COUNCIL OF THE EUROPEAN UNION

Brussels, 18 October 2010

15104/10

LIMITE

CSC 57

NOTE

From:	The General Secretariat
To:	The Security Committee
Subject:	Draft policy on creating and marking EU classified information

Delegations will find attached a draft policy on creating and marking EUCI, including a practical classification guide, for discussion at the Security Committee's next meeting.

Draft

Policy on creating and marking EU classified information

1. This policy on creating and marking EU classified information (EUCI) lays down general standards for protecting EU classified information. It constitutes a commitment to help achieve an equivalent level of implementation of the Council Security Rules[1] (hereafter the 'CSR').

2. This policy recalls the definition of EUCI and corresponding security classification levels; lists the entities which may create EUCI; provides guidance on how to classify information as EUCI and on its downgrading or declassification; describes the preparation of EU classified documents and the markings which may be used on them; and describes the regime applicable in the case of compromise of EUCI.

3. The Council and the General Secretariat of the Council (GSC) will apply this security policy with regard to protecting EUCI in their premises and communication and information systems (CIS).

4. The Member States will act in accordance with national laws and regulations to the effect that the standards laid down in this security policy with regard to protecting EUCI are respected when EUCI is handled in national structures, including on national CIS.

I. Definition of EUCI and EU security classifications

5. According to Article 2(1) of the CSR, EUCI means "any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States". The EU security classifications referred to in this definition and the corresponding descriptions are the following[2]:

---

[1] Council Decision …, OJ L …

[2] Article 2(2) of the CSR

(a) TRES SECRET UE/EU TOP SECRET: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States.

(b) SECRET UE/EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States.

(c) CONFIDENTIEL UE/EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States.

(d) RESTREINT UE/EU RESTRICTED: 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.

II. Originators of EUCI

6. The originator of EUCI is the entity which has created and classified information as "EU classified information". The entities referred to hereafter may create EUCI.

7. All classified information created by the European Council, the Council or the GSC is to be designated and marked as EUCI in accordance with the CSR.

8. All classified information created by the European Commission or by the Commission services is designated and marked as EUCI in accordance with the relevant security provisions[1].

9. All classified information created by the European External Action Service (EEAS) is designated and marked as EUCI in accordance with the security rules for the EEAS[2].

---

[1] Commission Decision 2001/844/EC, ECSC, Euratom, OJ L 317, 3.12.2001, p. 1

[2] Decision by the High Representative …

10. Where the founding acts of EU agencies and bodies provide for them to apply the CSR or the Commission's security provisions, all classified information created by them is designated and marked as EUCI.

11. All classified information created by the European Police Office (Europol) is designated and marked as EUCI in accordance with the rules on the confidentiality of Europol information.[1]

12. All classified information created by:

- EU missions established by the Council under the Common Security and Defence Policy (CSDP), or by

- EU Special Representatives (EUSRs) and their teams,

is designated and marked as EUCI in accordance with the Council Decisions establishing their mandates.

13. Member States may create EUCI in the context of the EU's activities. This is without prejudice to the possibility of introducing classified information bearing a national security classification marking into the structures or networks of the EU. In the latter case, the Council and the GSC, as well as EU agencies and bodies which apply the CSR, will protect that information in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Appendix B to the CSR.

14. Where Member States feed their national position or input into the EU's decision-making process, for instance through amendments to or comments on texts originating in the GSC:

[1] Council Decision 2009/968/JHA of 30 November 2009, OJ L 332, 17.12.2009, p. 17

– any such classified information from Member States will always be designated as EUCI and not bear a national classification marking;

– the function of originator with regard to such EUCI will be exercised by the EU institution, agency or body which created the original document on which comments and input are sought.

III. Classifying

15. The GSC and each Member State will designate the entities or functions authorised to create and classify information as EUCI, in particular at the level CONFIDENTIEL UE/EU CONFIDENTIAL and above. Such entities and functions may be the authors of classified documents.

16. Classifying information as EUCI amounts to taking a decision that the disclosure of such information 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. Such decisions must not be taken lightly; due consideration must be given to the actual content of a document before deciding that it needs to be classified.

17. Once a decision has been made to classify the information, the question must be asked as to the level of protection that it requires. The classification level attributed to the information determines the level of protection to which it will be subject in the personnel, physical, procedural and information assurance areas. The practical classification guide attached in Annex I contains criteria on the basis of which classification decisions should be taken. Annex II summarises the security measures applied to each security classification level in accordance with the CSR. Authors should be aware that security measures increase substantially from the level CONFIDENTIEL UE/EU CONFIDENTIAL.

