or copied the document.

10.4. Declassification does not affect any markings which may appear on the document.

10.5. The original classification at the top and bottom of every page shall be crossed out. The first (cover) page of the document shall be stamped and completed with the reference of the CIS.

10.6. The text of the declassified document shall be attached to the electronic fiche or equivalent system where it has been registered.

10.7. In the case of documents covered by the exception relating to privacy and the integrity of the individual or commercial interests of a natural or legal person and in the case of sensitive documents, Article 2 of Regulation (EEC, Euratom) No 354/83 shall apply.

10.8. In addition to the provisions of points 10.1 to 10.7, the following rules shall apply:

(a) as regards third-party documents, the CIS will consult the third party concerned before proceeding to carry out the declassification. The third party will have eight weeks in which to submit remarks;

(b) as regards the exception relating to privacy and the integrity of the individual, the declassification procedure will take into account, in particular, the agreement of the person concerned, the impossibility of identifying the person concerned and/or the fact that that person is no longer alive;

(c) as regards the exception relating to commercial interests of a natural or legal person, the person concerned can be notified via publication in the *Official Journal of the European Union* and given four weeks from the day of that publication in which to submit remarks.

PART 2

SECURITY CLEARANCE PROCEDURE

11. **Security clearance procedure for Members of the European Parliament**

11.1. In light of the European Parliament's prerogatives and competences, its Members may be granted access to EUCI up to and including the level of 'CONFIDENTIEL UE/EU CONFIDENTIEL' without security clearance. For information classified as 'CONFIDENTIEL UE/EU CONFIDENTIAL', they shall sign of a solemn declaration that they will not disclose the contents of that information to any third person.

11.2. In order to have access to information classified as 'TRÈS SECRET UE/EU TOP SECRET', or 'SECRET UE/EU SECRET', Members of the European Parliament must have been authorised in accordance with the procedure referred to in points 11.3 and 11.4.

11.3. Authorisation shall be granted only to Members of the European Parliament who have undergone security screening by the competent national authorities of the Member States in accordance with the procedure referred to in points 11.9 to 11.14. The President shall be responsible for granting the authorisation for Members.

11.4. The President may grant authorisation after obtaining the opinion of the competent national authorities of the Member States on the basis of security screening carried out in accordance with points 11.8 to 11.13.

11.5. The European Parliament's directorate responsible for security shall maintain an up-to-date list of all Members of the European Parliament who have been granted authorisation, including provisional authorisation within the meaning of point 11.15.

11.6. Authorisation shall be valid for a period of five years or for the duration of the tasks in respect of which it was granted, whichever is the shorter. It may be renewed in accordance with the procedure laid down in point 11.4.

11.7. Authorisation shall be withdrawn by the President where he/she considers that there are justified grounds for doing so. Any decision to withdraw authorisation shall be notified to the Member of the European Parliament concerned, who may ask to be heard by the President before the withdrawal takes effect, and to the competent national authority.

11.8. Security screening shall be carried out with the assistance of the Member of the European Parliament concerned and at the request of the President. The competent national authority for screening is that of the Member State of which the Member concerned is a national.

11.9. As part of the screening procedure, the Member of the European Parliament concerned shall be required to complete a personal information form.

11.10. The President shall specify in his/her request to the competent national authorities the level of classified information to be made available to the Member of the European Parliament concerned, so that they may carry out the screening process.

11.11. The entire security-screening process carried out by the competent national authorities, together with the results obtained, shall be in accordance with the relevant rules and regulations in force in the Member State concerned, including those concerning appeals.

11.12. Where the competent national authorities of the Member State give a positive opinion, the President may grant the Member of the European Parliament concerned authorisation.

11.13. A negative opinion by the competent national authorities shall be notified to the Member of the European Parliament concerned, who may ask to be heard by the President. Should he/she consider it necessary, the President may ask the competent national authorities for further clarification. If the negative opinion is confirmed, authorisation shall not be granted.

11.14. All Members of the European Parliament granted authorisation within the meaning of point 11.3 shall, at the time when the authorisation is granted and at regular intervals thereafter, receive any necessary guidelines concerning the protection of classified information and the means of ensuring such protection. Such Members shall sign a declaration acknowledging receipt of those guidelines.