18. Information which warrants classification should be classified regardless of its physical form. Its classification must be clearly communicated to its recipients, either by an announcement (if it is delivered in oral form, such as in a conversation or a presentation) or by a classification marking (if it is delivered in written form, be it on paper or in CIS). Classified material should be physically marked so as to allow for its security classification to be easily identified.

19. Information should be classified as soon as it takes form. For example, personal notes, drafts or e-mail messages containing information which warrants classification should be marked as classified information from the outset and should be produced and handled in accordance with the requirements of the CSR in physical and technical terms. Such information may then evolve into an official document which will in turn be appropriately marked and handled.

20. The decision on the security classification level to be attributed to EUCI (and the document or material containing it) will be taken by its author, in consultation with hierarchical superiors and other stakeholders as appropriate.

21. Departments may decide to attribute a standard classification level to categories of information which they create or handle on a regular basis. However, they must ensure that in so doing they do not systematically overclassify or underclassify individual pieces of information (see below).

IV. Overclassification and underclassification

22. Information should be classified at the level which best corresponds to the protective measures it warrants (see summary of security measures in Annex II): not higher, not lower.

23. Overclassification means the attribution to a piece of information of a classification level higher than that warranted by it. Overclassification should be avoided, since it puts an unnecessary (or even counterproductive) burden on the handling of the information and entails unnecessary costs.

24. Underclassification means the attribution to a piece of information of a classification level lower that that warranted by it. Underclassification should be avoided, since it exposes the information to increased risk of disclosure to unauthorised persons.

VI. Markings

25. EU classified information or material must always bear a security classification marking corresponding to its security classification level. In the case of a document, each page will bear this marking at the top and at the bottom.

26. In addition, EU classified information or material may bear markings such as the following:

(a) an identifier to designate the originator, such as "BELGIUM", "EDA" or "EULEX Kosovo". Such a marking should appear next to (i.e. beside or below) every occurrence of the security classification marking;

(b) any caveats, code words or acronyms specifying:

(i) the field of activity to which the document relates (such as "CSDP");
(ii) a particular distribution on a need-to-know basis (such as "… ONLY"); or
(iii) restrictions on use (such as "NOT TO BE FURTHER RELEASED WITHOUT PRIOR AUTHORISATION").

Such markings should appear in a clearly visible way at least on the first page of a document.

(c) releasability markings, such as "RELEASABLE TO [THIRD STATE]" or "RELEASABLE TO THE FADO COMMUNITY"; such marking should appear next to (i.e. beside or below) the security classification marking at least once on every page of a document;

(d) where applicable, the date or specific event after which it may be downgraded or declassified, such as:

(i) "CONFIDENTIEL UE/EU CONFIDENTIAL. From 1.1.2011: RESTREINT UE/EU RESTRICTED"; or
(ii) "DECLASSIFIED ON THE DATE OF PUBLICATION IN THE OJ").

Such markings should appear at least on the first page of a document.

VII. Classifying cover pages, excerpts, compilations

27. The overall classification level of a document or file will be at least as high as that of its most highly classified component. For example, a document or file containing unclassified components and SECRET UE/EU SECRET components will be classified SECRET UE/EU SECRET. Such components will be marked in accordance with paragraph 31 below.

28. When information from various sources is collated, the final product will be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts. For example, the collation of a number of documents classified RESTREINT UE/EU RESTRICTED may warrant classification at CONFIDENTIEL UE/EU CONFIDENTIAL (or higher) level.

29. The classification of a letter or note covering enclosures will be as high as the highest classification of its enclosures. The originator will indicate clearly at which level it is classified when detached from its enclosures by means of an appropriate marking, e.g.:

CONFIDENTIEL UE/EU CONFIDENTIAL
Without attachment(s) RESTREINT UE/EU RESTRICTED

30. Documents or files containing components with different classification levels are to be structured wherever possible so that components with a different classification level may be easily identified and detached if necessary.

31. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and shall be marked accordingly, including when stored in electronic form. The following standard abbreviations may be used within EU classified documents to indicate the classification level of sections or blocks of text of less than a single page:

TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

32. Such sections or blocks of texts may also be marked as LIMITE to indicate that they are internal to the Council.

33. Examples are provided in Annex III.

VIII. Preparing a classified document

34. A classified document may only be prepared where all the personnel, physical, procedural and Information Assurance requirements set out in the CSR are met. This implies, for example, that:

- in terms of personnel security, security clearance requirements apply for handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above;
- in terms of physical security, classified documents may only be prepared in a secure environment;
- in terms of procedural security, registration requirements apply to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above;
- in terms of Information Assurance requirements, EUCI may only be handled within accredited CIS. In addition, CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above must be protected against unintentional electromagnetic emanations ("TEMPEST security measures").

35. When creating an EU classified document:

(a) the originator must be clearly identifiable:

(b) the document is to be dated;

(c) each page is to be marked clearly with the classification level;

(d) each page is to be numbered;

(e) the document must bear a reference number and a subject. These are not classified information, unless marked as such with an abbreviated marking.

IX. Initial dissemination and further distribution

36. The originator establishes the initial "need-to-know" for the EUCI it has created by drawing up a distribution list. For information classified RESTREINT UE/EU RESTRICTED, copies can be made and distributed by the holder by appropriate means (i.e. in accordance with the requirements of the CSR in physical and technical terms). For information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, the distribution list (and any further instructions on distribution) is to be provided to the relevant registry, which will register and distribute the information.

37. Information classified TRES SECRET UE/EU TOP SECRET may only be further distributed with the prior written consent of the originator. Information classified SECRET UE/EU SECRET or below may be further distributed on instruction from the holder, provided that the originator has not imposed caveats on such further distribution.

38. In order to allow for the unique identification of copies in the case of a breach of security, each copy of a document classified CONFIDENTIEL UE/EU CONFIDENTIAL or above will be numbered on every page by means which prevent the deletion of the copy number. The copy number or an additional marking will allow for the identification of the registry which produced the copy.

V. Downgrading and declassification

39. Classification is to be maintained only as long as the information requires protection. When creating a document, the author will indicate where possible, and in particular for information classified RESTREINT UE/EU RESTRICTED, whether the document can be downgraded or declassified on a given date or following a specific event.

40. In order to avoid the unnecessary accumulation of classified information requiring appropriate security measures, the GSC [and Member States] will regularly review EU classified information held by it [them] to ascertain whether the classification level still applies. For EUCI which it has originated, the GSC will review the classification level at least every five years. As a general rule, information (in particular that classified as RESTREINT UE/EU RESTRICTED) should not remain classified for more than 30 years, so as to allow its transfer to the EU's historical archives[1].

41. EU classified information may be downgraded or declassified only with the authorisation of the originator and, if necessary, after discussion with other interested parties. Authorisation to downgrade or declassify will be confirmed in writing.

42. When the review of EUCI contained in an official Council document results in a recommendation to declassify it, it must be considered whether such document should be made public or bear the distribution marking LIMITE so that the information remains internal to the Council.

[1] Pursuant to Council Regulation (EEC, EURATOM) n° 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 43, 15.2.1983, p. 1), as amended.

X. Compromise of EUCI

43. The CSR (Article 13(5)) provide that *"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 applicable rules and regulations. Any individual who is responsible for compromising or losing EUCI shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations."*

44. As to the form which such disciplinary or legal action would take and to the applicable legal provisions:

(a) If EUCI is compromised by an EU official, he or she would be subject to disciplinary action commensurate with the seriousness of the compromise in accordance with the EU staff regulations[1], which foresee disciplinary measures ranging from a warning to dismissal.

This would be without prejudice to any legal action, which could be taken in accordance with either the host State law or the law of the official's State of origin.

(b) In the case of compromise of EUCI by a Member State official, disciplinary measures or legal action would be taken by the Member State in question, pursuant to the relevant provisions of its internal law regarding the compromise of classified information.

[1] Article 11 of the staff regulations provide that "*An official shall carry out his duties and conduct himself solely with the interests of the Communities in mind …*". Article 12 provides that "*An official shall refrain from any action or behaviour which might reflect adversely upon his position*". Finally, Article 17 of these regulations provides that "*An official shall refrain from any unauthorised disclosure of information received in the line of duty, unless that information has already been made public or is accessible to the public*".

(c) In the case of compromise of classified information received or provided by the EU under a security of information agreement concluded between the EU and a third State or international organisation, any individual responsible for such compromise would be liable to disciplinary measures according to the relevant rules and regulations of the Parties. Such measures would be without prejudice to any legal action in accordance with the respective laws or regulations applicable to the individual concerned within the respective Party.

45. On the basis of information provided by Member States, the GSC will keep an updated list of the legal provisions in force in Member States regarding criminal sanctions in the case of compromise of EUCI. This list is communicated to the Council Security Committee.