11.15. In exceptional circumstances, the President may, after notifying the competent national authorities and provided there is no reaction from them within one month, grant provisional authorisation to a Member of the European Parliament for a period not exceeding six months, pending the outcome of the screening referred to in point 11.11. The provisional authorisations thus granted shall not give access to information classified as 'TRÈS SECRET UE/EU TOP SECRET'.

12. **Security clearance procedure for officials of the European Parliament and other Parliament employees working for political groups**

12.1. Only officials of the European Parliament and other Parliament employees working for political groups who, by reason of their duties and in the requirements of the service, need to have knowledge of, or to use, classified information, may have access to such information.

12.2. In order to have access to information classified as 'TRÈS SECRET UE/EU TOP SECRET', 'SECRET UE/EU SECRET' and 'CONFIDENTIEL UE/EU CONFIDENTIAL', the persons referred to in point 12.1 must have been authorised in accordance with the procedure laid down in points 12.3 and 12.4.

12.3. Authorisation shall be granted only to the persons referred to in point 12.1 who have undergone security screening by the competent national authorities of the Member States in accordance with the procedure referred to in points 12.9 to 12.14. The Secretary-General shall be responsible for granting the authorisation for officials of the European Parliament and other Parliament employees working for political groups.

12.4. The Secretary General may grant authorisation after obtaining the opinion of the competent national authorities of the Member States on the basis of security screening carried out in accordance with points 12.8 to 12.13.

12.5. The European Parliament's directorate responsible for security shall maintain an up-to-date list of all posts requiring a security clearance, as provided by the relevant European Parliament services and of all persons who have been granted authorisation, including provisional authorisation within the meaning of point 12.15.

12.6. Authorisation shall be valid for a period of five years or for the duration of the tasks in respect of which it was granted, whichever is the shorter. It may be renewed in accordance with the procedure referred to in point 12.4.

12.7. Authorisation shall be withdrawn by the Secretary-General where he/she considers that there are justifiable grounds for doing so. Any decision to withdraw authorisation shall be notified to the official of the European Parliament or other Parliament employee working for a political group concerned, who may ask to be heard by the Secretary-General before the withdrawal takes effect, and to the competent national authority.

12.8. Security screening shall be carried out with the assistance of the person concerned and at the request of the Secretary-General. The competent national authority for screening is that of the Member State of which the person concerned is a national. Where permissible under national laws and regulations, the competent national authorities may conduct investigations in respect of non-nationals who require access to information classified as 'CONFIDENTIEL UE/EU CONFIDENTIAL' or above.

12.9. As part of the screening procedure, the official of the European Parliament or other Parliament employee working for a political group concerned shall be required to complete a personal information form.

12.10. The Secretary-General shall specify in his/her request to the competent national authorities the level of classified information to be made available to the person concerned, so that they may carry out the screening process and give their opinion as to the level of authorisation it would be appropriate to grant to that person.

12.11. The entire security-screening process carried out by the competent national authorities, together with the results obtained, shall be subject to the relevant rules and regulations in force in the Member State concerned, including those concerning appeals.

12.12. Where the competent national authorities of the Member State give a positive opinion, the Secretary-General may grant the person concerned authorisation.

12.13. A negative opinion by the competent national authorities shall be notified to the official of the European Parliament or other Parliament employee working for a political group concerned, who may ask to be heard by the Secretary-General. Should he/she consider it necessary, the Secretary-General may ask the competent national authorities for further clarification. If the negative opinion is confirmed, authorisation shall not be granted.

12.14. All officials of the European Parliament and other Parliament employees working for political groups who are granted authorisation within the meaning of points 12.4 and 12.5 shall, at the time when the authorisation is granted and at regular intervals thereafter, receive any necessary instructions concerning the protection of classified information and the means of ensuring such protection. Such officials and employees shall sign a declaration acknowledging receipt of those instructions and give an undertaking to obey them.

12.15. In exceptional circumstances, the Secretary-General may, after notifying the competent national authorities and provided there is no reaction from them within one month, grant provisional authorisation to an official of the European Parliament or other Parliament employee working for a political group for a period not exceeding six months, pending the outcome of the screening referred to in point 12.11 of this section. Provisional authorisations thus granted shall not give access to information classified as 'TRÈS SECRET UE/EU TOP SECRET'.