Practical classification guide

If the unauthorised disclosure of the document you are creating could…	i.e.	then you should classify it as…
be disadvantageous to the interests of the European Union or of one or more of the Member States	• adversely affect diplomatic relations • cause substantial distress to individuals • make it more difficult to maintain the operational effectiveness or security of Member States' or other contributors' deployed personnel • cause financial loss or facilitate improper gain or advantage for individuals or companies • breach undertakings to maintain the confidence of information provided by third parties • breach statutory restrictions on disclosure of information • prejudice the investigation or facilitate the commission of crime • disadvantage EU or Member States in commercial or policy negotiations with others • impede the effective development or operation of EU policies • undermine the proper management of the EU and its missions	RESTREINT UE/EU RESTRICTED
harm the essential interests of the European Union or of one or more of the Member States	• materially damage diplomatic relations, i.e. cause formal protest or other sanctions • prejudice individual security or liberty • cause damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the effectiveness of valuable security or intelligence operations • substantially undermine the financial viability of major organisations • impede the investigation or facilitate the commission of serious crime • work substantially against EU or Member States financial, monetary, economic and commercial interests • seriously impede the development or operation of major EU policies • shut down or otherwise substantially disrupt significant EU activities	CONFIDENTIEL UE/EU CONFIDENTIAL

If the unauthorised disclosure of the document you are creating could…	i.e.	then you should classify it as…
seriously harm the essential interests of the European Union or of one or more of the Member States	• raise international tensions • seriously damage relations with friendly States • threaten life directly or seriously prejudice public order or individual security or liberty • cause serious damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the continuing effectiveness of highly valuable security or intelligence operations • cause substantial material damage to EU or one of its Member States financial, monetary, economic and commercial interests	SECRET UE/EU SECRET
cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States	• threaten directly the internal stability of the EU or of one or more of its Member States or friendly States • cause exceptionally grave damage to relations with friendly States • lead directly to widespread loss of life • cause exceptionally grave damage to the operational effectiveness or security of Member States' or other contributors' deployed personnel, or to the continuing effectiveness of extremely valuable security or intelligence operations • cause severe long-term damage to the EU or Member States' economy.	TRES SECRET UE/EU TOP SECRET

ANNEX II

Summary of security measures

In a nutshell, the following security measures will apply to the document you are creating in accordance with the Council security rules. The contents of this table are purely indicative and do not replace the content of the security rules themselves, nor of security policies or guidelines implementing them.

	RESTREINT UE/ EU RESTRICTED	**CONFIDENTIEL UE/ EU CONFIDENTIAL**	**SECRET UE/ EU SECRET**	**TRES SECRET UE/ EU TOP SECRET**
Need-to-know	Yes	Yes	Yes	Yes
Security clearance	No	Yes	Yes	Yes
Registration for security purposes	No	Yes	Yes	Yes
Initial dissemination	Determined by originator through a distribution list; distribution may be carried out by originator	Determined by originator through a distribution list; distribution carried out by the relevant registry	Determined by originator through a distribution list; distribution carried out by the relevant registry	Determined by originator through a distribution list; distribution carried out by the relevant TRES SECRET UE/EU TOP SECRET registry
Copying, translation, further distribution	On instruction from the holder, unless otherwise specified by the originator	By the relevant registry, on instruction from the holder, unless otherwise specified by the originator	By the relevant registry, on instruction from the holder, unless otherwise specified by the originator	By the relevant TRES SECRET UE/EU TOP SECRET registry, subject to originator consent
Physical protection for handling	In administrative or secured areas, or outside such areas under conditions to be laid down by the competent security authority	In administrative or secured areas, or outside such areas under conditions to be laid down by the competent security authority	In administrative or secured areas, or outside such areas under conditions to be laid down by the competent security authority	Only in secured areas

	RESTREINT UE/ EU RESTRICTED	**CONFIDENTIEL UE/ EU CONFIDENTIAL**	**SECRET UE/ EU SECRET**	**TRES SECRET UE/ EU TOP SECRET**
Physical protection for storage	In administrative or secured areas, or temporarily outside such areas under conditions to be laid down by the competent security authority	Only in secured areas	Only in secured areas	Only in secured areas
CIS for handling and storing	Accredited	Accredited	Accredited	Accredited
TEMPEST measures	No	Yes	Yes	Yes
Carriage	(a) within a building or self-contained group of buildings: […] (b) within the EU: […] (c) from within the EU to the territory of a third State: […]	(a) within a building or self-contained group of buildings: […] (b) within the EU: […] (c) from within the EU to the territory of a third State: […]	(a) within a building or self-contained group of buildings: […] (b) within the EU: […] (c) from within the EU to the territory of a third State: […]	(a) within a building or self-contained group of buildings: […] (b) within the EU: […] (c) from within the EU to the territory of a third State: […]
Transmission by electronic means	Encrypted with authorised devices	Encrypted with authorised devices	Encrypted with authorised devices	Encrypted with authorised devices
Destruction	By holder, using approved methods	By registry, using approved methods	By registry, using approved methods and in the presence of a witness	By registry, using approved methods and in the presence of a witness

Fig. 1 - Example of a document containing parts (of less than a single page) with different classification levels:

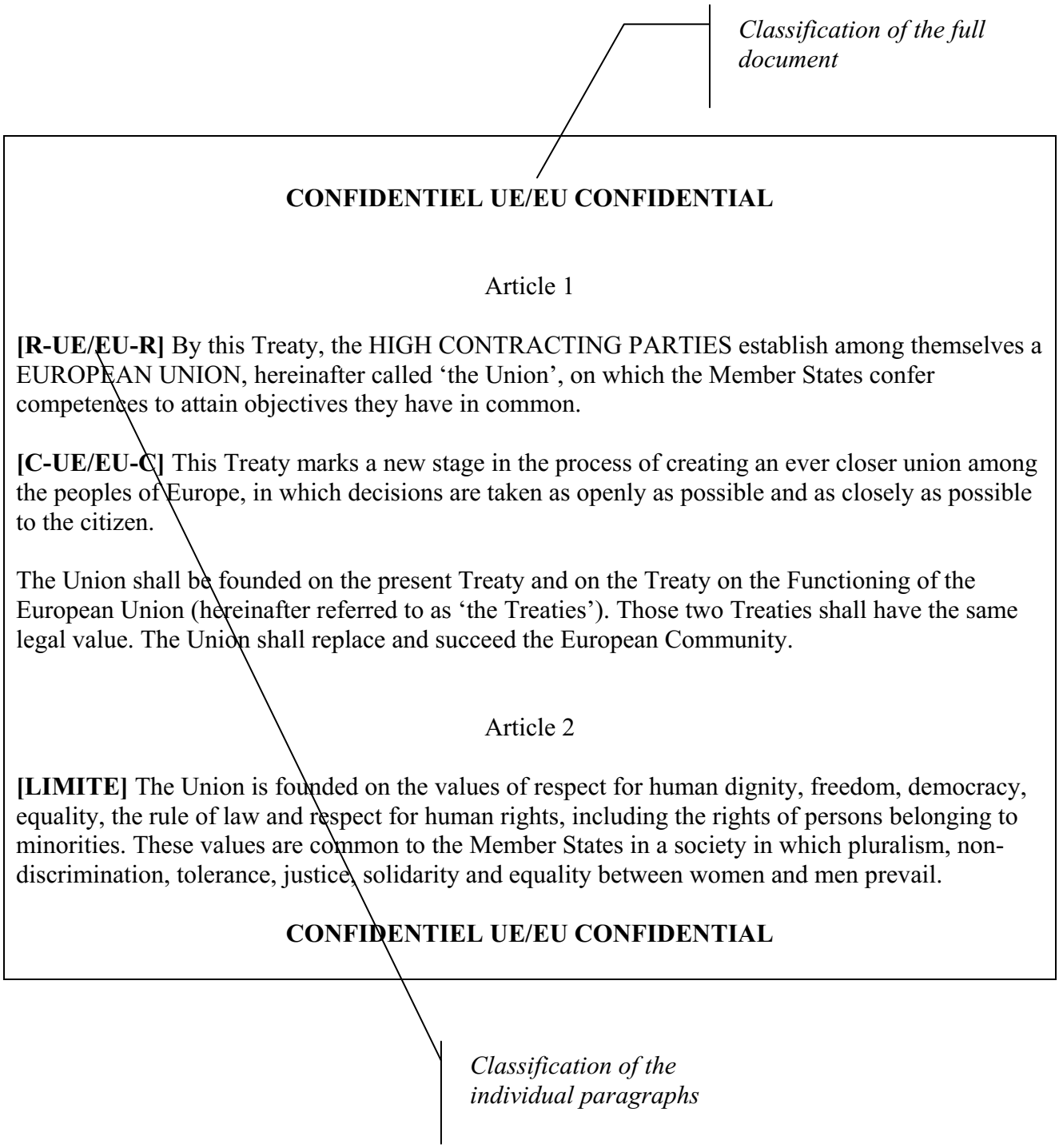

Fig 2 - Example of a web page containing documents with different classification levels: