Official Journal of the European Union

L 72

English edition

Legislation

Volume 58

17 March 2015

Contents

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

II

(Non-legislative acts)

REGULATIONS

COMMISSION IMPLEMENTING REGULATION (EU) 2015/434

of 16 March 2015

establishing the standard import values for determining the entry price of certain fruit and vegetables

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 1308/2013 of the European Parliament and of the Council of 17 December 2013 establishing a common organisation of the markets in agricultural products and repealing Council Regulations (EEC) No 922/72, (EEC) No 234/79, (EC) No 1037/2001 and (EC) No 1234/2007 ([1]),

Having regard to Commission Implementing Regulation (EU) No 543/2011 of 7 June 2011 laying down detailed rules for the application of Council Regulation (EC) No 1234/2007 in respect of the fruit and vegetables and processed fruit and vegetables sectors ([2]), and in particular Article 136(1) thereof,

Whereas:

(1) Implementing Regulation (EU) No 543/2011 lays down, pursuant to the outcome of the Uruguay Round multilateral trade negotiations, the criteria whereby the Commission fixes the standard values for imports from third countries, in respect of the products and periods stipulated in Annex XVI, Part A thereto.

(2) The standard import value is calculated each working day, in accordance with Article 136(1) of Implementing Regulation (EU) No 543/2011, taking into account variable daily data. Therefore this Regulation should enter into force on the day of its publication in the *Official Journal of the European Union*,

HAS ADOPTED THIS REGULATION:

Article 1

The standard import values referred to in Article 136 of Implementing Regulation (EU) No 543/2011 are fixed in the Annex to this Regulation.

([1]) OJ L 347, 20.12.2013, p. 671.
([2]) OJ L 157, 15.6.2011, p. 1.

Article 2

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

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 16 March 2015.

For the Commission,
On behalf of the President,
Jerzy PLEWA
Director-General for Agriculture and Rural Development

ANNEX

Standard import values for determining the entry price of certain fruit and vegetables

(EUR/100 kg)

CN code	Third country code (1)	Standard import value
0702 00 00	EG	65,8
	MA	84,9
	TR	86,4
	ZZ	79,0
0707 00 05	JO	229,9
	MA	183,9
	TR	185,1
	ZZ	199,6
0709 93 10	MA	119,5
	TR	192,4
	ZZ	156,0
0805 10 20	EG	45,8
	IL	72,7
	MA	56,7
	TN	57,3
	TR	63,6
	ZZ	59,2
0805 50 10	TR	61,4
	ZZ	61,4
0808 10 80	BR	70,9
	CA	81,0
	CL	100,9
	CN	91,1
	MK	25,2
	US	166,1
	ZZ	89,2
0808 30 90	AR	112,0
	CL	133,2
	US	124,8
	ZA	103,5
	ZZ	118,4

(1) Nomenclature of countries laid down by Commission Regulation (EU) No 1106/2012 of 27 November 2012 implementing Regulation (EC) No 471/2009 of the European Parliament and of the Council on Community statistics relating to external trade with non-member countries, as regards the update of the nomenclature of countries and territories (OJ L 328, 28.11.2012, p. 7). Code 'ZZ' stands for 'of other origin'.

DECISIONS

DECISION (EU) 2015/435 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 December 2014

on the mobilisation of the Contingency Margin

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to the Interinstitutional Agreement of 2 December 2013 between the European Parliament, the Council and the Commission on budgetary discipline, on cooperation in budgetary matters and on sound financial management ([1]), and in particular point 14 thereof,

Having regard to the proposal from the European Commission,

Whereas,

(1) Article 13 of Council Regulation (EU, Euratom) No 1311/2013 ([2]) has established a Contingency Margin of up to 0,03 % of the Gross National Income of the Union.

(2) In accordance with Article 6 of that Regulation, the Commission has calculated the absolute amount of the Contingency Margin for 2014 ([3]).

(3) After having examined all other financial possibilities to react to unforeseen circumstances that have arisen after the multiannual financial framework payment ceiling for 2014 was first established in February 2013, it appears necessary to mobilise the Contingency Margin to complement the payment appropriations in the general budget of the European Union for the financial year 2014, above the payment ceiling.

(4) An amount of EUR 350 million in payment appropriations should be included in the mobilisation of the Contingency Margin pending an agreement on payments for other special instruments.

(5) Having regard to the very particular situation which has arisen this year, the last-resort condition in Article 13(1) of Regulation (EU, Euratom) No 1311/2013 is fulfilled.

(6) To ensure compliance with Article 13(3) of Regulation (EU, Euratom) No 1311/2013, the Commission should present a proposal on the offsetting of the relevant amount in the MFF payment ceilings for one or more future financial years, having due regard to the agreement on payments for other special instruments, and without prejudice to the institutional prerogatives of the Commission,

([1]) OJ C 373, 20.12.2013, p. 1.
([2]) Council Regulation (EU, Euratom) No 1311/2013 of 2 December 2013 laying down the multiannual financial framework for the years 2014-2020 (OJ L 347, 20.12.2013, p. 884).
([3]) Communication from the Commission to the Council and the European Parliament of 20 December 2013 on the technical adjustment of the financial framework for 2014 in line with movements in GNI (COM(2013) 928).

HAVE ADOPTED THIS DECISION:

Article 1

For the general budget of the European Union for the financial year 2014, the Contingency Margin shall be used to provide the sum of EUR 3 168 233 715 in payment appropriations over and above the payment ceiling of the multiannual financial framework.

Article 2

The sum of EUR 2 818 233 715 shall be offset in three instalments against the margins under the payment ceilings for the following years:

(a) 2018: EUR 939 411 200;

(b) 2019: EUR 939 411 200;

(c) 2020: EUR 939 411 315.

The Commission is invited to present in a timely manner a proposal concerning the remaining amount of EUR 350 million.

Article 3

This decision shall be published in the *Official Journal of the European Union*.

Done at Strasbourg, 17 December 2014.

For the European Parliament	*For the Council*
The President	*The President*
M. SCHULZ	B. DELLA VEDOVA

DECISION (EU) 2015/436 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 December 2014

on the mobilisation of the European Union Solidarity Fund

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Council Regulation (EC) No 2012/2002 of 11 November 2002 establishing the European Union Solidarity Fund ([1]), and in particular Article 4(3) thereof,

Having regard to the Interinstitutional Agreement of 2 December 2013 between the European Parliament, the Council and the Commission on budgetary discipline, on cooperation in budgetary matters and on sound financial management ([2]), and in particular point 11 thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) The European Union has created a European Union Solidarity Fund (the 'Fund') to show solidarity with the population of regions struck by disasters.

(2) Article 10 of Council Regulation (EU, Euratom) No 1311/2013 ([3]) allows the mobilisation of the Fund within the annual ceiling of EUR 500 million (2011 prices).

(3) Regulation (EC) No 2012/2002 contains the provisions whereby the Fund may be mobilised.

(4) Italy has submitted an application to mobilise the Fund, concerning floods.

(5) Greece has submitted an application to mobilise the Fund, concerning an earthquake.

(6) Slovenia has submitted an application to mobilise the Fund, concerning ice storms.

(7) Croatia has submitted an application to mobilise the Fund, concerning ice storms followed by flooding,

HAVE ADOPTED THIS DECISION:

Article 1

For the general budget of the European Union for the financial year 2014, the European Union Solidarity Fund shall be mobilised to provide the sum of EUR 46 998 528 in commitment appropriations.

For the general budget of the European Union for the financial year 2015, the European Union Solidarity Fund shall be mobilised to provide the sum of EUR 46 998 528 in payment appropriations.

Article 2

This Decision shall be published in the *Official Journal of the European Union*.

Done at Strasbourg, 17 December 2014.

For the European Parliament	*For the Council*
The President	*The President*
M. SCHULZ	B. DELLA VEDOVA

([1]) OJ L 311, 14.11.2002, p. 3.
([2]) OJ C 373, 20.12.2013, p. 1.
([3]) Council Regulation (EU, Euratom) No 1311/2013 of 2 December 2013 laying down the multiannual financial framework for the years 2014-2020 (OJ L 347, 20.12.2013, p. 884).

DECISION (EU) 2015/437 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 December 2014

on the mobilisation of the European Union Solidarity Fund

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Council Regulation (EC) No 2012/2002 of 11 November 2002 establishing the European Union Solidarity Fund ([1]), and in particular Article 4(3) thereof,

Having regard to the Interinstitutional Agreement of 2 December 2013 between the European Parliament, the Council and the Commission on budgetary discipline, on cooperation in budgetary matters and on sound financial management ([2]), and in particular point 11 thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) The European Union has created a European Union Solidarity Fund (the 'Fund') to show solidarity with the population of regions struck by disasters.

(2) Article 10 of Council Regulation (EU, Euratom) No 1311/2013 ([3]) allows the mobilisation of the Fund within the annual ceiling of EUR 500 million (2011 prices).

(3) Regulation (EC) No 2012/2002 contains the provisions whereby the Fund may be mobilised.

(4) Serbia has submitted an application to mobilise the Fund, concerning floods.

(5) Croatia has submitted an application to mobilise the Fund, concerning floods.

(6) Bulgaria has submitted an application to mobilise the Fund, concerning floods,

HAVE ADOPTED THIS DECISION:

Article 1

For the general budget of the European Union for the financial year 2014, the European Union Solidarity Fund shall be mobilised to provide the sum of EUR 79 726 440 in commitment appropriations.

For the general budget of the European Union for the financial year 2015, the European Union Solidarity Fund shall be mobilised to provide the sum of EUR 79 726 440 in payment appropriations

Article 2

This Decision shall be published in the *Official Journal of the European Union*.

Done at Strasbourg, 17 December 2014.

For the European Parliament	*For the Council*
The President	*The President*
M. SCHULZ	B. DELLA VEDOVA

([1]) OJ L 311, 14.11.2002, p. 3.
([2]) OJ C 373, 20.12.2013, p. 1.
([3]) Council Regulation (EU, Euratom) No 1311/2013 of 2 December 2013 laying down the multiannual financial framework for the years 2014-2020 (OJ L 347, 20.12.2013, p. 884).

COUNCIL DECISION (EU) 2015/438

of 2 March 2015

establishing the position to be taken on behalf of the European Union within the Joint Committee set up under the Agreement between the European Union and Ukraine on the facilitation of the issuance of visas, with regard to the adoption of common guidelines for the implementation of the Agreement

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular point (a) of Article 77(2) in conjunction with Article 218(9) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) Article 12 of the Agreement between the European Union and Ukraine on the facilitation of the issuance of visas ([1]) ('the Agreement') sets up a Joint Committee. It provides that the Joint Committee is in particular to monitor the implementation of the Agreement.

(2) The Agreement between the European Union and Ukraine amending the Agreement between the European Community and Ukraine on the facilitation of the issuance of visas ([2]) ('the amending Agreement') entered into force on 1 July 2013.

(3) Regulation (EC) No 810/2009 of the European Parliament and of the Council ([3]) established the procedures and conditions for issuing visas for transit through or intended stays on the territory of the Member States not exceeding 90 days in any 180-day period.

(4) Within its responsibility, the Joint Committee noted the need for common guidelines in order to ensure a fully harmonised implementation of the Agreement amongst the consulates of the Member States, and for clarifying the relationship between the provisions of the Agreement and the provisions of the contracting parties that continue to apply to visa issues not covered by the Agreement.

(5) The Joint Committee adopted such guidelines on 25 November 2009 by its Decision No 1/2009. Those guidelines should be adapted to the new provisions of the Agreement introduced by the amending Agreement and to the changes in Union internal law on visa policy. In the interests of clarity it is appropriate to replace those guidelines.

(6) It is appropriate to establish the position to be adopted on the Union's behalf within the Joint Committee with regard to the adoption of common guidelines for the implementation of the Agreement,

HAS ADOPTED THIS DECISION:

Article 1

The position to be adopted on the Union's behalf within the Joint Committee set up by Article 12 of the Agreement between the European Union and Ukraine on the facilitation of the issuance of visas, with regard to the adoption of common guidelines for the implementation of the Agreement, shall be based on the draft Decision of the Joint Committee attached to this Decision.

([1]) OJ L 332, 18.12.2007, p. 68.
([2]) OJ L 168, 20.6.2013, p. 11.
([3]) Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

Article 2

This Decision shall enter into force on the date of its adoption.

Done at Brussels, 2 March 2015.

For the Council
The President
D. REIZNIECE-OZOLA

DRAFT

DECISION No …/2014 OF THE JOINT COMMITTEE SET UP BY THE AGREEMENT BETWEEN THE EUROPEAN UNION AND UKRAINE ON THE FACILITATION OF THE ISSUANCE OF VISAS

of …

with regard to the adoption of common guidelines for the implementation of the Agreement

THE JOINT COMMITTEE,

Having regard to the Agreement between the European Union and Ukraine on the facilitation of the issuance of visas ('the Agreement'), and in particular Article 12 thereof,

Whereas the Agreement entered into force on 1 January 2008,

HAS DECIDED THE FOLLOWING:

Article 1

The common guidelines for the implementation of the Agreement between the European Union and Ukraine on the facilitation of the issuance of visas are established in the annex to this Decision.

Article 2

Decision No 1/2009 of the Joint Committee is repealed.

Article 3

This Decision shall enter into force on the day of its adoption.

Done at…

For the European Union *For Ukraine*

ANNEX

COMMON GUIDELINES FOR THE IMPLEMENTATION OF THE AGREEMENT BETWEEN THE EUROPEAN UNION AND UKRAINE ON THE FACILITATION OF THE ISSUANCE OF VISAS

The purpose of the Agreement between the European Union and Ukraine on the facilitation of the issuance of visas, which entered into force on 1 January 2008, as amended by the Agreement between the European Union and Ukraine of 23 July 2012, which entered into force on 1 July 2013 ('the Agreement'), is to facilitate, on the basis of reciprocity, the procedures for issuing visas for an intended stay of no more than 90 days per period of 180 days to the citizens of Ukraine.

The Agreement establishes, on the basis of reciprocity, legally binding rights and obligations for the purpose of simplifying the visa issuing procedures for Ukrainian citizens.

These Guidelines, adopted by the Joint Committee established by Article 12 of the Agreement ('the Joint Committee'), aim at ensuring a correct and harmonised implementation of the provisions of the Agreement by the diplomatic missions and consular posts of the Member States. These Guidelines are not part of the Agreement and therefore they are not legally binding. However, it is highly recommended that diplomatic and consular staff consistently follow them when implementing the provisions of the Agreement.

These Guidelines are intended to be updated in light of experience of the implementation of the Agreement under the responsibility of the Joint Committee. The Guidelines adopted by the Joint Committee on 25 November 2009 have been adapted in line with the Agreement between the European Union and Ukraine amending the Agreement between the European Community and Ukraine on the facilitation of the issuance of visas ('the amending Agreement'), and with new Union legislation such as Regulation (EC) No 810/2009 of the European Parliament and of the Council [1] ('the Visa Code').

I. GENERAL ISSUES

1.1. **Purpose and scope of application**

Article 1 of the Agreement stipulates that: 'The purpose of this Agreement is to facilitate the issuance of visas for an intended stay of no more than 90 days per period of 180 days to the citizens of Ukraine.'.

The Agreement applies to all Ukrainian citizens who apply for a short-stay visa, whatever the country in which they reside.

Article 1(2) of the Agreement stipulates that: 'Ukraine may only reintroduce the visa requirement for citizens or certain categories of citizens of all Member States and not for citizens or certain categories of citizens of individual Member States. If Ukraine would reintroduce the visa requirement for EU citizens or certain categories of EU citizens, the same facilitations granted under this agreement to the Ukrainian citizens would automatically, on the basis of reciprocity, apply to EU citizens concerned.'.

According to the decisions taken by the Ukrainian government, as from 1 May 2005 or 1 January 2008 respectively, EU citizens are exempted from the visa requirement when travelling to Ukraine for a period of time not exceeding 90 days or transiting through the territory of Ukraine. This provision does not affect the right of the Ukrainian government to amend those decisions.

1.2. **Scope of the Agreement**

Article 2 of the Agreement stipulates that:

> '1. The visa facilitations provided in this Agreement shall apply to citizens of Ukraine only insofar as they are not exempted from the visa requirement by the laws and regulations of the European Union or the Member States, the present agreement or other international agreements.
>
> 2. The national law of Ukraine, or of the Member States or European Union law shall apply to issues not covered by the provisions of this Agreement, such as the refusal to issue a visa, recognition of travel documents, proof of sufficient means of subsistence and the refusal of entry and expulsion measures.'.

[1] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).

Without prejudice to its Article 10 (which provides for the exemption from the visa requirement for holders of diplomatic passports and biometric service passports of Ukraine), the Agreement does not affect the existing rules on visa obligations and visa exemptions. For instance, Article 4 of Council Regulation (EC) No 539/2001 ([1]) allows Member States to exempt from the visa requirement civilian air and sea crews among other categories.

Schengen rules and, where appropriate, national law continue to apply to all issues not covered by the Agreement such as the refusal to issue a visa, recognition of travel documents, proof of sufficient means of subsistence, the refusal of entry, and expulsion measures. This also applies to the Schengen rules determining the Schengen Member State responsible for processing a visa application. Therefore, a Ukrainian citizen should continue to apply for a visa to the consulate of the Member State of the main destination of his/her travelling; if there is no main destination, (s)he should apply to the consulate of the Member State of first entry into the Schengen area.

Even if the conditions foreseen in the Agreement are met, for example, proof of documentary evidence regarding the purpose of the journey for the categories foreseen in its Article 4 is provided by the visa applicant, the issuance of the visa still can be refused if the conditions laid down in Article 5 of Regulation (EC) No 562/2006 of the European Parliament and of the Council ([2]) ('the Schengen Borders Code') are not fulfilled, i.e. the person is not in possession of a valid travel document, an alert in the SIS has been issued, the person is considered a threat for public policy, internal security, etc.

Other possibilities for flexibility in the issuing of visas allowed in the Visa Code for issuing visas continue to apply. For instance, multiple-entry visas for a long period of validity- up to five years- can be issued to categories of persons other than those mentioned in Article 5 of the Agreement, if the conditions foreseen in the Visa Code are met (cfr. Article 24(2) of the Visa Code). In the same way, the provisions contained in the Visa Code allowing waiver or reduction of the visa fee will continue to apply (cfr. II.2.1.1).

1.3. **Types of visas falling within the scope of the Agreement**

Article 3(d) of the Agreement defines 'visa' as 'an authorisation issued by a Member State or a decision taken by such State which is required with a view to:

— entry for an intended stay in that Member State or in several Member States of no more than 90 days in total,

— entry for transit through the territory of that Member State or several Member States;'.

The following type of visas is covered by the Agreement:

— 'C' visas (short-stay visas).

The facilitations provided by the Agreement apply both to uniform visas valid for the entire territory of the Member States and to visas with limited territorial validity (LTV).

1.4. **Calculation of the length of stay authorised by a visa and in particular the question on how to determine the six month period**

The recent modification of the Schengen Borders Code has re-defined the notion of short stay. The current definition reads as follows: '90 days in any 180 day-period, which entails considering the 180-day period preceding each day of stay'.

The day of entry will be calculated as the first day of stay in the territory of the Member States and the day of exit will be calculated as the last day of stay in the territory of the Member States. The notion of 'any' implies the application of a 'moving' 180-day reference period, looking at each day of the stay back to the last 180 days period, in order to verify if the 90/180 day requirement continues to be fulfilled. This means that an absence for an uninterrupted period of 90 days allows for a new stay of up to 90 days.

The definition entered into force on 18 October 2013. The calculator may be found on-line at the following address: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/index_en.htm

([1]) Council Regulation (EC) No 539/2001 of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement (OJ L 81, 21.3.2001, p. 1).

([2]) Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ L 105, 13.4.2006, p. 1).

Example of calculation of stay on the basis of the new definition:

A person holding a multiple-entry visa for 1 year (18.4.2014 – 18.4.2015) enters for the first time on 19.4.2014 and stays for 3 days. Then he enters again on 18.6.2014 and stays for 86 days. What is the situation on specific dates? When will this person be allowed to enter again?

On 11.9.2014: Over the last 180 days (16.3.2014 – 11.9.2014) the person had stayed for 3 days (19. – 21.4.2014) plus 86 days (18.6.2014 – 11.9.2014) = 89 days = No overstay. The person may still stay for up to 1 day.

As of 16.10.2014: The person might enter for a stay of 3 additional days (on 16.10.2014 the stay on 19.4.2014 becomes irrelevant (outside the 180 days period); on 17.10.2014 the stay on 20.4.2014 becomes irrelevant (outside the 180 days period; etc.).

As of 15.12.2014: The person might enter for 86 additional days (on 15.12.2014, the stay on 18.6.2014 becomes irrelevant (outside the 180 days period); on 16.12.2014, the stay on 19.6.2014 becomes irrelevant, etc.).

1.5. **Situation regarding the Member States that do not yet fully apply the Schengen *acquis*, the Member States that do not participate in the EU Common Visa Policy and associated countries**

Member States that joined the Union in 2004 (the Czech Republic, Estonia, Cyprus, Latvia, Lithuania, Hungary, Malta, Poland, Slovenia and Slovakia), 2007 (Bulgaria and Romania), and 2013 (Croatia) are bound by the Agreement as from its entry into force.

Only Bulgaria, Croatia, Cyprus and Romania do not yet fully implement the Schengen *acquis*. They will continue issuing national visas with a validity limited to their own national territory. Once those Member States fully implement the Schengen *acquis*, they will continue to apply the Agreement.

National law continues to apply to all issues not covered by the Agreement until the date of full implementation of the Schengen *acquis* by those Member States. As from that date, Schengen rules/national law will apply to issues not regulated by the Agreement.

Bulgaria, Croatia, Cyprus and Romania are authorised to recognise residence permits, D visas and short stay visas issued by Schengen States and associated countries for short stays on their territory.

According to Article 21 of the Convention Implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at the common borders, all Schengen States must recognise the long-stay visas and residence permits issued by each other as valid for short stays on each other's territories. Schengen Member States accept residence permits, D visas and short stay visas of associated countries for entry and short stay and vice versa.

The Agreement does not apply to Denmark, Ireland and the United Kingdom but comprises joint declarations about the desirability of those Member States to conclude bilateral agreements on visa facilitation with Ukraine.

A bilateral agreement on visa facilitation between Denmark and Ukraine entered into force on 1 March 2009. No negotiations on visa facilitation have taken place between Ukraine and, respectively, Ireland and the United Kingdom.

Although associated to Schengen, the Agreement does not apply to Iceland, Liechtenstein, Norway and Switzerland but comprises joint declarations about the desirability of those Schengen countries to conclude bilateral agreements on visa facilitation with Ukraine.

Norway has signed a bilateral visa facilitation agreement on 13 February 2008. That agreement entered into force on 1 September 2011.

Switzerland finalised the negotiations on a bilateral visa facilitation agreement in November 2011. Iceland has indicated that negotiations with Ukraine have begun.

1.6. **The Agreement/bilateral agreements**

Article 13(1) of the Agreement stipulates that:

> '1. As from its entry into force, this Agreement shall take precedence over provisions of any bilateral or multilateral agreements or arrangements concluded between individual Member States and Ukraine, insofar as the provisions of the latter agreements or arrangements cover issues dealt with by the present Agreement.'.

As from the date of entry into force of the Agreement, provisions in the bilateral agreements in force between Member States and Ukraine on issues dealt with by the Agreement ceased to apply. In accordance with Union law, Member States have to take the necessary measures to eliminate the incompatibilities between their bilateral agreements and the Agreement.

However, Article 13(2) of the Agreement stipulates that:

> '2. The provisions of bilateral Agreements or arrangements between individual Member States and Ukraine concluded before the entry into force of this Agreement providing for the exemption of the holders of non-biometric service passports from the visa requirement shall continue to apply without prejudice to the right of the Member States concerned or Ukraine to denounce or suspend these bilateral agreements or arrangements.'.

The following Member States have a bilateral agreement with Ukraine providing for the exemption from the visa obligation for holders of service passports: Bulgaria, Croatia, Cyprus, Latvia, Lithuania, Hungary, Poland, Romania and Slovakia.

In accordance with Article 13(1) of the Agreement, in so far as those bilateral agreements cover biometric service passport holders, Article 10(2) of the Agreement takes precedence over those bilateral agreements. In accordance with Article 13(2) of the Agreement, those bilateral agreements, which were concluded before the entry into force of the amending Agreement, continue to apply in so far as they cover non-biometric service passport holders, without prejudice to the right of the Member States concerned or Ukraine to denounce or suspend those bilateral agreements or arrangements. The visa exemption for the holders of non-biometric service passport granted by a Member State only applies for travelling on the territory of that Member State and not for travelling to the other Schengen Member States.

Should a Member State have concluded a bilateral agreement or arrangement with Ukraine on issues not covered by the Agreement, that exemption would continue to apply after the entry into force of the Agreement.

1.7. **European Community Declaration on access of visa applicants and harmonisation of information on procedures for issuing short-stay visas and documents to be submitted when applying for short-stay visas**

In accordance with that European Community Declaration attached to the Agreement, common basic information on access of visa applicants to diplomatic missions and consular posts of the Member States and on the procedures and conditions for issuing visas and on the validity of visas issued has been drafted to ensure that applicants are given coherent and uniform information. That information is available at website of the EU Delegation to Ukraine: http://eeas.europa.eu/delegations/ukraine/index_en.htm

Diplomatic missions and consular posts of the Member States are requested to disseminate widely this information (on the information boards, in leaflets, on websites, etc.) and to disseminate also precise information on the conditions for issuing visas, representation of Member States in Ukraine and the harmonised EU list of required supporting documentation.

II. GUIDELINES ON SPECIFIC PROVISIONS

2.1. **Rules that apply to all visa applicants**

Important: It is recalled that the facilitations mentioned below regarding the visa handling fee, the length of procedures for processing visa applications, departure in case of lost or stolen documents, and the extension of visa in exceptional circumstances apply to all Ukrainian visa applicants and visa holders.

2.1.1. *Visa handling fee*

Article 6(1) of the Agreement stipulates that:

> 'The fee for processing visa applications of Ukrainian citizens shall amount to EUR 35. The aforementioned amount may be reviewed in accordance with the procedure provided for in Article 14(4).'.

In accordance with Article 6(1), the fee for processing a visa application is 35 EUR. That fee will apply to all Ukrainian visa applicants (including tourists) and concerns short-stay visas, irrespective of the number of entries. It also applies to visa applications lodged at the external borders.

Article 6(2) of the Agreement stipulates that:

> 'If Ukraine would reintroduce the visa requirement for EU citizens, the visa fee to be charged by Ukraine shall not be higher than EUR 35 or the amount agreed if the fee is reviewed in accordance with the procedure provided for in Article 14(4).'.

Article 6(3) of the Agreement stipulates that:

> 'The Member States shall charge a fee of EUR 70 for processing visas in cases where, based on the distance between the applicant's place of residence and the place where the application has been submitted, the applicant has requested that a decision on the application be taken within three days of its submission, and the consulate has accepted to take a decision within three days.'.

A EUR 70 fee will be charged for processing visa applications in cases where the visa application and the supporting documents have been submitted by the visa applicant whose place of residence is known to be in the oblast in which the Member State to which the applicant wishes to travel has no consular representation (if in that oblast there is no consulate, nor visa centre, nor consulates of the Member States that have concluded representation agreements with the Member State to which the applicant wishes to travel), and when the diplomatic mission or consular post has agreed to take a decision on the visa application within three days. Evidence regarding the place of residence of visa applicant is provided in the visa application form.

In principle, Article 6(3) of the Agreement aims at facilitating applying for a visa by the applicants living at a large distance from the consulate. Should a long trip be needed in order to apply for the visa, the aim is to issue it quickly, so that the applicant can receive the visa without having the need of undertaking the same lengthy travel for a second time.

For the above mentioned reasons, in cases where the 'standard' processing time for a visa application by a given diplomatic mission or consular post takes three days or less, the standard EUR 35 visa fee will be charged.

For diplomatic missions and consular posts that have an appointment system, the period of time to get an appointment is not counted as part of the processing time (see also II.2.1.2).

Article 6(4) of the Agreement stipulates that:

> '4. Without prejudice to paragraph 5 fees for processing the visa application are waived for the following categories of persons:
>
> (a) for close relatives — spouses, children (including adopted) parents (including custodians), grandparents and grandchildren — of citizens of Ukraine legally residing in the territory of the Member States or citizens of the European Union residing in the territory of the Member State of which they are nationals;'

(N.B. That point regulates the situation of Ukrainian close relatives travelling to the Member States to visit Ukrainian citizens legally residing in the Member States or citizens of the European Union residing in the territory of the Member State of which they are nationals. Ukrainian visa applicants who are family members of a Union citizen, in the meaning of Article 5(2) of Directive 2004/38/EC of the European Parliament and of the Council ([1]), will be issued visas free of charge, as soon as possible and on the basis of an accelerated procedure.)

> '(b) for members of official delegations who, following an official invitation addressed to Ukraine, shall participate in meetings, consultations, negotiations or exchange programmes, as well as in events held in the territory of one of the Member States by intergovernmental organisations;
>
> (c) members of national and regional Governments and Parliaments, Constitutional Courts and Supreme Courts, in case they are not exempted from the visa requirement by the present Agreement;
>
> (d) pupils, students, post-graduate students and accompanying teachers who undertake trips for the purpose of study or educational training;
>
> (e) disabled persons and the person accompanying them, if necessary;' (N.B. In order to benefit from the fee waiver, evidence should be provided that each of visa applicants falls under this category.)
>
> '(f) persons who have presented documents proving the necessity of their travel on humanitarian grounds, including to receive urgent medical treatment and the person accompanying such person, or to attend a funeral of a close relative, or to visit a close relative seriously ill;
>
> (g) participants in international sports events and persons accompanying them;' (N.B. Only accompanying persons travelling in a professional capacity are covered; supporters will thus not be considered as accompanying persons.)

([1]) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

'(h) persons participating in scientific, cultural and artistic activities including university and other exchange programmes;

(i) participants in official exchange programmes organised by twin cities and other municipal entities;

(j) journalists and the technical crew accompanying them in a professional capacity;' (N.B. journalists covered by Article 4(1)(e) of the Agreement are covered by this point.)

'(k) pensioners;' (N.B. In order to benefit of the waiving of the fee from this category, visa applicants have to present evidence proving their pensioner status.)

'(l) drivers conducting international cargo and passenger transportation services to the territories of the Member States in vehicles registered in Ukraine;

(m) members of train, refrigerator and locomotive crews in international trains, travelling to the territories of the Member States;

(n) children under the age of 18 and dependant children under the age of 21;' (N.B. In order to benefit from the fee waiver for this category, visa applicants have to present evidence proving their age; and –if under the age of 21– in addition proving their dependency.)

'(o) representatives of the religious communities;

(p) for members of the professions participating in international exhibitions, conferences, symposia, seminars or other similar events held in the territory of the Member States;

(q) participants aged 25 years or less in seminars, conferences, sports, cultural or educational events, organised by non-profit organisations;

(r) representatives of civil society organisations undertaking trips for the purposes of educational training, seminars, conferences, including in the framework of exchange programmes;

(s) for participants in official European Union cross-border cooperation programmes, such as under the European Neighbourhood and Partnership Instrument (ENPI).

The first subparagraph shall apply also where the purpose of the journey is transit.'.

The second subparagraph of Article 6(4) of the Agreement applies only if the purpose of travel to the third country is equivalent to one of the purposes listed under points (a) to (s) of Article 6(4) of the Agreement e.g. if the transit is needed to attend a seminar, to visit family members, to participate in an exchange programme of civil society organisations, etc. in the third country.

The fee is fully waived for the abovementioned categories of persons. Moreover, according to Article 16(6) of the Visa Code 'in individual cases, the amount of the fee to be charged may be waived or reduced when to do so serves to promote cultural or sporting interests as well as interests in the field of foreign policy, development policy, other areas of vital public interest or for humanitarian reasons.'.

However, that rule cannot be applied to waive the EUR 70 visa fee for processing visas in individual cases where the visa application and the supporting documents have been submitted by the visa applicant whose place of residence is known to be based far away from the diplomatic mission or consular post of the Member State and who belongs to one of the visa fee exempted categories listed in Article 6(4) of the Agreement.

It should also be recalled that categories of persons exempted from the visa fee could still be subject to a service fee in case a Member State cooperates with an external service provider.

Article 6(5) of the Agreement stipulates that:

'5. If a Member State cooperates with an external service provider in view of issuing a visa the external service provider may charge a service fee. This fee shall be proportionate to the costs incurred by the external service provider while performing its tasks and shall not exceed EUR 30. The Member States shall maintain the possibility for all applicants to lodge their applications directly at their consulates. If applicants are required to obtain an appointment for the lodging of an application the appointment shall, as a rule, take place within a period of two weeks from the date when the appointment was requested.'.

Maintaining the possibility for all categories of visa applicants to lodge their applications directly at the consulate instead of through an external service provider implies that there should be a genuine choice between those two possibilities. Even if direct access does not have to be organised under identical or similar conditions to those for access to the service provider, the conditions should not make direct access impossible in practice. Even if it is acceptable to have a different waiting time for obtaining an appointment in the case of direct access, the waiting time should not be so long that it would render direct access impossible in practice.

2.1.2. *Length of procedures for processing visa applications*

Article 7 of the Agreement stipulates that:

> '1. Diplomatic missions and consular posts of the Member States shall take a decision on the request to issue a visa within 10 calendar days of the date of the receipt of the application and documents required for issuing the visa.
>
> 2. The period of time for taking a decision on a visa application may be extended up to 30 calendar days in individual cases, notably when further scrutiny of the application is needed.
>
> 3. The period of time for taking a decision on a visa application may be reduced to two working days or less in urgent cases.'.

A decision on the visa application will be taken, in principle, within 10 calendar days of the date of the receipt of the complete visa application and supporting documents.

That period may be extended up to 30 calendar days when further scrutiny is needed- for example, for consultation of central authorities.

All those deadlines start running only when the application file is complete, i.e. as from the date of reception of the visa application and the supporting documents.

For diplomatic missions and consular posts that have an appointment system, the period of time to get an appointment is not counted as part of the processing time. When setting the appointment, account should be taken of possible urgency claimed by the visa applicant in view of the implementation of Article 7(3) of the Agreement. As a rule, appointments should take place within a period of two weeks from the date when the appointment was requested (cfr. Article 6(5) of the Agreement). A longer period should be an exception, including in peak periods. The Joint Committee will monitor this issue carefully. The Member States will endeavour to ensure that appointments at the request of the members of official delegations of Ukraine to lodge applications at diplomatic missions and consular posts should take place as soon as possible, preferably within a period of two working days, in urgent cases when the invitation has been sent out late.

The decision about the reduced time for taking a decision on a visa application as defined in Article 7(3) of the Agreement is taken by the consular officer.

2.1.3. *Extension of visa in exceptional circumstances*

Article 9 of the Agreement stipulates that:

> 'The citizens of Ukraine who do not have the possibility to leave the territory of the Member States by the time stated in their visas for reasons of force majeure shall have the term of their visas extended free of charge in accordance with the legislation applied by the receiving State for the period required for their return to the State of their residence.'.

Regarding the possibility of extending the validity of the visa in cases of force majeure -for instance, stay in a hospital due to unforeseen reasons/sudden illness/accident — where the holder of the visa does not have the possibility to leave the territory of the Member State by the date stated in the visa, the provisions of the Article 33(1) of the Visa Code apply as long as they are compatible with the Agreement (for example, the extended visa remains a uniform visa, entitling entry to the territory of all the Schengen Member States for which the visa was valid at the time of issue). However, under the Agreement the extension of the visa is done for free in case of force majeure.

2.2. **Rules that apply to certain categories of visa applicants**

2.2.1. *Documentary evidence regarding the purpose of the journey*

For all the categories of persons listed in Article 4(1) of the Agreement including drivers conducting international cargo and passenger transportation services, only the indicated documentary evidence will be required regarding the purpose of the journey. For those categories of applicants no other documents regarding the purpose of stay must be asked for. As stated in Article 4(3) of the Agreement, no other justification, invitation or validation regarding the purpose of the journey will be required.

If in individual cases doubts remain regarding the real purpose of the journey, the visa applicant will be called for an (additional) in depth interview to the embassy/consulate where (s)he can be questioned regarding the actual purpose of the visit or the applicant's intention to return- cfr. Article 21(8) of the Visa Code. In such individual cases, additional documents can be provided by the visa applicant or exceptionally requested by the consular officer. The Joint Committee will closely monitor the issue.

For the categories of persons not mentioned in Article 4(1) of the Agreement, the current rules continue to apply regarding documentation proving the purpose of the journey. The same applies to documents regarding parents' consent for travel of children under 18 years old.

Schengen rules or national law apply to issues not covered by the provisions of the Agreement, such as recognition of travel documents, travel medical insurance and guarantees regarding return and sufficient means of subsistence (cfr. I.1.2).

In line with the European Union Declaration on documents to be submitted when applying for short-stay visas, attached to the amending Agreement, 'the European Union will establish a harmonised list of supporting documents, in accordance with Article 48(1)(a) of the Visa Code, in order to ensure that applicants from Ukraine are required to submit, in principle, the same supporting documents'. Member States' consulates, acting in Local Schengen Cooperation, are asked to ensure that Ukrainian visa applicants are given coherent and uniform basic information and are required to submit, in principle, the same supporting documents irrespectively of the consulate of the Member State where they apply.

In principle, the original request or certificate of the document required by Article 4(1) of the Agreement will be submitted with the visa application. However, the consulate can start processing the visa application with facsimile or copies of the request or certificate of the document. Nevertheless, the consulate may ask for the original document in case of the first application and will ask for it in individual cases where there are doubts.

As the below lists of authorities sometimes also contain the name of the person who can sign the relevant requests/certificates, the Ukrainian authorities should inform the Local Schengen Cooperation when those persons are replaced.

Article 4 of the Agreement stipulates that:

'1. For the following categories of citizens of Ukraine, the following documents are sufficient for justifying the purpose of the journey to the other Party:

(a) for members of official delegations who, following an official invitation addressed to Ukraine, shall participate in meetings, consultations, negotiations or exchange programmes, as well as in events held in the territory of one of the Member States by intergovernmental organisations:

— a letter issued by an Ukrainian authority confirming that the applicant is a member of its delegation travelling to the other Party to participate at the aforementioned events, accompanied by a copy of the official invitation;'

The applicant's name must be indicated in the letter issued by the competent authority confirming that the person is part of the delegation travelling to the territory of the other Party to participate in the official meeting. The name of the applicant must not necessarily also be indicated in the official invitation to participate in the meeting, although this might be the case when the official invitation is addressed to a specific person.

That provision applies to members of official delegations whatever the passport (non-biometric service or ordinary passport) they hold.

'(b) for business people and representatives of business organisations:

— a written request from a host legal person or company, or an office or a branch of such legal person or company, State and local authorities of the Member States or organising committees of trade and industrial exhibitions, conferences and symposia held in the territories of the Member States;

(c) for drivers conducting international cargo and passenger transportation services to the territories of the Member States in vehicles registered in Ukraine:

— a written request from the national association of carriers of Ukraine providing for international road transportation, stating the purpose, duration, destination(s), and frequency of the trips;'

The competent authorities that provide for the international road transportation and are responsible for stating the purpose, duration, destination(s) and frequency of the trips of the drivers conducting international cargo and passenger transportation services to the territories of the Member States in vehicles registered in Ukraine, are:

1. Association of International Road Carriers of Ukraine (AsMAP/'АсМАП')

   The mailing address of the AsMAP is:

   11, Shorsa str.

   Kyiv, 03150, Ukraine

   Officials entitled to sign the requests are:

   Kostiuchenko Leonid — President of the AsMAP of Ukraine;

   Dokil' Leonid — Vice-President of the AsMAP of Ukraine;

   Kuchynskiy Yurii — Vice-President of the AsMAP of Ukraine.

2. State Enterprise 'Service on International Road Carriages' (SE 'SIRC')

   The mailing address of the SE 'SIRC' is:

   57, av. Nauka

   Kyiv, 03083, Ukraine

   Tel. +38 044 524 21 01

   Fax +38 044 524 00 70

   Officials entitled to sign the requests are:

   Tkachenko Anatolij — Director of the SE 'SIRC';

   Neronov Oleksandr — First Deputy Director of the SE 'SIRC'.

3. Ukrainian Road Transport and Logistics Union

   The mailing address of the Ukrainian Road Transport and Logistics Union is:

   28, Predslavinska str.

   Kyiv, 03150, Ukraine

   Tel./fax +38 044 528 71 30/+38 044 528 71 46/+38 044 529 44 40

   Official entitled to sign the requests is:

   Lypovskiy Vitalij — President of the Union

4. All-Ukrainian Association of Automobile Carriers (AAAC) (Всеукраїнська асоціація автомобільних перевізників)

   The mailing address of the AAAC is:

   139, Velyka Vasylkivska str.

   Kyiv, 03150, Ukraine

   Tel./fax +38044-538-75-05, +38044-529-25-21

   Officials entitled to sign the requests are:

   Reva Vitalii (Віталій Рева) — President of the AAAC

   Glavatskyi Petro (Петро Главатський) — Vice President of the AAAC

   e-mail: vaap@i.com.ua

5. All-Ukrainian Association of Automobile Carriers (AAAC) (Всеукраїнська асоціація автомобільних перевізників)

   The mailing address of the AAAC is:

   3, Rayisy Okipnoyi str.

   Kyiv, 02002, Ukraine

   Tel./fax +38044-517-44-31, +38044-516-47-26

   Officials entitled to sign the requests are:

   Vakulenko Volodymyr (Вакуленко Володимир Михайлович) — Vice President of the AAAC

6. Ukrainian State Enterprise 'Ukrinteravtoservice' (Українське державне підприємство по обслуговуванню іноземних та вітчизняних автотранспортних засобів 'Укрінтеравтосервіс')

   The mailing address of the Ukrainian State Enterprise 'Ukrinteravtoservice' is:

   57, av. Nauky

   Kyiv, 03083, Ukraine

   Officials entitled to sign the requests are:

   Dobrohod Serhii (Доброход Сергій Олександрович) — Director-General of the Ukrainian State Enterprise 'Ukrinteravtservice' (phone: +38 044 524-09-99; cell. +38 050 463-89-32);

   Kubalska Svitlana (Кубальська Світлана Сергіївна) — Deputy Director-General of the Ukrainian State Enterprise 'Ukrinteravtoservice' (phone: +38 044 524-09-99; cell. +38 050 550-82-62);

Taking into account the current problems with that category of visa applicants the Joint Committee will closely monitor the implementation of that provision.

'(d) for members of train, refrigerator and locomotive crews in international trains, travelling to the territories of the Member States:

— a written request from the competent railway company of Ukraine stating the purpose, duration and frequency of the trips;'

The competent authority in the field of the rail transportation of Ukraine is the State Administration of Railway Transport of Ukraine ('Ukrzaliznytsia'/'Укрзалізниця').

The mailing address of 'Ukrzaliznytsia' is:

5-7 Tverskaya str.
Kyiv, 03680, Ukraine

According to the responsibility allocation in the leadership of 'Ukrzaliznytsia', the officials in charge responsible for providing the information concerning the purpose, duration and frequency of the trips of the members of train, refrigerator and locomotive crews in international trains traveling to the territories of the Member States are:

Bolobolin Serhii (Болоболін Сергій Петрович) — First Director-General of Ukrzaliznytsia (phone: +38 044 465 00 10);

Serhiyenko Mykola (Сергієнко Микола Іванович) — First Deputy Director-General of Ukrzaliznytsia (phone: +38 044 465 00 01);

Zhurakivskyy Vitaliy (Жураківський Віталій Олександрович) — First Deputy Director-General of Ukrzaliznytsia (phone: +38 044 465 00 41);

Slipchenko Oleksiy (Сліпченко Олексій Леонтійович) — Deputy Director-General of Ukrzaliznytsia (phone: +38 044 465 00 14);

Naumenko Petro (Науменко Петро Петрович) –Deputy Director-General of Ukrzaliznytsia (phone: +38 044 465 00 12);

Chekalov Pavlo (Чекалов Павло Леонтійович) — Deputy Director-General of Ukrzaliznytsia (phone: +38 044 465 00 13);

Matviiv Igor — Head of the Department of International Relations of Ukrzaliznytsia (phone: +38 044 465 04 25).

'(e) for journalists and the technical crew accompanying them in a professional capacity:

— a certificate or other document issued by a professional organisation or the applicant's employer proving that the person concerned is a qualified journalist and stating that the purpose of the journey is to carry out journalistic work or proving that the person is a member of the technical crew accompanying the journalist in a professional capacity;'

This category does not cover free-lance journalists.

The certificate or document proving that the applicant is a professional journalist and the original document issued by his/her employer stating that the purpose of the journey is to carry out a journalistic work or proving that the person is a member of the technical crew accompanying the journalist in a professional capacity must be presented.

The competent Ukrainian professional organisation proving that the person concerned is a qualified journalist is:

1. National Union of Journalists of Ukraine (NUJU) ('Національна спілка журналістів України', НСЖУ).

   NUJU issues to the qualified mass-media employees the national professional journalist's cards and international press-cards of the standard pattern set by the International Federation of Journalists.

   The mailing address of the NUJU is:

   27-a Khreschatyk str.

   Kyiv, 01001, Ukraine

   The authorized person of the NUJU is:

   Nalyvaiko Oleg Igorovych (Наливайко Олег Ігорович) — Head of the NUJU

   Phone/Fax +38044-234-20-96; +38044-234-49-60; +38044-234-52-09

   e-mail: spilka@nsju.org; admin@nsju.org.

2. Independent Media Union of Ukraine (IMUU) ('Незалежна медіа-профспілка України').

   The mailing address of the IMUU is:

   Office 25,

   27 — A, Khreshchatyk Str.,

   Kyiv, 01001, Ukraine

   The authorized persons are:

   Lukanov Yurii (Луканов Юрій Вадимович)– Head of the IMUU

   Vynnychuk Oksana (Оксана Винничук) — Executive Secretary of the IMUU

   Phone + 38 050 356 57 58

   e-mail: secretar@profspilka.org.ua

'(f) for persons participating in scientific, cultural and artistic activities, including university and other exchange programmes:

— a written request from the host organisation to participate in those activities;

(g) for pupils, students, post-graduate students and accompanying teachers who undertake trips for the purposes of study or educational training, including in the framework of exchange programmes as well as other school related activities:

— a written request or a certificate of enrolment from the host university, college or school or student cards or certificates of the courses to be attended;'

A student card can only be accepted as justification of the purpose of the journey when it is issued by the host university, college or school where the studies or educational training is going to take place.

'(h) for participants in international sports events and persons accompanying them in a professional capacity:

— a written request from the host organisation: competent authorities, national sport Federations and National Olympic Committees of the Member States;'

The list of accompanying persons in case of international sports events will be limited to those accompanying the sportsman/woman in a professional capacity: coaches, masseurs, manager, medical staff and head of the sports club. Supporters will not be considered as accompanying persons.

'(i) for participants in official exchange programmes organised by twin cities and other municipal entities:

— a written request of the Head of Administration/Mayor of those cities or other municipal entities;'

The Head of Administration/Mayor of the city or other municipal entity competent to issue the written request is the Head of Administration/Mayor of the host city or the municipality where the twinning activity is going to take place. This category only covers official twinnings.

'(j) for close relatives — spouse, children (including adopted), parents (including custodians), grandparents and grandchildren — visiting citizens of Ukraine legally residing in the territory of the Member States or citizens of the European Union residing in the territory of the Member State of which they are nationals:

— a written request from the host person;'

That point regulates the situation of Ukrainian close relatives travelling to the Member States to visit Ukrainian citizens legally residing in the Member States or citizens of the European Union residing in the territory of the Member State of which they are nationals.

The authenticity of the signature of the inviting person must be proved by the competent authority according to the national legislation of the country of residence.

It is also necessary to prove the legal residence of the inviting person and the family tie; for example providing together with the written request from the host person, copies of documents explaining his/her status, such as a photocopy of the residence permit and confirming the family ties.

That provision also applies to relatives of staff working in diplomatic missions and consulates travelling for a family visit of up to 90 days to the territory of the Member States except for the need to proof legal residence and family ties.

In line with the European Union Declaration on facilitations for family members, attached to the amending Agreement, 'In order to ease the mobility of an extended number of persons which have family links (in particular sisters and brothers and their children) with citizens of Ukraine legally residing in the territories of Member States or with citizens of the European Union residing in the territory of the Member State of which they are nationals, the European Union invites the Member States' consular offices to make full use of the existing possibilities in the Visa Code for facilitating the issuance of visas to this category of persons, including in particular, the simplification of documentary evidence requested for the applicants, exemptions from handling fees and, where appropriate, the issuing of multiple-entry visas.'.

'(k) relatives visiting for burial ceremonies:

— an official document confirming the fact of death as well as confirmation of the family or other relationship between the applicant and the buried;'

The Agreement does not specify which country's authorities should issue the above mentioned official document: the country where the burial ceremony will take place or the country where resides the person who wants to visit the burial ceremony. It should be accepted that the competent authorities of both countries could issue such official document.

The above mentioned official document confirming the fact of death as well as the family or other relationship between the applicant and the deceased must be presented; e.g. birth and/or marriage certificates.

'(l) for visiting military and civil burial grounds:

— an official document confirming the existence and preservation of the grave as well as family or other relationship between the applicant and the buried;'

The Agreement does not specify whether the abovementioned official document should be issued by the authorities of the country where the burial ground is located or those of the country in which the person who wants to visit the burial ground resides. It should be accepted that the competent authorities of both countries could issue such official document.

The abovementioned official document confirming the existence and preservation of the grave as well as of the family or other relationship between the applicant and the buried must be presented.

In accordance with the European Community Declaration on issuance of short-stay visas for visits of military and civil burial grounds, attached to the Agreement, as a general rule, short-stay visas for persons visiting military and civil burial grounds will be issued for a period of up to 14 days.

'(m) for visiting for medical reasons and necessary accompanying persons:

— an official document of the medical institution confirming the necessity of medical care in that institution, the necessity of being accompanied and proof of sufficient financial means to pay the medical treatment;'

The document of the medical institution confirming the necessity of medical care in this institution and the proof of sufficient financial means to pay for the medical treatment, will be submitted; it should also confirm that it is necessary to be accompanied.

'(n) for representatives of civil society organisations when undertaking trips for the purposes of educational training, seminars, conferences, including in the framework of exchange programmes:

— a written request issued by the host organisation, a confirmation that the person is representing the civil society organisation and the certificate on establishment of such organisation from the relevant Register issued by a state authority in accordance with the national legislation;'

The document proving registration in Ukraine of a civil society organisation is a letter issued by the State Registration Service of Ukraine with information from the Register of Public Associations.

'(o) for members of the professions participating in international exhibitions, conferences, symposia, seminars or other similar events held in the territory of the Member States:

— a written request from the host organisation confirming that the person concerned is participating in the event;

(p) for representatives of religious communities:

— a written request from a religious community registered in Ukraine, stating the purpose, duration and frequency of the trips;'

The document proving registration in Ukraine of a religious community is an extract from the Unified State Register of legal entities and individual entrepreneurs with information that organisational and legal form of a legal entity is religious community.

'(q) for participants in official European Union cross-border cooperation programmes, such as under the European Neighbourhood and Partnership Instrument (ENPI):

— a written request by the host organisation.'.

Important: The Agreement does not create any new liability rules for the physical or legal persons issuing the written requests. The respective EU/national law applies in case of false issuance of such requests.

2.2.2. *Issuance of multiple-entry visas*

In cases where the visa applicant needs to travel frequently or regularly to the territory of the Member States, short-stay visas will be issued for several visits, provided that the total length if those visits does not exceed 90 days per period of 180 days.

Article 5(1) of the Agreement stipulates that:

'1. Diplomatic missions and consular posts of the Member States shall issue multiple-entry visas with the term of validity of five years to the following categories of persons:

(a) members of national and regional Governments and Parliaments, Constitutional Courts and Supreme Courts, national and regional prosecutors and their deputies, if they are not exempted from the visa requirement by the present Agreement, in the exercise of their duties;

(b) permanent members of official delegations who, following official invitations addressed to Ukraine, shall regularly participate in meetings, consultations, negotiations or exchange programmes, as well as in events held in the territory of the Member States by intergovernmental organisations;

(c) spouses and children (including adopted), who are under the age of 21 or are dependant, and parents (including custodians) visiting citizens of Ukraine legally residing in the territory of the Member States or citizens of the European Union residing in the territory of the Member State of which they are nationals;

(d) business people and representatives of business organisations who regularly travel to the Member States;

(e) journalists and the technical crew accompanying them in a professional capacity.

By way of derogation from the first subparagraph, where the need or the intention to travel frequently or regularly is manifestly limited to a shorter period, the term of validity of the multiple-entry visa shall be limited to that period, in particular where

— in the case of the persons referred to in point (a), the term of office,

— in the case of the persons referred to in point (b), the term of the validity of the status as a permanent member of an official delegation,

— in the case of the persons referred to in point (c), the period of validity of the authorisation for legal residence of citizens of Ukraine legally residing in the European Union,

— in the case of the persons referred to in point (d), the term of validity of the status as a representative of the business organisation or the work contract,

— in the case of the persons referred to in point (e), the work contract

is less than five years.'.

For those categories of persons, taking into account their professional status or the family relationship with a Ukrainian citizen legally residing in the territory of the Member States or a citizen of the European Union residing in the territory of the Member State of which they are nationals, it is justified to issue, as a rule, a multiple-entry visa with a validity of five years. In the initial version of the Agreement the expression 'with the term of validity of up to five years' left discretion to consulates in deciding on the period of validity of the visa, setting up only the maximum length of validity. With the amending Agreement that discretion has disappeared with the new wording 'with the term of validity of five years', stipulating that, should the applicant meet all the requirements of Article 5(1) of the Agreement, 'diplomatic missions and consular posts of the Member States shall issue multiple-entry visas with the term of validity of five years'.

For persons falling under point (a) of Article 5(1) of the Agreement, confirmation should be given regarding their professional status and the duration of their mandate.

That provision will not apply to persons falling under point (a) of Article 5(1) of the Agreement if they are exempted from the visa requirement by the Agreement, i.e. if they are holders of a diplomatic or biometric service passports.

For persons falling under point (b) of Article 5(1) of the Agreement, proof must be presented regarding their permanent status as a member of the delegation and the need to participate regularly in meetings, consultations, negotiations or exchange programs.

For persons falling under point (c) of Article 5(1) of the Agreement, proof must be presented regarding the legal residence of the inviting person (cfr. II.2.2.1).

For persons falling under points (d) and (e) of Article 5(1) of the Agreement, proof must be presented regarding their professional status and the duration of their activities.

Article 5(2) of the Agreement stipulates that:

'2. Diplomatic missions and consular posts of the Member States shall issue multiple-entry visas with the term of validity of one year to the following categories of persons, provided that during the previous year they have obtained at least one visa, have made use of it in accordance with the laws on entry and stay of the visited State:

(a) drivers conducting international cargo and passenger transportation services to the territories of the Member States in vehicles registered in Ukraine;

(b) members of train, refrigerator and locomotive crews in international trains, travelling to the territories of the Member States;

(c) persons participating in scientific, cultural and artistic activities, including university and other exchange programmes, who regularly travel to the Member States;

(d) participants in international sports events and persons accompanying them in a professional capacity;

(e) participants in official exchange programmes organised by twin cities and other municipal entities;

(f) representatives of civil society organisations travelling regularly to Member States for the purposes of educational training, seminars, conferences, including in the framework of exchange programmes;

(g) for participants in official European Union cross-border cooperation programmes, such as under the European Neighbourhood and Partnership Instrument (ENPI);

(h) students and post-graduate students who regularly travel for the purposes of study or educational training, including in the framework of exchange programmes;

(i) for representatives of religious communities;

(j) for members of the professions participating in international exhibitions, conferences, symposia, seminars or other similar events held in the territory of the Member States;

(k) persons needing to visit regularly for medical reasons and necessary accompanying persons.

By way of derogation from the first subparagraph, where the need or the intention to travel frequently or regularly is manifestly limited to a shorter period, the term of validity of the multiple-entry visa shall be limited to that period.'.

In the initial version of the Agreement the expression 'with the term of validity of up to one year' left discretion to consulates in deciding on the period of validity of the visa, setting up only the maximum length of validity. With the amending Agreement that discretion has disappeared with the new wording 'with the term of validity of one year', stipulating that, should the applicant meet all the requirements of Article 5(2) of the Agreement, 'diplomatic missions and consular posts of the Member States shall issue multiple-entry visas with the term of validity of one year'. It is to be noted that multiple-entry visas valid for one year will be issued to the above mentioned categories if during the previous year (12 months) the visa applicant has obtained at least one Schengen visa and has made use of it in conformity with the laws on entry and stay of the State(s) visited (for instance, the person has not overstayed) and if there are reasons for requesting a multiple-entry visa. The Schengen visa obtained during the previous year can be one that has been issued by a Schengen State other than the one where the applicant requested the new visa. In cases where it is not justified to issue a visa valid for one year, (for instance, if the duration of the exchange programme is of less than one year or the person does not need to travel frequently or regularly for a full year) the validity of the visa will be of less than one year, provided that the other requirements for issuing the visa are met.

Article 5(3) and (4) of the Agreement stipulate that:

'3. Diplomatic missions and consular posts of the Member States shall issue multiple-entry visas with the term of validity of a minimum of two years and a maximum of five years to the categories of persons referred to in paragraph 2 of this Article, provided that during the previous two years they have made use of the one year multiple-entry visas in accordance with the laws on entry and stay of the visited State unless the need or the intention to travel frequently or regularly is manifestly limited to a shorter period, in which case the term of validity of the multiple-entry visa shall be limited to that period.

4. The total period of stay of persons referred to in paragraphs 1 to 3 of this Article shall not exceed 90 days per period of 180 days in the territory of the Member States.'.

Multiple-entry visas valid from two years up to five years will be issued to the categories mentioned under Article 5(2) of the Agreement, provided that during the previous two years they have made use of the one year multi-entry Schengen visas in accordance with the laws on entry and stay in the territory(ies) of the visited State(s) and that the need to travel frequently or regularly is not manifestly limited to a shorter period. It has to be noted that a visa with a validity from two to five years will only be issued if the visa applicant has been issued two visas valid for one year -and not less- during the previous two years, and if (s)he has used those visas in accordance with the laws of entry and stay in the territory(ies) of the visited State(s). Diplomatic missions and consular posts of the Member States will decide, on the basis of the assessment of each visa application, the period of validity of those visas — i.e. from two to five years.

Regarding the definition of the criteria in Article 5(2) of the Agreement: 'provided that … there are reasons for requesting a multiple-entry visa', and Article 5(3) of the Agreement: 'provided that … the reasons for requesting a multiple-entry visa are still valid', the criteria set up in point (a) of Article 24(2) of the Visa Code for issuing those type of visas apply, i.e. that the person needs to travel frequently to one or several Member States, for example on business.

There is no obligation to issue a multiple-entry visa if the applicant did not make use of a previous visa. Nevertheless, such a visa can be issued if the non-use of the previous visa is due to circumstances independent of the will of the applicant; for instance, a long absence from his job of a lorry driver due to illness.

Cfr. II.2.2.1 regarding documents justifying the purpose of the journey for issuing multiple-entry visas for the categories mentioned in Article 5 of the Agreement.

2.2.3. *Holders of diplomatic and service passports*

Article 10 of the Agreement stipulates that:

> '1. Citizens of Ukraine, holders of valid diplomatic passports can enter, leave and transit through the territories of the Member States without visas.
>
> 2. Citizens of Ukraine who are holders of valid biometric service passports can enter, leave and transit through the territories of the Member States without visas.
>
> 3. Persons mentioned in paragraphs 1 and 2 of this Article may stay in the territories of the Member States for a period not exceeding 90 days per period of 180 days.'.

Existing bilateral agreements or arrangements providing for the visa exemption for holders of non-biometric service passports will continue to apply, unless denounced or suspended (cfr. I.1.6).

The posting of diplomats in the Member States is not regulated by the Agreement. The usual accreditation procedure applies.

III. STATISTICS

In order to allow the Joint Committee to monitor effectively the Agreement, diplomatic missions and consular posts of the Member States must submit statistics to the Commission every six months, regarding in particular, where possible, and specifying by month:

— types of visas issued to the different categories of persons covered by the Agreement;

— the number of visa refusals for the different categories of persons covered by the Agreement;

— percentages of applicants called for a personal interviews per categories of persons;

— five year multiple-entry visas issued for Ukrainian nationals (by country);

— percentages of visas issued free of charge to the different categories of persons covered by the Agreement.

COUNCIL DECISION (CFSP) 2015/439

of 16 March 2015

extending the mandate of the European Union Special Representative for the Sahel

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 33 and Article 31(2) thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 18 March 2013, the Council adopted Decision 2013/133/CFSP [1] appointing Mr Michel Dominique REVEYRAND — DE MENTHON as the European Union Special Representative (EUSR) for the Sahel. The EUSR's mandate has been extended by Council Decision 2014/130/CFSP [2] and is to expire on 28 February 2015.

(2) The mandate of the EUSR should be extended for a further period of 8 months.

(3) The EUSR will implement his mandate in the context of a situation which may deteriorate and could impede the achievement of the objectives of the Union's external action as set out in Article 21 of the Treaty,

HAS ADOPTED THIS DECISION:

Article 1

European Union Special Representative

1. The mandate of Mr Michel Dominique REVEYRAND — DE MENTHON as the EUSR for the Sahel is extended until 31 October 2015. The mandate of the EUSR may be terminated earlier, if the Council so decides, on a proposal of the High Representative of the Union for Foreign Affairs and Security Policy (HR).

2. For the purposes of the EUSR's mandate, the Sahel is defined as comprising the primary focus of the EU Strategy for Security and Development in the Sahel (the 'Strategy'), namely Burkina Faso, Chad, Mali, Mauritania and Niger. For issues with broader regional implications, the EUSR shall engage with other countries and regional or international entities beyond the Sahel, and also West Africa and the Gulf of Guinea, as appropriate.

3. In view of the need for a regional approach to the inter-related challenges facing the region, the EUSR for the Sahel shall work in close consultation with other relevant EUSRs, including the EUSR for the Southern Mediterranean region, the EUSR for Human Rights and the EUSR to the African Union.

Article 2

Policy objectives

1. The mandate of the EUSR shall be based on the policy objective of the Union in relation to the Sahel to contribute actively to regional and international efforts to achieve lasting peace, security and development in the region. The EUSR shall furthermore aim to enhance the quality, intensity and impact of the Union's multi-faceted engagement in the Sahel.

2. The EUSR shall contribute to developing and implementing the Union approach encompassing all aspects of Union action, in particular in the political, security and development areas, including the Strategy, and to coordinating all relevant instruments for Union actions.

3. Initial priority shall be given to Mali and to its long-term stabilisation and to the regional dimensions of the conflict there.

---

[1] Council Decision 2013/133/CFSP of 18 March 2013 appointing the European Union Special Representative for the Sahel (OJ L 75, 19.3.2013, p. 29).

[2] Council Decision 2014/130/CFSP of 10 March 2014 extending the mandate of the European Union Special Representative for the Sahel (OJ L 71, 12.3.2014, p. 14).

4. Regarding Mali, the Union's policy objectives aim, through the coordinated and effective use of all its instruments, to promote a return for Mali and its people to a path of peace, reconciliation, security and development. Due attention should also be paid to Burkina Faso and Niger, particularly looking ahead to elections in those countries.

Article 3

Mandate

1. In order to achieve the Union's policy objectives in relation to the Sahel, the mandate of the EUSR shall be to:

(a) actively contribute to the implementation, coordination and further development of the Union's comprehensive approach to the regional crisis, on the basis of its Strategy, with a view to enhancing the overall coherence and effectiveness of Union activities in the Sahel, in particular in Mali;

(b) engage with all relevant stakeholders of the region, governments, regional authorities, regional and international organisations, civil society and diasporas, with a view to furthering the Union's objectives and contribute to a better understanding of the role of the Union in the Sahel;

(c) represent the Union in relevant regional and international fora, including the Support and Follow-Up Group on the situation in Mali, and ensure visibility for Union support to crisis management and conflict prevention, including the European Union military mission to contribute to the training of the Malian Armed Forces (EUTM Mali) and the European Union CSDP mission in Niger (EUCAP Sahel Niger);

(d) maintain close cooperation with the United Nations (UN), in particular the Special Representative of the Secretary-General for West Africa and the Special Representative of the Secretary-General for Mali, the African Union (AU), in particular the AU High Representative for Mali and the Sahel, the Economic Community of West African States (Ecowas) and other leading national, regional and international stakeholders including other Special Envoys for the Sahel, as well as with the relevant bodies in the Maghreb area;

(e) closely follow the regional and trans-boundary dimensions of the crisis, including terrorism, organised crime, arms smuggling, human trafficking, drug trafficking, refugee and migration flows and related financial flows; in close cooperation with the EU Counter-Terrorism Coordinator, contribute to the further implementation of the EU Counter-Terrorism Strategy;

(f) maintain regular high level political contacts with the countries in the region affected by terrorism and international crime in order to ensure a coherent and comprehensive approach and to ensure the Union's key role in the international efforts to fight terrorism and international crime. This includes the Union's active support to regional capacity-building in the security sector, and ensuring that the root causes of terrorism and international crime in the Sahel are adequately addressed;

(g) closely follow the political and security consequences of humanitarian crises in the region;

(h) with regard to Mali, contribute to regional and international efforts to facilitate the resolution of the crisis in Mali, in particular a full return to constitutional normalcy and governance throughout the territory and a credible national inclusive dialogue leading to a sustainable political settlement;

(i) promote institution building, security sector reform and long-term peace building and reconciliation in Mali;

(j) contribute to the implementation of the Union's human rights policy in the region in cooperation with the EUSR for Human Rights, including the EU Guidelines on human rights, in particular the EU Guidelines on Children and Armed Conflict, as well as on violence against women and girls and combating all forms of discrimination against them, and the Union's policy on Women, Peace and Security, including by monitoring and reporting on developments, as well as formulating recommendations in this regard and maintain regular contacts with the relevant authorities in Mali and in the region, the Office of the Prosecutor of the International Criminal Court, the Office of the High Commissioner for Human Rights and the human rights defenders and observers in the region;

(k) follow up and report on compliance with relevant resolutions of the UN Security Council (UNSCRs), in particular UNSCRs 2056 (2012), 2071 (2012), 2085 (2012) and 2100 (2013).

2. For the purpose of the fulfilment of his mandate, the EUSR shall, inter alia:

(a) advise and report on the formulation of Union positions in regional and international fora, as appropriate, in order to proactively promote and strengthen the Union's comprehensive approach towards the crisis in the Sahel;

(b) maintain an overview of all activities of the Union and cooperate closely with relevant Union delegations.

Article 4

Implementation of the mandate

1. The EUSR shall be responsible for the implementation of the mandate acting under the authority of the HR.

2. The Political and Security Committee (PSC) shall maintain a privileged link with the EUSR and shall be the EUSR's primary point of contact with the Council. The PSC shall provide the EUSR with strategic guidance and political direction within the framework of the mandate, without prejudice to the responsibilities of the HR.

3. The EUSR shall work in close coordination with the European External Action Service (EEAS) and the relevant departments thereof, in particular with the Sahel Coordinator.

Article 5

Financing

1. The financial reference amount intended to cover the expenditure related to the mandate of the EUSR in the period from 1 March 2015 to 31 October 2015 shall be EUR 900 000.

2. The expenditure shall be managed in accordance with the procedures and rules applicable to the general budget of the Union.

3. The management of the expenditure shall be subject to a contract between the EUSR and the Commission. The EUSR shall be accountable to the Commission for all expenditure.

Article 6

Constitution and composition of the team

1. Within the limits of the EUSR's mandate and the corresponding financial means made available, the EUSR shall be responsible for constituting his team. The team shall include the expertise on specific policy and security issues as required by the mandate. The EUSR shall keep the Council and the Commission promptly informed of the composition of the team.

2. Member States, institutions of the Union, and the EEAS may propose the secondment of staff to work with the EUSR. The salary of personnel who are seconded to the EUSR shall be covered by the Member State concerned, the institution of the Union concerned or the EEAS. Experts seconded by Member States to the institutions of the Union or the EEAS may also be posted to the EUSR. International contracted staff shall have the nationality of a Member State.

3. All seconded personnel shall remain under the administrative authority of the sending Member State, institution of the Union or the EEAS and shall carry out their duties and act in the interest of the mandate of the EUSR.

4. The EUSR staff shall be co-located with the relevant EEAS departments or Union delegations in order to ensure coherence and consistency of their respective activities.

Article 7

Privileges and immunities of the EUSR and of the EUSR's staff

The privileges, immunities and further guarantees necessary for the completion and smooth functioning of the mission of the EUSR and the members of his staff shall be agreed with the host countries, as appropriate. Member States and the EEAS shall grant all necessary support to such effect.

Article 8

Security of EU classified information

The EUSR and the members of EUSR's team shall respect the security principles and minimum standards established by Council Decision 2013/488/EU ([1]).

([1]) Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

Article 9

Access to information and logistical support

1. Member States, the Commission, the EEAS and the General Secretariat of the Council shall ensure that the EUSR is given access to any relevant information.

2. The Union delegations and/or Member States, as appropriate, shall provide logistical support in the region.

Article 10

Security

In accordance with the Union's policy on the security of personnel deployed outside the Union in an operational capacity under Title V of the Treaty, the EUSR shall take all reasonably practicable measures, in conformity with his mandate and on the basis of the security situation in the geographical area of responsibility, for the security of all personnel under his direct authority, in particular by:

(a) establishing a specific security plan based on guidance from the EEAS, including specific physical, organisational and procedural security measures, governing the management of the secure movement of personnel to, and within, the geographic area, as well as management of security incidents and a mission contingency and evacuation plan;

(b) ensuring that all personnel deployed outside the Union are covered by high-risk insurance as required by the conditions in the geographic area;

(c) ensuring that all members of the team to be deployed outside the Union, including locally contracted personnel, have received appropriate security training before or upon arriving in the geographic area, based on the risk ratings assigned to that area;

(d) ensuring that all agreed recommendations made following regular security assessments are implemented and providing the Council, the HR and the Commission with written reports on their implementation and on other security issues within the framework of the progress report and with the mandate implementation report.

Article 11

Reporting

1. The EUSR shall regularly provide the HR and the PSC with reports. The EUSR shall also report as necessary to Council working parties. Regular reports shall be circulated through the COREU network. The EUSR may provide the Foreign Affairs Council with reports. In accordance with Article 36 of the Treaty, the EUSR may be involved in briefing the European Parliament.

2. The EUSR shall report on the best way of pursuing Union initiatives, such as the contribution of the Union to reforms, and including the political aspects of relevant Union development projects, in coordination with Union delegations in the region.

Article 12

Coordination with other Union actors

1. In the framework of the Strategy, the EUSR shall contribute to the unity, consistency and effectiveness of the Union's political and diplomatic action and shall help ensure that all Union instruments and Member States' actions are engaged consistently, to attain the Union's policy objectives.

2. The activities of the EUSR shall be coordinated with those of Union delegations and of the Commission, as well as those of other EUSRs active in the region. The EUSR shall provide Member States' missions and Union delegations in the region with regular briefings.

3. In the field, close liaison shall be maintained with the Heads of Union delegations and Member States' Heads of Mission. The EUSR, in close cooperation with relevant Union delegations shall provide local political guidance to the Heads of Mission of EUCAP Sahel Niger and EUCAP Sahel Mali and Mission Commander of EUTM Mali. The EUSR, the Mission Commander of EUTM Mali and the Civilian Operation Commander of EUCAP Sahel Niger and EUCAP Sahel Mali shall consult each other as required.

Article 13

Review

The implementation of this Decision and its consistency with other contributions from the Union to the region shall be kept under regular review. The EUSR shall present the Council, the HR and the Commission with a comprehensive mandate implementation report by the end of August 2015.

Article 14

Entry into force

This Decision shall enter into force on the date of its adoption.

It shall apply from 1 March 2015.

Done at Brussels, 16 March 2015.

For the Council
The President
F. MOGHERINI

COUNCIL DECISION (CFSP) 2015/440

of 16 March 2015

extending the mandate of the European Union Special Representative for the Horn of Africa

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 33 and Article 31(2) thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 8 December 2011, the Council adopted Decision 2011/819/CFSP [1] appointing Mr Alexander RONDOS as the European Union Special Representative (EUSR) for the Horn of Africa. The EUSR's mandate is to expire on 28 February 2015.

(2) The mandate of the EUSR should be further extended until 31 October 2015.

(3) The EUSR will implement the mandate in the context of a situation which may deteriorate and could impede the achievement of the objectives of the Union's external action as set out in Article 21 of the Treaty,

HAS ADOPTED THIS DECISION:

Article 1

European Union Special Representative

The mandate of Mr Alexander RONDOS as the EUSR for the Horn of Africa is extended until 31 October 2015. The Council may decide that the mandate of the EUSR be terminated earlier, based on an assessment by the Political and Security Committee (PSC) and a proposal from the High Representative of the Union for Foreign Affairs and Security Policy (HR).

For the purposes of the mandate of the EUSR, the Horn of Africa is defined as comprising the Republic of Djibouti, the State of Eritrea, the Federal Democratic Republic of Ethiopia, the Republic of Kenya, the Federal Republic of Somalia, the Republic of the Sudan, the Republic of South Sudan and the Republic of Uganda. For issues with broader regional implications, the EUSR shall engage with countries and regional entities beyond the Horn of Africa, as appropriate.

Article 2

Policy objectives

1. The mandate of the EUSR shall be based on the policy objectives of the Union in relation to the Horn of Africa, as set out in its strategic framework adopted on 14 November 2011 and in relevant Council conclusions, namely to contribute actively to regional and international efforts to achieve peaceful coexistence and lasting peace, security and development within and among the countries in the region. The EUSR shall furthermore aim to enhance the quality, intensity, impact and visibility of the Union's multifaceted engagement in the Horn of Africa.

2. The policy objectives shall include, inter alia:

(a) the continued stabilisation of Somalia, particularly as approached from a regional dimension;

(b) the peaceful coexistence of Sudan and South Sudan as two viable and prosperous states with robust and accountable political structures;

(c) the resolution of current conflicts and avoidance of potential conflicts between or within countries in the region;

(d) support for political, security and economic regional cooperation.

[1] Council Decision 2011/819/CFSP of 8 December 2011 appointing the European Union Special Representative for the Horn of Africa (OJ L 327, 9.12.2011, p. 62).

Article 3

Mandate

1. In order to achieve the Union's policy objectives in relation to the Horn of Africa, the mandate of the EUSR shall be to:

(a) engage with all relevant stakeholders of the region, governments, regional authorities, international and regional organisations, civil society and diasporas, with a view to furthering the Union's objectives, and contribute to a better understanding of the role of the Union in the region;

(b) represent the Union in relevant international forums, as appropriate, and ensure visibility for Union support to crisis management, as well as conflict resolution and prevention;

(c) encourage and support effective political and security cooperation and economic integration in the region through the Union's partnership with the African Union (AU) and regional organisations, in particular the Intergovernmental Authority on Development (IGAD);

(d) follow political developments in the region and contribute to the development of the Union's policy towards the region, including in relation to Somalia, Sudan, South Sudan, the Ethiopia-Eritrea border issue and implementation of the Algiers Agreement, the Nile Basin initiative and other concerns in the region that impact on its security, stability and prosperity;

(e) with regard to Somalia, and working in close coordination with the EU Special Envoy for Somalia and relevant regional and international partners, including the United Nations (UN) Secretary-General Special Representative for Somalia and the AU, contribute actively to actions and initiatives leading to further stabilisation and post transition arrangements for Somalia, with an emphasis on promoting a coordinated and coherent international approach towards Somalia, building good neighbourly relations and supporting the development of the security sector in Somalia, including, through the European Union military mission to contribute to the training of Somali security forces (EUTM Somalia), the European Union-led naval force (EUNAVFOR Atalanta), the European Union Mission on Regional Maritime Capacity Building in the Horn of Africa (EUCAP Nestor) and the Union's continued support to the African Union Mission in Somalia (Amisom), working closely with Member States;

(f) with regard to Sudan and South Sudan, and working in close cooperation with the respective Heads of Union delegations, contribute to the coherence and effectiveness of Union policy towards Sudan and South Sudan and support their peaceful coexistence, in particular through implementation of the Addis Agreements and resolution of the outstanding issues following the Comprehensive Peace Agreement, including Abyei, political solutions to the ongoing conflicts, particularly in Darfur, Southern Kordofan and Blue Nile, institution-building in South Sudan and national reconciliation. In this regard, the EUSR shall contribute to a coherent international approach in close cooperation with the AU and in particular the AU High Level Implementation Panel for Sudan (AUHIP), the UN and other leading regional and international stakeholders;

(g) follow closely the trans-boundary challenges affecting the Horn of Africa, including terrorism, radicalisation, maritime security and piracy, organised crime, arms smuggling, refugee and migration flows and any political and security consequences of humanitarian crises;

(h) promote humanitarian access throughout the region;

(i) contribute to the implementation of Council Decision 2011/168/CFSP [1] and the Union's human rights policy, in cooperation with the EUSR for Human Rights, including the EU Guidelines on human rights, in particular the EU Guidelines on children and armed conflict as well as the EU Guidelines on violence against women and girls and combating all forms of discrimination against them, and the Union's policy regarding UN Security Council Resolution 1325 (2000), including by monitoring and reporting on developments as well as formulating recommendations in this regard.

2. For the purpose of the fulfilment of the mandate, the EUSR shall, inter alia:

(a) advise and report on the definition of Union positions in international forums, as appropriate, in order to promote proactively the Union's comprehensive policy approach towards the Horn of Africa;

(b) maintain an overview of all activities of the Union.

[1] Council Decision 2011/168/CFSP of 21 March 2011 on the International Criminal Court and repealing Common Position 2003/444/CFSP (OJ L 76, 22.3.2011, p. 56).

Article 4

Implementation of the mandate

1. The EUSR shall be responsible for the implementation of the mandate, acting under the authority of the HR.

2. The PSC shall maintain a privileged link with the EUSR and shall be the EUSR's primary point of contact with the Council. The PSC shall provide the EUSR with strategic guidance and political direction within the framework of the mandate, without prejudice to the powers of the HR.

3. The EUSR shall work in close coordination with the European External Action Service (EEAS) and its relevant departments, Union delegations in the region and the Commission.

Article 5

Financing

1. The financial reference amount intended to cover the expenditure related to the mandate of the EUSR for the period from 1 March 2015 to 31 October 2015 shall be EUR 1 770 000.

2. The expenditure shall be managed in accordance with the procedures and rules applicable to the general budget of the Union.

3. The management of the expenditure shall be subject to a contract between the EUSR and the Commission. The EUSR shall be accountable to the Commission for all expenditure.

Article 6

Constitution and composition of the team

1. Within the limits of the EUSR's mandate and the corresponding financial means made available, the EUSR shall be responsible for constituting his team. The team shall include the expertise on specific policy and security issues as required by the mandate. The EUSR shall promptly and regularly inform the Council and the Commission of the composition of his team.

2. Member States, the institutions of the Union and the EEAS may propose the secondment of staff to work with the EUSR. The salary of such seconded personnel shall be covered by the Member State, the institution of the Union concerned or the EEAS, respectively. Experts seconded by Member States to the institutions of the Union or the EEAS may also be posted to the EUSR. International contracted staff shall have the nationality of a Member State.

3. All seconded personnel shall remain under the administrative authority of the sending Member State, the sending institution of the Union or the EEAS, and shall carry out their duties and act in the interest of the mandate of the EUSR.

4. The EUSR staff shall be co-located with the relevant EEAS departments or Union delegations in order to contribute to the coherence and consistency of their respective activities.

Article 7

Privileges and immunities of the EUSR and the staff of the EUSR

The privileges, immunities and further guarantees necessary for the completion and smooth functioning of the mission of the EUSR and the members of the EUSR's staff shall be agreed with the host countries, as appropriate. Member States and the EEAS shall grant all necessary support to such effect.

Article 8

Security of EU classified information

The EUSR and the members of his team shall respect the security principles and minimum standards established by Council Decision 2013/488/EU ([1]).

([1]) Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

Article 9

Access to information and logistical support

1. Member States, the Commission, the EEAS and the General Secretariat of the Council shall ensure that the EUSR is given access to any relevant information.

2. The Union delegations in the region and the Member States, as appropriate, shall provide logistical support in the region.

Article 10

Security

In accordance with the Union's policy on the security of personnel deployed outside the Union in an operational capacity under Title V of the Treaty, the EUSR shall take all reasonably practicable measures, in accordance with the EUSR's mandate and the security situation in the geographical area of responsibility, for the security of all personnel under the direct authority of the EUSR, in particular by:

(a) establishing a mission-specific security plan based on guidance from the EEAS, including mission-specific physical, organisational and procedural security measures, governing the management of the secure movement of personnel to, and within, the mission area as well as the management of security incidents and including a mission contingency plan and evacuation plan;

(b) ensuring that all personnel deployed outside the Union are covered by high-risk insurance, as required by the conditions in the mission area;

(c) ensuring that all members of the EUSR's team to be deployed outside the Union, including locally contracted personnel, have received appropriate security training before or upon arriving in the mission area, based on the risk ratings assigned to the mission area by the EEAS;

(d) ensuring that all agreed recommendations made following regular security assessments are implemented, and providing the Council, the HR and the Commission with written reports on their implementation and on other security issues within the framework of the progress and the mandate implementation reports.

Article 11

Reporting

1. The EUSR shall regularly provide the HR and the PSC with oral and written reports. The EUSR shall also report to Council working parties, as necessary. Regular reports shall be circulated through the COREU network. The EUSR may provide the Foreign Affairs Council with reports. In accordance with Article 36 of the Treaty, the EUSR may be involved in briefing the European Parliament.

2. The EUSR shall report on the best way of pursuing Union initiatives, such as the contribution of the Union to reforms, and including the political aspects of relevant Union development projects, in coordination with the Union delegations in the region.

Article 12

Coordination

1. The EUSR shall contribute to the unity, consistency and effectiveness of the Union's actions and shall help ensure that all Union instruments and Member States' action are engaged consistently, to attain the Union's policy objectives. The activities of the EUSR shall be coordinated with those of Union delegations and of the Commission. The EUSR shall provide regular briefings to Member States' missions and Union delegations in the region.

2. In the field, close liaison shall be maintained with the Heads of the Union delegations and the Heads of Member States' missions. They shall make every effort to assist the EUSR in the implementation of the mandate. The EUSR, in close coordination with the relevant Union delegations, shall provide local political guidance to the Force Commander of EUNAVFOR Atalanta, the EU Mission Commander of EUTM Somalia and the Head of Mission of EUCAP Nestor. The EUSR, the EU Operation Commanders and the Civilian Operation Commander shall consult each other as required.

3. The EUSR shall closely cooperate with the authorities of the countries involved, the UN, the AU, IGAD, other national regional and international stakeholders, and also with civil society in the region.

Article 13

Review

The implementation of this Decision and its consistency with other contributions from the Union to the region shall be kept under regular review. The EUSR shall present the Council, the HR and the Commission with a comprehensive mandate implementation report by 31 August 2015.

Article 14

Entry into force

This Decision shall enter into force on the date of its adoption.

It shall apply from 1 March 2015.

Done at Brussels, 16 March 2015.

For the Council
The President
F. MOGHERINI

COUNCIL DECISION (CFSP) 2015/441

of 16 March 2015

amending and extending Decision 2010/96/CFSP on a European Union military mission to contribute to the training of Somali security forces

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 42(4) and 43(2) thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 15 February 2010, the Council adopted Decision 2010/96/CFSP [1]. The mandate of the EU military mission ends on 31 March 2015.

(2) The Brussels Conference on Somalia, held on 16 September 2013, provided the basis for the Somalia Compact and triggered a mechanism for coordination and Somali ownership through the Somalia 'New Deal' task force.

(3) During the United Kingdom and Somalia co-hosted international meeting, held in London on 18 September 2014, the Federal Government outlined the Ministry of Defence's path to development of the Somali National Army up to 2019, and its immediate requirements.

(4) Following the Strategic Review in October 2014, the mandate of the EU military mission should be extended until 31 December 2016.

(5) In accordance with Article 5 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark does not participate in the elaboration and implementation of decisions and actions of the Union which have defence implications. Denmark does not participate in the implementation of this Decision and therefore does not participate in the financing of this mission.

(6) The mandate of the EU military mission should be further extended with an adapted mandate,

HAS ADOPTED THIS DECISION:

Article 1

Decision 2010/96/CFSP is hereby amended as follows:

(1) In Article 1, paragraph 2 is replaced by the following:

'2. In order to achieve the objectives set out in paragraph 1, the EU military mission shall be deployed in Somalia in order to address both institutional building in the defence sector through strategic advice as well as direct support to the Somali National Army through training, advice and mentoring. The EU military mission shall also be ready to provide support, within its means and capabilities, to other Union actors in the implementation of their respective mandates in the security and defence area in Somalia.'.

(2) Article 3 is replaced by the following:

'*Article 3*

Designation of the Mission Headquarters

1. The Mission Headquarters shall be located in Somalia, at Mogadishu International Airport in Mogadishu. It shall perform the functions of both Operational Headquarters and Force Headquarters.

2. The Mission Headquarters shall include a liaison and support office in Nairobi and a support cell in Brussels.'.

[1] Council Decision 2010/96/CFSP of 15 February 2010 on a European Union military mission to contribute to the training of Somali security forces (OJ L 44, 19.2.2010, p. 16).

(3) In Article 7, paragraph 4 is replaced by the following:

'4. The EU military mission shall operate, within its means and capabilities, in close cooperation with other international actors in the region, in particular the United Nations and AMISOM in line with the agreed requirements of the Federal Government of Somalia.'.

(4) In Article 10, the following paragraph is added:

'5. The financial reference amount for the common costs of the EU military mission for the period from 1 April 2015 until 31 December 2016 shall be EUR 17 507 399. The percentage of this reference amount referred to in Article 25(1) of ATHENA shall be 30 % and the percentage for commitment referred to in Article 32(3) of ATHENA shall be 90 %.'.

(5) The following Article is inserted:

'Article 10b

Project cell

1. The EU military mission shall have a project cell for identifying and implementing projects, to be financed by Member States or third States which are consistent with the mission's objectives and contribute to the mandate's delivery.

2. Subject to paragraph 3, the EU Mission Commander shall be authorised to seek recourse to financial contributions from the Member States or third States to implement projects identified as supplementing the EU military mission's other actions in a consistent manner. In such a case, the EU Mission Commander shall conclude an arrangement with those States, covering in particular the specific procedures for dealing with any complaint from third parties concerning damage caused as a result of acts or omissions by the EU Mission Commander in the use of the funds provided by those States.

Under no circumstances shall the Union or the HR be held liable by contributing States as a result of acts or omissions by the EU Mission Commander in the use of the funds provided by those States.

3. The PSC shall agree on the acceptance of a financial contribution from third States to the project cell.'.

(6) Article 11 is amended as follows:

(a) in paragraph 1, the introductory wording is replaced by 'The HR shall be authorised to release to the third States associated with this Decision, as appropriate and in accordance with the needs of the Mission, EU classified information generated for the purposes of the Mission, in accordance with Council Decision 2013/488/EU (*):

(*) Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).';

(b) in paragraphs 2 and 3, the words 'Decision 2011/292/EU' are replaced by the words 'Decision 2013/488/EU'.

(7) In Article 12, paragraphs 2 and 3 are replaced by the following:

'2. The mandate of the EU military mission shall end on 31 December 2016.

3. This Decision shall be repealed as from the date of closure of the EU Headquarters, the liaison and support office in Nairobi and the support cell in Brussels, in accordance with the plans approved for the termination of the EU military mission, and without prejudice to the procedures regarding the audit and presentation of the accounts of the EU military mission, laid down in ATHENA.'.

Article 2

This Decision shall enter into force on the date of its adoption.

It shall apply from 1 April 2015.

Done at Brussels, 16 March 2015.

For the Council

The President

F. MOGHERINI

COUNCIL DECISION (CFSP) 2015/442

of 16 March 2015

launching the European Union CSDP Military Advisory Mission in the Central African Republic (EUMAM RCA) and amending Decision 2015/78/CFSP

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 42(4) and 43(2) thereof,

Having regard to Council Decision 2015/78/CFSP of 19 January 2015 on a European Union CSDP Military Advisory Mission in the Central African Republic (EUMAM RCA) ([1]), and in particular Article 4 thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 19 January 2015, the Council adopted Decision 2015/78/CFSP.

(2) On 9 February 2015, the Council approved the Rules of Engagement of EUMAM RCA.

(3) On 6 March 2015, the Council approved the Mission Plan of EUMAM RCA.

(4) On 11 March 2015, the Political and Security Committee welcomed the letter from the Mission Commander regarding the recommendation to launch EUMAM RCA and the envisaged time frame for declaring Initial Operating Capability of EUMAM RCA.

(5) EUMAM RCA should be launched on 16 March 2015.

(6) In accordance with Article 5 of the Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark does not participate in the elaboration and the implementation of decisions and actions of the Union which have defence implications. Consequently, Denmark does not participate in the implementation of this Decision and therefore does not participate in the financing of this mission,

HAS ADOPTED THIS DECISION:

Article 1

The European Union CSDP Military Advisory Mission in the Central African Republic ('EUMAM RCA') shall be launched on 16 March 2015.

Article 2

The EU Mission Commander of EUMAM RCA is hereby authorised with immediate effect to start execution of the mission.

Article 3

Article 4(2) of Decision 2015/78/CFSP is replaced by the following:

'2. EUMAM RCA shall be launched by a Council Decision on the date recommended by the Mission Commander, following approval of the Mission Plan and, if required, of additional Rules of Engagement.'.

([1]) OJ L 13, 20.1.2015, p. 8.

Article 4

This Decision shall enter into force on the date of its adoption.

Done at Brussels, 16 March 2015.

For the Council
The President
F. MOGHERINI

COMMISSION DECISION (EU, Euratom) 2015/443

of 13 March 2015

on Security in the Commission

THE EUROPEAN COMMISSION,

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

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

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

Whereas:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HAS ADOPTED THIS DECISION:

CHAPTER 1

GENERAL PROVISIONS

Article 1

Definitions

For the purposes of this Decision the following definitions apply:

(1) 'assets' means all movable and immovable property and possessions of the Commission;

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

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

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

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

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

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

(8) 'personal data' means personal data as defined in Article 2(a) of Regulation (EC) No 45/2001 of the European Parliament and of the Council ([3]);

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

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

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

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

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

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

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

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

(14) 'Staff Regulations' means the Staff Regulations of officials of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No 259/68 of the Council [1] and its amending acts;

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

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

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

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

Article 2

Subject matter

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

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

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

4. The provisions of this Decision shall be without prejudice to Commission Decision 2002/47/EC, ECSC, Euratom [3] and Commission Decision 2004/563/EC, Euratom [4], Commission Decision C(2006) 1623 [5] and Commission Decision C(2006) 3602 [6].

CHAPTER 2

PRINCIPLES

Article 3

Principles for security in the Commission

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

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

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

---

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

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

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

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

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

[6] C(2006) 3602 of 16 August 2006 concerning the security of information systems used by the European Commission.

4. Any security measure shall be taken overtly unless this can reasonably be expected to impair its effect. Addressees of a security measure shall be informed in advance of the reasons for and the impact of the measure, unless the effect of the measure can reasonably be expected to be impaired by providing such information. In this case, the addressee of the security measure shall be informed after the risk of impairing the effect of the security measure has ceased.

5. Commission departments shall ensure that security issues are taken into account from the start of the development and implementation of Commission policies, decisions, programmes, projects and activities for which they are responsible. In order to do so, they shall involve the Directorate-General for Human Resources and Security in general and the Chief Information Security Officer of the Commission as regards IT systems from the earliest stages of preparation.

6. The Commission shall, where appropriate, seek cooperation with the competent authorities of the host state, of other Member States and of other EU institutions, agencies or bodies, where feasible, taking account of the measures taken or planned by those authorities to address the risk to security concerned.

Article 4

Obligation to comply

1. Compliance with this Decision and its implementing rules and with the security measures and the instructions given by mandated staff shall be mandatory.

2. Non-compliance with the security rules may trigger liability to disciplinary action in accordance with the Treaties, the Staff Regulations, to contractual sanctions and/or to legal action under national laws and regulations.

CHAPTER 3

DELIVERING SECURITY

Article 5

Mandated staff

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

(1) Carry side arms;

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

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

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

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

Article 6

General provisions regarding security measures

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

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

(b) it shall only transfer information on an individual to recipients, other than Community institutions and bodies, which are not subject to national law adopted pursuant to Directive 95/46/EC of the European Parliament and of the Council [1], in accordance with Article 9 of Regulation (EC) No 45/2001;

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

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

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

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

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

2. The Security Directorate of the Directorate-General for Human Resources and Security shall establish an overview of security measures which may require an order by a judge in accordance with the laws and regulations of the Member States hosting Commission premises.

3. The Security Directorate of the Directorate-General for Human Resources and Security may turn to a contractor to carry out, under the direction and supervision of the Security Directorate, tasks relating to security.

Article 7

Security measures regarding persons

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

2. In case of major risks to security, the Directorate-General for Human Resources and Security shall provide close protection for Members of the Commission or other staff where a threat assessment has indicated that such protection is needed to ensure their safety and security.

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

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

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

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

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

Article 8

Security measures regarding physical security and assets

1. Security of assets shall be ensured by applying appropriate physical and technical protective measures and corresponding procedures, hereinafter called 'physical security', creating a multi-layered system.

2. Measures may be adopted pursuant to this Article in order to protect persons or information in the Commission as well as to protect assets.

3. Physical security shall have the following objectives:

— preventing acts of violence directed against Members of the Commission or persons falling within the scope of this Decision,

— preventing espionage and eavesdropping on sensitive or classified information,

— preventing theft, acts of vandalism, sabotage and other violent actions aimed at damaging or destroying Commission buildings and assets,

— enabling investigation and inquiry into security incidents including through checks on access and exit control log files, CCTV coverage, telephone call recordings and similar data as referred to in Article 22(2) hereunder and other information sources.

4. Physical security shall include:

— an access policy applicable to any person or vehicle requiring access to Commission premises, including the parking lots,

— an access control system comprising guards, technical equipment and measures, information systems or a combination of all of those elements.

5. In order to ensure physical security, the following actions may be taken:

— recording entry to and exit from Commission premises of persons, vehicles, goods and equipment,

— identity controls at its premises,

— inspection of vehicles, goods and equipment by visual or technical means,

— preventing unauthorised persons, vehicles and goods, from entering Commission premises.

Article 9

Security measures regarding information

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

2. Security of information, regardless of its form, shall balance transparency, proportionality, accountability and efficiency with the need to protect information from unauthorised access, use, disclosure, modification or destruction.

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

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

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

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

(b) 'Sensitive non-classified information', that is to say information or material the Commission must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information includes, but is not limited to, information or material covered by the obligation of professional secrecy, as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council [1] read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EC) No 45/2001.

6. Sensitive non-classified information shall be subject to rules regarding its handling and storage. It shall only be released to those individuals who have a 'need-to-know'. When deemed necessary for the effective protection of its confidentiality, it shall be identified by a security marking and corresponding handling instructions approved by the Director-General for Human Resources and Security. When handled or stored on Communication and Information Systems, such information shall be protected also in compliance with Decision C(2006) 3602, its implementing rules and corresponding standards.

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

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

Article 10

Security measures regarding Communication and Information Systems

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

2. Commission services owning, managing or operating CIS shall only allow other Union institutions, agencies, bodies or other organisations to have access to those systems provided that those Union institutions, agencies, bodies or other organisations can provide reasonable assurance that their IT systems are protected at a level equivalent to the Commission's Information Systems Security Policy as set out in Decision C(2006) 3602, its implementing rules and corresponding security standards. The Commission shall monitor such compliance, and in case of serious non-compliance or continued failure to comply, be entitled to prohibit access.

Article 11

Forensic analysis regarding cyber-security

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

Article 12

Security measures regarding persons and objects

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

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

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

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

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

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

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

2. Under exceptional circumstances, staff members of the Security Directorate of the Directorate-General for Human Resources and Security, mandated in accordance with Article 5, may take any urgent measures needed, in strict compliance with the principles laid down in Article 3. As soon as possible after having taken those measures, they shall inform the Director of the Security Directorate, who shall seek the appropriate mandate from the Director-General for Human Resources and Security, confirming the measures taken and authorising any further necessary actions and shall liaise, where appropriate with the competent national authorities.

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

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

Article 13

Inquiries

1. Without prejudice to Article 86 and Annex IX of the Staff Regulations and to any special arrangement between the Commission and the EEAS, such as the special arrangement signed on 28 May 2014 between the Directorate General for Human Resources and Security of the European Commission and the European External Action Service on the duty of care towards Commission staff posted in Union Delegations, security inquiries may be conducted:

(a) in case of incidents affecting security at the Commission, including suspected criminal offences;

(b) in case of potential leakage, mishandling or compromise of sensitive non-classified information, EUCI or Euratom Classified Information;

(c) in the context of counter-intelligence and counter-terrorism;

(d) in case of serious cyber-incidents.

2. The decision to conduct a security inquiry shall be taken by the Director-General for Human Resources and Security who will also be the recipient of the inquiry report.

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

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

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

6. The Directorate-General for Human Resources and Security shall inform the competent authorities of the host Member State or any other Member State concerned, where appropriate, and in particular if the inquiry has given rise to indications of a criminal act having been perpetrated. In this context, the Directorate-General for Human Resources and Security may, where appropriate or required, provide support to the authorities of the host Member State or any other Member State concerned.

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

8. Security inquiries shall be documented.

Article 14

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

1. Where the Security Directorate of the Directorate-General for Human Resources and Security conducts security inquiries, as referred to in Article 13, and if these enquiries fall within the competences of the European Anti-Fraud Office (OLAF) or the Investigation and Disciplinary Office of the Commission (IDOC), it shall liaise with those bodies at once with a view, in particular, not to compromise later steps by either OLAF or IDOC. Where appropriate, the Security Directorate of the Directorate-General for Human Resources and Security shall invite OLAF or IDOC to be involved in the investigation.

2. The security enquiries, as referred to in Article 13, shall be without prejudice to the powers of OLAF and IDOC as laid down in the rules governing those bodies. The Security Directorate of the Directorate-General for Human Resources and Security may be requested to provide technical assistance for inquiries initiated by OLAF or IDOC.

3. The Security Directorate of the Directorate-General for Human Resources and Security may be asked to assist OLAF's agents when they access Commission premises in accordance with Articles 3(5) and 4(4) of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council [1], in order to facilitate their tasks. The Security

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

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

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

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

Article 15

Security inspections

1. The Directorate-General for Human Resources and Security shall undertake security inspections in order to verify compliance by Commission services and individuals with this Decision and its implementing rules and to formulate recommendations when deemed necessary.

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

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

Article 16

Alert states and management of crisis situations

1. The Directorate-General for Human Resources and Security shall be responsible for putting in place appropriate alert state measures in anticipation of or in response to threats and incidents affecting security at the Commission, and for measures required for managing crisis situations.

2. The alert state measures referred to in paragraph 1 shall be commensurate with the level of threat to security. The alert states levels shall be defined in close cooperation with the competent services of other Union institutions, agencies and bodies, and of the Member State or Member States hosting Commission premises.

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

CHAPTER 4

ORGANISATION

Article 17

General responsibilities of Commission services

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

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

3. The responsibilities for implementing this Decision and its implementing rules and for day-to-day compliance may be delegated to other Commission departments, whenever decentralised delivery of security offers significant efficiency, resource or time savings, for instance because of the geographical location of the services concerned.

4. Where paragraph 3 applies, the Directorate-General for Human Resources and Security, and where appropriate the Director-General for Informatics, shall conclude arrangements with individual Commission departments establishing clear roles and responsibilities for the implementation and monitoring of security policies.

Article 18

The Directorate-General for Human Resources and Security

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

(1) developing the Commission's security policy, implementing rules and security notices;

(2) gathering information in view of assessing threats and risks to security and on all issues which may affect security in the Commission;

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

(4) providing a 24-hour/7-day emergency service for Commission services and staff for any safety- and security-related issues;

(5) implementing security measures aimed at mitigating risks to security and developing and maintaining appropriate CIS to cover its operational needs, particularly in the domains of physical access control, administration of security authorisations and handling of sensitive and EU classified information;

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

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

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

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

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

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

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

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

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

Article 19

The Commission Security Expert Group (ComSEG)

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

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

Article 20

Local Security Officers (LSOs)

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

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

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

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

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

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

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

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

CHAPTER 5

IMPLEMENTATION

Article 21

Implementing rules and security notices

1. As necessary, the adoption of the implementing rules for this Decision will be the subject of a separate empowerment decision of the Commission in favour of the Member of the Commission responsible for security matters, in full compliance with the internal rules of procedure.

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

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

CHAPTER 6

MISCELLANEOUS AND FINAL PROVISIONS

Article 22

Processing of personal data

1. The Commission shall process personal data needed for implementing this Decision in accordance with Regulation (EC) No 45/2001.

2. Notwithstanding the measures already in place at the time of adoption of this Decision and notified to the European Data Protection Supervisor ([1]), any measure under this Decision involving the processing of personal data, such as relating to access and exit logs, CCTV recordings, recordings of telephone calls to duty offices or dispatch centres and similar data, which are required for reasons of security or crisis response, shall be subject to implementing rules in accordance with Article 21, which shall lay down appropriate safeguards for data subjects.

3. The Director-General of the Directorate-General for Human Resources and Security shall be responsible for the security of any processing of personal data undertaken in the context of this Decision.

4. Those implementing rules and procedures shall be adopted after consultation of the Data Protection Officer and the European Data Protection Supervisor in accordance with Regulation (EC) No 45/2001.

Article 23

Transparency

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

Article 24

Repeal of previous decisions

Decision C(94) 2129 is repealed.

Article 25

Entry into force

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

Done at Brussels, 13 March 2015.

For the Commission
The President
Jean-Claude JUNCKER

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

COMMISSION DECISION (EU, Euratom) 2015/444

of 13 March 2015

on the security rules for protecting EU classified information

THE EUROPEAN COMMISSION,

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

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

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

Whereas:

(1) The Commission's security provisions regarding the protection of European Union Classified Information (EUCI) need to be reviewed and updated, taking into account institutional, organisational, operational and technological developments.

(2) The European Commission has entered into instruments on security matters for its principal sites with the governments of Belgium, Luxembourg and Italy ([1])

(3) The Commission, the Council and the European External Action Service are committed to applying equivalent security standards for protecting EUCI.

(4) It is important that, where appropriate, the European Parliament and other Union institutions, agencies, bodies or offices, are associated with the principles, standards and rules for protecting classified information which are necessary in order to protect the interests of the Union and its Member States.

(5) Risk to EUCI shall be managed as a process. This process shall be aimed at determining known security risks, defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in this Decision and at applying these measures in line with the concept of defence in depth. The effectiveness of such measures shall be continuously evaluated.

(6) Within the Commission, physical security aimed at protecting classified information is the application of physical and technical protective measures intended to prevent unauthorised access to EUCI.

(7) The management of EUCI is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Chapters 2, 3 and 5 of this Decision and thereby help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, storage, registration, copying, translation, downgrading, declassification, carriage and destruction of EUCI and they supplement the general rules on document management of the Commission (Decisions 2002/47/EC ([2]), ECSC, Euratom and 2004/563/EC, Euratom ([3])).

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

([2]) Commission Decision 2002/47/EC, ECSC, Euratom of 23 January 2002 amending its rules of procedure (OJ L 21, 24.1.2002, p. 23).

([3]) Commission Decision 2004/563/EC, Euratom of 7 July 2004 amending its Rules of Procedure (OJ L 251, 27.7.2004, p. 9).

(8) The provision of this Decision shall be without prejudice to:

(a) Regulation (Euratom) No 3 ([1]);

(b) Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([2]);

(c) Regulation (EC) No 45/2001 of the European Parliament and of the Council ([3]);

(d) Council Regulation (EEC, Euratom) No 354/83 ([4]),

HAS ADOPTED THIS DECISION:

CHAPTER 1

BASIC PRINCIPLES AND MINIMUM STANDARDS

Article 1

Definitions

For the purpose of this Decision, the following definitions shall apply:

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

(2) 'cryptographic (Crypto) material' means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material;

(3) 'declassification' means the removal of any security classification;

(4) 'defence in depth' means the application of a range of security measures organised as multiple layers of defence;

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

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

(7) 'handling' of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, registration, processing, carriage, downgrading, declassification and destruction. In relation to Communication and Information Systems (CIS) it also comprises its collection, display, transmission and storage;

(8) 'holder' means a duly authorised individual with an established need-to-know who is in possession of an item of EUCI and is accordingly responsible for protecting it;

(9) 'implementing rules' means any set of rules or security notices adopted in accordance with Chapter 5 of Commission Decision (EU, Euratom) 2015/443 ([5]);

(10) 'material' means any medium, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture;

(11) '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;

(12) 'premises' means any immovable or assimilated property and possessions of the Commission;

([1]) Regulation (Euratom) No 3 of 31 July 1958 implementing Article 24 of the Treaty establishing the European Atomic Energy Community (OJ 17, 6.10.1958, p. 406/58).
([2]) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).
([3]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).
([4]) 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 (OJ L 43, 15.2.1983, p. 1).
([5]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (See page 41 of this Official Journal).

(13) '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;

(14) 'Staff Regulations' means the Staff Regulations of officials of the European Union and the Conditions of Employment of other servants of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No 259/68 of the Council [1];

(15) '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;

(16) '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.

Article 2

Subject matter and scope

1. This Decision lays down the basic principles and minimum standards of security for protecting EUCI.

2. This Decision shall apply to all Commission departments and in all premises of the Commission.

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

4. The provisions of this Decision shall be without prejudice to Decision 2002/47/EC, ECSC, Euratom and Decision 2004/563/EC, Euratom.

Article 3

Definition of EUCI, security classifications and markings

1. 'European Union classified information' (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.

2. EUCI shall be classified at one of the following levels:

(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.

3. EUCI shall bear a security classification marking in accordance with paragraph 2. It may bear additional markings, which are not classification markings, but are intended to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

---

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

Article 4

Classification management

1. Each Member of the Commission or Commission department shall ensure that EUCI it creates, is appropriately classified, clearly identified as EUCI and retains its classification level for only as long as necessary.

2. Without prejudice to Article 26 below, EUCI shall not be downgraded or declassified nor shall any of the security classification markings referred to in Article 3(2) be modified or removed without the prior written consent of the originator.

3. Where appropriate, implementing rules on handling EUCI, including a practical classification guide, shall be adopted in accordance with Article 60 below.

Article 5

Protection of classified information

1. EUCI shall be protected in accordance with this Decision and its implementing rules.

2. The holder of any item of EUCI shall be responsible for protecting it, in accordance with this Decision and its implementing rules, according to the rules laid out in Chapter 4 below.

3. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the Commission, the Commission shall 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 Annex I.

4. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.

Article 6

Security risk management

1. Security measures for protecting EUCI 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 EUCI 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 EUCI 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 EUCI shall be included in all services' business continuity plans.

Article 7

Implementation of this Decision

1. Where necessary, implementing rules to supplement or support this Decision shall be adopted in accordance with Article 60 below.

2. The Commission departments shall take all necessary measures falling under their responsibility in order to ensure that, when handling or storing EUCI or any other classified information, this Decision and the relevant implementing rules are applied.

3. The security measures taken in implementation of this Decision shall be compliant with the principles for security in the Commission laid down in Article 3 of Decision (EU, Euratom) 2015/443.

4. The Director-General for Human Resources and Security shall set up the Commission Security Authority within the Directorate-General for Human Resources and Security. The Commission Security Authority shall have the responsibilities assigned to it by this Decision and its implementing rules.

5. Within each Commission department, the Local Security Officer (LSO), as referred to in Article 20 of Decision (EU, Euratom) 2015/443, shall have the following overall responsibilities for protecting EUCI in accordance with this Decision, in close cooperation with the Directorate-General for Human Resources and Security:

(a) managing requests for security authorisations for staff;

(b) contributing to security training and awareness briefings;

(c) supervising the department's Registry Control Officer (RCO);

(d) reporting on breaches of security and compromise of EUCI;

(e) holding spare keys and a written record of each combination setting;

(f) assuming other tasks related to the protection of EUCI or defined by implementing rules.

Article 8

Breaches of security and compromise of EUCI

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 EUCI 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 Commission Security Authority.

4. Where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, a security inquiry shall be conducted in accordance with Article 13 of Decision (EU, Euratom) 2015/443.

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

CHAPTER 2

PERSONNEL SECURITY

Article 9

Definitions

For the purpose of this Chapter, the following definitions apply:

(1) 'authorisation for access to EUCI' means a decision by the Commission Security Authority taken on the basis of an assurance given by a competent authority of a Member State that a Commission official, other servant or seconded national expert may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be 'security authorised'.

(2) 'personnel security authorisation' is the application of measures to ensure that access to EUCI is granted only to individuals who have:

(a) a need-to-know;

(b) been security authorised to the relevant level, where appropriate; and

(c) been briefed on their responsibilities.

(3) 'Personnel Security Clearance' (PSC) means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date;

(4) 'Personnel Security Clearance Certificate' (PSCC) means a certificate issued by a competent authority establishing that an individual holds a valid security clearance or a security authorisation issued by the Commission Security Authority and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the period of validity of the relevant security clearance or authorisation and the date of expiry of the certificate itself.

(5) 'security investigation' means the investigative procedures conducted by the competent authority of a Member State in accordance with its national laws and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a security clearance up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above).

Article 10

Basic Principles

1. An individual shall only be granted access to EUCI after

(1) his need-to-know has been determined;

(2) he has been briefed on the security rules for protecting EUCI and the relevant security standards and guidelines, and has acknowledged his responsibilities with regard to protecting such information;

(3) for information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above, he has been security authorised to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations.

2. All individuals whose duties may require them to have access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security authorised to the relevant level before being granted access to such EUCI. The individual concerned shall consent in writing to being submitted to the personnel security clearance procedure. Failure to do so shall mean that the individual cannot be assigned to a post, function or task which involves access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above.

3. Personnel security clearance procedures shall be designed to determine whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to access EUCI.

4. The loyalty, trustworthiness and reliability of an individual for the purposes of being security cleared for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be determined by means of a security investigation conducted by the competent authorities of a Member State in accordance with its national laws and regulations.

5. The Commission Security Authority shall be solely responsible for liaising with the national security authorities ('NSAs') or other competent national authorities in the context of all security clearance issues. All contacts between Commission services and their staff and the NSAs and other competent authorities shall be conducted through the Commission Security Authority.

Article 11

Security authorisation procedure

1. Each Director-General or head of service within the Commission shall identify the positions within his department for which the holders need to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above to perform their duties and so need to be security authorised.

2. As soon as it is known that an individual will be appointed to a position requiring access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, the LSO of the Commission department concerned shall inform the Commission Security Authority, which shall transmit to the individual the security clearance questionnaire issued by the NSA of the Member State under whose nationality the individual has been appointed as a staff member of the European institutions. The individual shall consent in writing to being submitted to the security clearance procedure and return the completed questionnaire within the shortest deadline to the Commission Security Authority.

3. The Commission Security Authority shall forward the completed security clearance questionnaire to the NSA of the Member State under whose nationality the individual has been appointed as a staff member of the European institutions, requesting that a security investigation be undertaken for the level of EUCI to which the individual will require access.

4. Where information relevant to a security investigation is known to the Commission Security Authority concerning an individual who has applied for a security clearance, the Commission Security Authority, acting in accordance with the relevant rules and regulations, shall notify the competent NSA thereof.

5. Following completion of the security investigation, and as soon as possible after having been notified by the relevant NSA of its overall assessment of the findings of the security investigation, the Commission Security Authority:

(a) may grant an authorisation for access to EUCI to the individual concerned and authorise access to EUCI up to the relevant level until a date specified by him but for a maximum of 5 years, where the security investigation results in an assurance that nothing adverse is known which would call into question the loyalty, trustworthiness and reliability of the individual;

(b) shall, where the security investigation does not result in such an assurance, in accordance with the relevant rules and regulations, notify the individual concerned, who may ask to be heard by the Commission Security Authority, who in turn may ask the competent NSA for any further clarification it can provide according to its national laws and regulations. If the outcome of the security investigation is confirmed, the authorisation for access to EUCI shall not be issued.

6. The security investigation together with the results obtained shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the Commission Security Authority shall be subject to appeals in accordance with the Staff Regulations.

7. The Commission shall accept the authorisation for access to EUCI granted by any other Union institution, body or agency provided it remains valid. Authorisations shall cover any assignment by the individual concerned within the Commission. The Union institution, body or agency in which the individual is taking up employment will notify the relevant NSA of the change of employer.

8. If an individual's period of service does not commence within 12 months of the notification of the outcome of the security investigation to the Commission Security Authority, or if there is a break of 12 months in an individual's service, during which time he has not been employed by the Commission or by any other Union Institution, body or agency, or in a position with a national administration of a Member State, the Commission Security Authority shall refer the matter to the relevant NSA for confirmation that the security clearance remains valid and appropriate.

9. Where information becomes known to the Commission Security Authority concerning a security risk posed by an individual who holds a valid security authorisation, the Security Authority, acting in accordance with the relevant rules and regulations, shall notify the competent NSA thereof.

10. Where an NSA notifies the Commission Security Authority of the withdrawal of an assurance given in accordance with paragraph 5(a) for an individual who holds a valid authorisation for access to EUCI, the Commission Security Authority may ask for any clarification the NSA can provide according to its national laws and regulations. If the adverse information is confirmed by the relevant NSA, the security authorisation shall be withdrawn and the individual shall be excluded from access to EUCI and from positions where such access is possible or where he might endanger security.

11. Any decision to withdraw or suspend an authorisation for access to EUCI from any individual falling under the scope of this Decision, and, where appropriate, the reasons for doing so, shall be notified to the individual concerned, who may ask to be heard by the Commission Security Authority. Information provided by an NSA shall be subject to the relevant laws and regulations in force in the Member State concerned. Decisions made in this context by the Commission Security Authority shall be subject to appeals in accordance with the Staff Regulations.

12. Commission departments shall make sure that national experts seconded to them for a position requiring security authorisation to access EUCI shall present, prior to taking up their assignment, a valid PSC or Personnel Security Clearance Certificate ('PSCC'), according to national law and regulations, to the Commission Security Authority, who, on the basis thereof, will grant a security authorisation for access to EUCI up to the level equivalent to the one referred to in the national security clearance, with a maximum validity for the duration of their assignment.

Access to EUCI for individuals duly authorised by virtue of their functions

13. The Members of the Commission, who have access to EUCI by virtue of their functions on the basis of the Treaty, shall be briefed on their security obligations in respect of protecting EUCI.

Security Clearance and security authorisation records

14. Records of security clearances and authorisations granted for access to EUCI shall be maintained by the Commission Security Authority in accordance with this Decision. These records shall contain as a minimum the level of EUCI to which the individual may be granted access, the date of issue of the security clearance and its period of validity.

15. The Commission Security Authority may issue a PSCC showing the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant authorisation for access to EUCI and the date of expiry of the certificate itself.

Renewal of security authorisations

16. After the initial granting of security authorisations and provided that the individual has had uninterrupted service with the European Commission or another Union Institution, body or agency and has a continuing need for access to EUCI, the security authorisation for access to EUCI shall be reviewed for renewal, as a general rule, every five years from the date of notification of the outcome of the last security investigation on which it was based.

17. The Commission Security Authority may extend the validity of the existing security authorisation for a period of up to 12 months, if no adverse information has been received from the relevant NSA or other competent national authority within a period of two months from the date of transmission of the request for renewal and the corresponding security clearance questionnaire. If, at the end of this 12-month period, the relevant NSA or other competent national authority has not notified the Commission Security Authority of its opinion, the individual shall be assigned to duties which do not require a security authorisation.

Article 12

Security authorisation briefings

1. After having participated in the security authorisation briefing organised by the Commission Security Authority, all individuals who have been security authorised shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Commission Security Authority.

2. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware, and periodically briefed on the threats to security and must report immediately to the Commission Security Authority any approach or activity that they consider suspicious or unusual.

3. All individuals who cease to be employed in duties requiring access to EUCI shall be made aware of, and where appropriate acknowledge in writing, their obligations in respect of the continued protection of EUCI.

Article 13

Temporary security authorisations

1. In exceptional circumstances, where duly justified in the interests of the service and pending completion of a full security investigation, the Commission Security Authority, may, after consulting the NSA of the Member State of which the individual is a national and subject to the outcome of preliminary checks to verify that no relevant adverse information is known, grant a temporary authorisation for individuals to access EUCI for a specific function, without prejudice to the provisions regarding renewal of security clearances. Such temporary authorisations for access to EUCI shall be valid for a single period not exceeding six months and shall not permit access to information classified TRES SECRET UE/EU TOP SECRET.

2. After having been briefed in accordance with Article 12(1), all individuals who have been granted a temporary authorisation shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Commission Security Authority

Article 14

Attendance at classified meetings organised by the Commission

1. Commission departments responsible for organising meetings at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed shall, through their LSO or through the meeting organiser, inform the Commission Security Authority well in advance of the dates, times, venue and participants of such meetings.

2. Subject to the provisions of Article 11(13), individuals assigned to participate in meetings organised by the Commission at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed, may only do so upon confirmation of their security clearance or security authorisation status. Access to such classified meetings shall be denied to individuals for whom the Commission Security Authority has not seen a PSCC or other proof of security clearance, or, to participants of the Commission who are not in possession of a security authorisation.

3. Before organising a classified meeting, the responsible meeting organiser or the LSO of the Commission department organising the meeting, shall request external participants to provide the Commission Security Authority a PSCC or other proof of security clearance. The Commission Security Authority shall inform the LSO or the meeting organiser of PSCC or other proof of PSC received. Where applicable, a consolidated list of names may be used, giving the relevant proof of security clearance.

4. Where the Commission Security Authority is informed by the competent authorities that a PSC has been withdrawn from an individual whose duties require attendance at meetings organised by the Commission, the Commission Security Authority shall notify the LSO of the Commission department responsible for organising the meeting.

Article 15

Potential Access to EUCI

Couriers, guards and escorts shall be security authorised to the appropriate level or otherwise appropriately investigated in accordance with national laws and regulations, be briefed on security procedures for protecting EUCI and be instructed on their duties for protecting such information entrusted to them.

CHAPTER 3

PHYSICAL SECURITY AIMED AT PROTECTING CLASSIFIED INFORMATION

Article 16

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 EUCI 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 EUCI by:

(a) ensuring that EUCI is handled and stored in an appropriate manner;

(b) allowing for segregation of personnel in terms of access to EUCI on the basis of their need-to-know and, where appropriate, their security authorisation;

(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 EUCI is handled or stored, including areas housing communication and information systems as referred to in Chapter 5.

4. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with this Chapter and accredited by the Commission Security Accreditation Authority.

5. Only equipment or devices approved by the Commission Security Authority shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

Article 17

Physical security requirements and measures

1. Physical security measures shall be selected on the basis of a threat assessment made by the Commission Security Authority, where appropriate in consultation with other Commission departments, other Union institutions, agencies or bodies and/or competent authorities in the Member States. The Commission shall apply a risk management process for protecting EUCI 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 EUCI;

(b) the form and volume of EUCI, bearing in mind that large quantities or a compilation of EUCI may require more stringent protective measures to be applied;

(c) the surrounding environment and structure of the buildings or areas housing EUCI; 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 Commission Security Authority, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. To that effect, the Commission Security Authority shall develop minimum standards, norms and criteria, set out in implementing rules.

3. The Commission Security Authority is authorised to conduct entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of EUCI from premises or buildings.

4. When EUCI is at risk of being overlooked, even accidentally, the Commission departments concerned shall take the appropriate measures, as defined by the Commission Security Authority, to counter this risk.

5. For new facilities, physical security requirements and their functional specifications shall be defined in consent with the Commission Security Authority 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 implementing rules.

Article 18

Equipment for the physical protection of EUCI

1. Two types of physically protected areas shall be established for the physical protection of EUCI:

(a) Administrative Areas; and

(b) Secured Areas (including technically Secured Areas).

2. The Commission Security Accreditation Authority shall establish that an area meets the requirements to be designated as an Administrative Area, a Secured Area or a technically Secured 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 Commission Security Authority or any other competent authority; and

(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

4. For Secured Areas:

(a) a visibly defined and protected perimeter shall be established through which all entry and exit is controlled by means of a pass or personal recognition system;

(b) unescorted access shall be granted only to individuals who are security-cleared and specifically authorised to enter the area on the basis of their need-to-know;

(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

5. Where entry into a Secured Area constitutes, for all practical purposes, direct access to the classified information contained in it, the following additional requirements shall apply:

(a) the level of highest security classification of the information normally held in the area shall be clearly indicated;

(b) all visitors shall require specific authorisation to enter the area, shall be escorted at all times and shall be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible.

6. Secured Areas protected against eavesdropping shall be designated technically Secured Areas. The following additional requirements shall apply:

(a) such areas shall be equipped with an Intrusion Detection System ('IDS'), be locked when not occupied and be guarded when occupied. Any keys shall be managed in accordance with Article 20;

(b) all persons and material entering such areas shall be controlled;

(c) such areas shall be regularly physically and/or technically inspected by the Commission Security Authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such entry; and

(d) such areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment.

7. Notwithstanding point (d) of paragraph 6, before being used in areas where meetings are held or work is being performed involving information classified SECRET UE/EU SECRET and above, and where the threat to EUCI is assessed as high, any communications devices and electrical or electronic equipment shall first be examined by the Commission Security Authority to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area.

8. Secured Areas which are not occupied by duty personnel on a 24-hour basis shall, where appropriate, be inspected at the end of normal working hours and at random intervals outside normal working hours, unless an IDS is in place.

9. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.

10. The LSO of the Commission department concerned shall draw up Security Operating Procedures (SecOPs) for each Secured Area under his responsibility stipulating, in accordance with the provisions of this Decision and its implementing rules:

(a) the level of EUCI which may be handled and stored in the area;

(b) the surveillance and protective measures to be maintained;

(c) the individuals authorised to have unescorted access to the area by virtue of their need-to-know and security authorisation;

(d) where appropriate, the procedures for escorts or for protecting EUCI when authorising any other individuals to access the area;

(e) any other relevant measures and procedures.

11. Strong rooms shall be constructed within Secured Areas. The walls, floors, ceilings, windows and lockable doors shall be approved by the Commission Security Authority and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

Article 19

Physical protective measures for handling and storing EUCI

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

(a) in a Secured Area,

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals, or

(c) outside a Secured Area or an Administrative Area provided the holder carries the EUCI in accordance with Article 31 and has undertaken to comply with compensatory measures, set out in implementing measures, to ensure that EUCI is protected from access by unauthorised persons.

2. EUCI which is classified RESTREINT UE/EU RESTRICTED shall be stored in suitable locked office furniture in an Administrative Area or a Secured Area. It may temporarily be stored outside an Administrative Area or a Secured Area provided the holder has undertaken to comply with compensatory measures laid down in implementing rules.

3. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be handled:

(a) in a Secured Area;

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals; or

(c) outside a Secured Area or an Administrative Area provided the holder:

(i) has undertaken to comply with compensatory measures, set out in implementing rules, to ensure the EUCI is protected from access by unauthorised persons;

(ii) keeps the EUCI at all times under his personal control; and

(iii) in the case of documents in paper form, has notified the relevant registry of the fact.

4. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be stored in a Secured Area in a security container or a strong room.

5. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be handled in a Secured Area, set up and maintained by the Commission Security Authority, and accredited to that level by the Commission Security Accreditation Authority.

6. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be stored in a Secured Area, accredited to that level by the Commission Security Accreditation Authority, under one of the following conditions:

(a) in a security container in accordance with the provisions of Article 18 with one or more of the following supplementary controls:

(1) continuous protection or verification by cleared security staff or duty personnel;

(2) an approved IDS in combination with security response personnel;

or

(b) in an IDS-equipped strong room in combination with security response personnel.

Article 20

Management of keys and combinations used for protecting EUCI

1. Procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers shall be laid down in implementing rules according to Article 60 below. Such procedures shall be intended to guard against unauthorised access.

2. Combination settings shall be committed to memory by the smallest possible number of individuals needing to know them. Combination settings for security containers and strong rooms 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 4

MANAGEMENT OF EU CLASSIFIED INFORMATION

Article 21

Basic principles

1. All EUCI documents should be managed in compliance with the Commission's policy on document management and consequently should be registered, 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.

2. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt. Information classified TRES SECRET UE/EU TOP SECRET shall be registered in designated registries.

3. Within the Commission, a EUCI registry system shall be set up in accordance with the provisions of Article 27.

4. Commission departments and premises where EUCI is handled or stored shall be subject to regular inspection by the Commission Security Authority.

5. 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 5;

(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 5; or

(ii) in all other cases, as prescribed in implementing rules.

Article 22

Classifications and markings

1. Information shall be classified where it requires protection with regard to its confidentiality, in accordance with Article 3(1).

2. The originator of EUCI shall be responsible for determining the security classification level, in accordance with the relevant implementing rules, standards and guidelines regarding classification, and for the initial dissemination of the information.

3. The classification level of EUCI shall be determined in accordance with Article 3(2) and with the relevant implementing rules.

4. The security classification shall be clearly and correctly indicated, regardless of whether the EUCI is on paper, oral, electronic or in any other form.

5. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and be marked accordingly, including when stored in electronic form.

6. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.

7. To the extent possible, documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.

8. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator shall 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

Article 23

Markings

In addition to one of the security classification markings set out in Article 3(2), EUCI 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 downgraded or declassified.

Article 24

Abbreviated classification markings

1. Standardised abbreviated classification markings may be used to indicate the classification level of individual paragraphs of a text. Abbreviations shall not replace the full classification markings.

2. 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

Article 25

Creation of EUCI

1. 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 registration number and a subject, which is not itself classified information, unless it is marked as such;

(d) the document shall be dated;

(e) documents classified SECRET UE/EU SECRET or above shall bear a copy number on every page, if they are to be distributed in several copies.

2. Where it is not possible to apply paragraph 1 to EUCI, other appropriate measures shall be taken in accordance with implementing rules.

Article 26

Downgrading and declassification of EUCI

1. At the time of its creation, the originator shall indicate, where possible, whether EUCI can be downgraded or declassified on a given date or following a specific event.

2. Each Commission department shall regularly review EUCI for which it is the originator to ascertain whether the classification level still applies. A system to review the classification level of registered EUCI which has originated in the Commission no less frequently than every five years shall be established by implementing rules. Such a review shall not be necessary where the originator has indicated from the outset that the information will automatically be downgraded or declassified and the information has been marked accordingly.

3. Information classified RESTREINT UE/EU RESTRICTED having originated in the Commission will be considered to be automatically declassified after thirty years, in accordance with Regulation (EEC, Euratom) No 354/83 as amended by Council Regulation (EC, Euratom) No 1700/2003 ([1]).

Article 27

EUCI registry system in the Commission

1. Without prejudice to Article 52 paragraph 5 below, in each Commission department in which EUCI is handled or stored at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET, a responsible local EUCI registry shall be identified to ensure that EUCI is handled in accordance with this Decision.

2. The EUCI registry managed by the Secretariat-General shall be the Commission's Central EUCI Registry. It shall act as:

— the Local EUCI Registry for the Commission's Secretariat-General,

— the EUCI registry for the private offices of Members of the Commission, unless these have a designated local EUCI registry,

— the EUCI registry for Directorates-General or services which do not have a local EUCI registry,

— the main point of entry and exit for all information classified RESTREINT UE/EU RESTRICTED and up to including SECRET UE/EU SECRET exchanged between the Commission and its services and third States and international organisations, and, when provided for in specific arrangements, for other Union institutions, agencies and bodies.

3. Within the Commission, a registry shall be designated by the Commission Security Authority to act as the central receiving and dispatching authority for information classified TRES SECRET UE/EU TOP SECRET. Where necessary, subordinate registries may be designated to handle that information for registration purposes.

4. The subordinate registries may not transmit TRES SECRET UE/EU TOP SECRET documents directly to other subordinate registries of the same central TRES SECRET UE/EU TOP SECRET registry or externally without the express written approval of the latter.

5. EUCI registries shall be established as Secured Areas as defined in Chapter 3, and accredited by the Commission's Security Accreditation Authority (SAA).

Article 28

Registry control officer

1. Each EUCI registry shall be managed by a Registry Control Officer ('RCO').

2. The RCO shall be appropriately security-cleared.

3. The RCO shall be subject to the supervision of the LSO within the Commission department, as far as the application of the provisions regarding the handling of EUCI documents and compliance with the relevant security rules, standards and guidelines is concerned.

4. Within his responsibility for managing the EUCI Registry to which he has been assigned, the RCO shall assume the following overall tasks in accordance with this Decision and the relevant implementing rules, standards and guidelines:

— manage operations relating to the registration, preservation, reproduction, translation, transmission, dispatch and destruction or transfer to the historical archives service of EUCI,

— verify periodically the need to maintain the classification of information,

— assume any other tasks related to the protection of EUCI defined in implementing rules.

Article 29

Registration of EUCI for security purposes

1. For the purposes of this Decision, registration for security purposes (hereinafter referred to as 'registration') means the application of procedures which record the life-cycle of EUCI, including its dissemination.

([1]) 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).

2. All information or material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered in designated registries when it is received in or dispatched from an organisational entity.

3. When EUCI is handled or stored using a Communication and Information System (CIS), registration procedures may be performed by processes within the CIS itself.

4. More detailed provisions concerning the registration of EUCI for security purposes shall be laid down in implementing rules.

Article 30

Copying and translating EU classified documents

1. TRES SECRET UE/EU TOP SECRET documents shall not be copied or translated without the prior written consent of the originator.

2. Where the originator of documents classified SECRET UE/EU SECRET and below has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder.

3. The security measures applicable to the original document shall apply to copies and translations thereof.

Article 31

Carriage of EUCI

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

2. 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 a Commission building or a self-contained group of Commission buildings,

  — between Commission buildings located in the same Member State,

  — within the Union,

  — from within the Union to the territory of a third State, and

  — be adapted to the nature and form of the EUCI.

3. These protective measures shall be laid down in detail in implementing rules, or, in case of projects and programmes referred to in Article 42, as an integral part of the relevant Programme or Project Security Instructions (PSI).

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

— the type of carriage, such as hand carriage, carriage by diplomatic or military 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,

— registration procedures,

— use of security authorised personnel.

5. When EUCI is carried on electronic media, and notwithstanding Article 21, paragraph 5, the protective measures set out in the relevant implementing rules may be supplemented by appropriate technical countermeasures approved by the Commission Security Authority so as to minimise the risk of loss or compromise.

Article 32

Destruction of EUCI

1. EU classified documents which are no longer required may be destroyed, taking account of regulations on archives and of the Commission's rules and regulations on document management and archiving, and in particular with the Common Commission-Level Retention List.

2. EUCI of the level of CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be destroyed by the RCO of the responsible EUCI registry on instruction from the holder or from a competent authority. The RCO shall update the logbooks and other registration information accordingly.

3. For documents classified SECRET UE/EU SECRET or TRES SECRET UE/EU TOP SECRET, such destruction shall be performed by the RCO in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.

4. The registrar and the witness, where the presence of the latter is required, shall sign a destruction certificate, which shall be filed in the registry. The RCO of the responsible EUCI registry shall keep destruction certificates of TRES SECRET UE/EU TOP SECRET documents for a period of at least 10 years and for documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET for a period of at least five years.

5. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which shall be defined in implementing rules and which shall meet relevant EU or equivalent standards.

6. Computer storage media used for EUCI shall be destroyed in accordance with procedures laid down in implementing rules.

Article 33

Destruction of EUCI in emergencies

1. Commission departments holding EUCI shall prepare plans based on local conditions for the safeguarding of EU classified material in a crisis including if necessary emergency destruction and evacuation plans. They shall promulgate instructions deemed necessary to prevent EUCI from falling into unauthorised hands.

2. The arrangements for the safeguarding and/or destruction of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET material in a crisis shall under no circumstances adversely affect the safeguarding or destruction of TRES SECRET UE/EU TOP SECRET material, including the enciphering equipment, whose treatment shall take priority over all other tasks.

3. In the event of an emergency, if there is an imminent risk of unauthorised disclosure, EUCI shall be destroyed by the holder in such a way that it cannot be reconstructed in whole or in part. The originator and originating registry shall be informed of the emergency destruction of registered EUCI.

4. More detailed provisions for destruction of EUCI shall be laid down in implementing rules.

CHAPTER 5

PROTECTION OF EU CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

Article 34

Basic principles of Information Assurance

1. Information Assurance (IA) 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. IA shall be based on a risk management process.

Article 35

Definitions

For the purpose of this Chapter, the following definitions apply:

(a) 'Accreditation' means the formal authorisation and approval granted to a communication and information system by the Security Accreditation Authority (SAA) to process EUCI in its operational environment, following the formal validation of the Security Plan and its correct implementation;

(b) '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;

(c) 'Communication and Information System' (CIS) means any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources;

(d) '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;

(e) '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;

(f) 'Risk acceptance' is the decision to agree to the further existence of a residual risk after risk treatment;

(g) 'Risk assessment' consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact;

(h) 'Risk communication' consists of developing awareness of risks among CIS user communities, informing approval authorities of such risks and reporting them to operating authorities;

(i) 'Risk treatment' consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk.

Article 36

CIS handling EUCI

1. CIS shall handle EUCI in accordance with the concept of IA.

2. For CIS handling EUCI, compliance with the Commission's information systems security policy, as referred to in Commission Decision C(2006)3602 ([1]), 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;

([1]) C(2006) 3602 of 16 August 2006 concerning the security of information systems used by the European Commission.

(d) all mandatory security measures as determined by the policy on 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 EUCI shall notify to the SAA all potential security weaknesses, incidents, breaches of security or compromise which may have an impact on the protection of the CIS and/or the EUCI therein.

4. Where the protection of EUCI 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 of the Commission Security Expert Group;

(b) where warranted on specific operational grounds, the Commission Crypto Approval Authority (CAA) may, upon recommendation of the Commission Security Expert Group, waive the requirements referred to under a) and grant an interim approval for a specific period.

5. During transmission, processing and storage of EUCI 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 CAA.

6. Security measures shall be implemented to protect CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above against compromise of such information through unintentional electromagnetic emanations ('TEMPEST security measures'). Such security measures shall be commensurate with the risk of exploitation and the level of classification of the information.

7. The Commission Security Authority shall assume the following functions:

— IA Authority (IAA),

— Security Accreditation Authority (SAA),

— TEMPEST Authority (TA),

— Crypto Approval Authority (CAA),

— Crypto Distribution Authority (CDA).

8. The Commission Security Authority shall appoint for each system the IA Operational Authority.

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

Article 37

Accreditation of CIS handling EUCI

1. All CIS handling EUCI shall undergo an accreditation process, based upon the principles of IA, whose level of detail must be commensurate with the level of protection required.

2. The accreditation process shall include the formal validation by the Commission SAA of the Security Plan for the CIS concerned in order to obtain assurance that:

(a) the risk management process, as referenced in Article 36(2), has been properly carried out;

(b) the System Owner 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 Commission's SAA shall issue an accreditation statement which determines the maximum classification level of the EUCI that may be handled in the CIS as well as the corresponding terms and conditions for operation. This is without prejudice to the tasks entrusted to the Security Accreditation Board defined in Article 11 of Regulation (EU) No 512/2014 of the European Parliament and of the Council [1].

4. A joint Security Accreditation Board (SAB) shall be responsible for accrediting Commission's CIS involving several parties. It shall be composed of a SAA representative of each party involved and be chaired by an SAA representative of the Commission.

5. 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.

6. The accreditation shall be the responsibility of the Commission SAA, 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 operation are no any 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 operation are again satisfied.

7. The accreditation process shall be established in a standard on the accreditation process for CIS handling EUCI, which shall be adopted in accordance with Article 10(3) of Decision C(2006) 3602.

Article 38

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. EUCI may be transmitted using cryptographic products which have been approved for a lower classification level or 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 and to the Commission Security Expert Group.

CHAPTER 6

INDUSTRIAL SECURITY

Article 39

Basic principles

1. Industrial security is the application of measures to ensure the protection of EUCI

(a) within the framework of classified contracts, by:

(i) candidates or tenderers throughout the tendering and contracting procedure;

(ii) contractors or subcontractors throughout the life-cycle of classified contracts;

[1] Regulation (EU) No 512/2014 of the European Parliament and of the Council of 16 April 2014 amending Regulation (EU) No 912/2010 setting up the European GNSS Agency (OJ L 150, 20.5.2014, p. 72).

(b) within the framework of classified grant agreements, by

(i) applicants during grant award procedures;

(ii) beneficiaries throughout the life-cycle of classified grant agreements.

2. Such contracts or grant agreements shall not involve information classified TRES SECRET UE/EU TOP SECRET.

3. Unless stated otherwise, provisions in this Chapter referring to classified contracts or contractors shall be applicable also to classified subcontracts or subcontractors.

Article 40

Definitions

For the purpose of this Chapter, the following definitions shall apply:

(a) 'Classified contract' means a framework contract or contract, as referred to in Council Regulation (EC, Euratom) No 1605/2002 ([1]), entered into by the Commission or one of its departments, with a contractor for the supply of movable or immovable assets, the execution of works or the provision of services, the performance of which requires or involves the creation, handling or storing of EUCI;

(b) 'Classified subcontract' means a contract entered into by a contractor of the Commission or one of its departments, with another contractor (i.e. the subcontractor) for the supply of movable or immovable assets, the execution of works or the provision of services, the performance of which requires or involves the creation, handling or storing of EUCI;

(c) 'Classified grant agreement' means an agreement whereby the Commission awards a grant, as referred to in Part I, Title VI, of Regulation (EC, Euratom) No 1605/2002, the performance of which requires or involves the creation, handling or storing of EUCI;

(d) 'Designated Security Authority' (DSA) means an authority responsible to the National Security Authority (NSA) of a Member State which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority.

Article 41

Procedure for classified contracts or grant agreements

1. Each Commission department, as contracting authority, shall ensure that the minimum standards on industrial security set out in this Chapter, are referred to or incorporated in the contract, and complied with when awarding classified contracts or grant agreements.

2. For the purposes of paragraph 1, the competent services within the Commission shall seek the advice of the Directorate-General for Human Resources and Security, and in particular its Security Directorate, and shall ensure that model contracts and subcontracts and model grant agreements include provisions reflecting the basic principles and minimum standards for protecting EUCI to be complied with by contractors and subcontractors, and respectively beneficiaries of grant agreements.

3. The Commission shall closely cooperate with the NSA, the DSA or any other competent authority of the Member States concerned.

4. When a contracting authority, intends to launch a procedure aimed at concluding a classified contract or grant agreement, it shall seek the advice of the Commission Security Authority on issues regarding the classified nature and elements of the procedure, during all its stages.

5. Templates for and models of classified contracts and subcontracts, classified grant agreements, contract notices, guidance on the circumstances where Facility Security Clearances (FSCs) are required, Programme or Project Security Instructions (PSI), Security Aspects Letters (SALs), visits, transmission and carriage of EUCI under classified contracts or classified grant agreements shall be laid down in implementing rules on industrial security, after consulting the Commission Security Expert Group.

([1]) Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities (OJ L 248, 16.9.2002, p. 1).

6. The Commission may conclude classified contracts or grant agreements which entrust tasks involving or entailing access to or the handling or storage of EUCI by economic operators registered in a Member State or in a third State with which an agreement or an administrative arrangement has been concluded in accordance with Chapter 7 of this Decision.

Article 42

Security elements in a classified contract or grant agreement

1. Classified contracts or grant agreements shall include the following security elements:

Programme or Project Security Instructions

(a) 'Programme or Project Security Instruction' (PSI) means a list of security procedures which are applied to a specific programme or project in order to standardise security procedures. It may be revised throughout the programme or project.

(b) The Directorate-General Human Resources and Security shall develop a generic PSI, the Commission departments responsible for programmes or projects involving handling or storage of EUCI may develop, where appropriate, specific PSIs, which shall be based upon the generic PSI.

(c) A specific PSI shall be developed in particular for programmes and projects characterised by their considerable scope, scale or complexity, or by the multitude and/or the diversity of contractors, beneficiaries and other partners and stakeholders involved, for instance as regards their legal status. The specific PSI shall be developed by the Commission department(s) managing the programme or project, in close cooperation with the Directorate-General Human Resources and Security.

(d) The Directorate-General Human Resources and Security shall submit both the generic and specific PSIs for advice to the Commission Security Expert Group.

Security Aspects Letter

(a) 'Security Aspects Letter' (SAL) means a set of special contractual conditions, issued by the contracting authority, which forms an integral part of any classified contract involving access to or the creation of EUCI, that identifies the security requirements and those elements of the contract requiring security protection.

(b) The contract-specific security requirements shall be described in a SAL. The SAL shall, where appropriate, contain the Security Classification Guide ('SCG') and shall be an integral part of a classified contract or sub-contract, or grant agreement.

(c) The SAL shall contain the provisions requiring the contractor or beneficiary to comply with the minimum standards laid down in this Decision. The contracting authority shall ensure the SAL indicates that non-compliance with these minimum standards may constitute sufficient grounds for the contract or the grant agreement to be terminated.

2. Both PSIs and SALs shall include a SCG as a mandatory security element:

(a) 'Security Classification Guide' (SCG) means a document which describes the elements of a programme, project, contract or grant agreement which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme, project, contract or grant agreement and the elements of information may be re-classified or downgraded; where an SCG exists it shall be part of the SAL.

(b) Prior to launching a call for tender or letting a classified contract, the Commission department, as contracting authority, shall determine the security classification of any information to be provided to candidates and tenderers or contractors, as well as the security classification of any information to be created by the contractor. For that purpose, it shall prepare an SCG to be used for the performance of the contract, in accordance with this Decision and its implementing rules, after consulting the Commission Security Authority.

(c) In order to determine the security classification of the various elements of a classified contract, the following principles shall apply:

(i) in preparing an SCG, the Commission department, as the contracting authority, shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract by the originator of the information;

(ii) the overall level of classification of the contract may not be lower than the highest classification of any of its elements; and

(iii) where relevant, the contracting authority shall liaise, through the Commission Security Authority, with the Member States' NSAs, DSAs or any other competent security authority concerned in the event of any changes regarding the classification of information created by or provided to contractors in the performance of a contract and when making any subsequent changes to the SCG.

Article 43

Access to EUCI for contractors' and beneficiaries' staff

The contracting or granting authority, shall ensure that the classified contract or classified grant agreement includes provisions indicating that staff of a contractor, subcontractor or beneficiary who, for the performance of the classified contract, subcontract or grant agreement, require access to EUCI, shall be granted such access only if:

(a) he has been security authorised to the relevant level or is otherwise duly authorised by their need-to-know has been determined;

(b) they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regard to protecting such information;

(c) they have been security cleared at the relevant level for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET by the respective NSA, DSA or any other competent authority.

Article 44

Facility security clearance

1. 'Facility Security Clearance' (FSC) means an administrative determination by a NSA, DSA or any other competent security authority that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI to a specified security classification level.

2. A FSC granted by the NSA or DSA or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an economic operator can protect EUCI at the appropriate classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) within its facilities, shall be presented to the Commission Security Authority, which will forward it to the Commission department acting as the contracting or granting authority, before a candidate, tenderer or contractor, or grant applicant or beneficiary may be provided with or granted access to EUCI.

3. Where relevant, the contracting authority shall notify, through the Commission Security Authority, the appropriate NSA, DSA or any other competent security authority that an FSC is required for performing the contract. A FSC or PSC shall be required where EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the procurement or grant award procedure.

4. The contracting or granting authority shall not award a classified contract or a grant agreement to a preferred bidder or participant before having received confirmation from the NSA, DSA or any other competent security authority of the Member State in which the contractor or subcontractor concerned is registered that, where required, an appropriate FSC has been issued.

5. When the Commission Security Authority has been notified by the NSA, DSA or any other competent security authority which has issued a FSC about changes affecting the FSC, it shall inform the Commission department, acting as contracting or granting authority. In the case of a sub-contract, the NSA, DSA or any other competent security authority shall be informed accordingly.

6. Withdrawal of a FSC by the relevant NSA, DSA or any other competent security authority shall constitute sufficient grounds for the contracting or granting authority, to terminate a classified contract or exclude a candidate, tenderer or applicant from the competition. A provision to that effect shall be included in the model contracts and grant agreements to be developed.

Article 45

Provisions for classified contracts and grant agreements

1. Where EUCI is provided to a candidate, tenderer or applicant during the procurement procedure, the call for tender or call for proposal shall contain a provision obliging the candidate, tenderer or applicant failing to submit a tender or proposal or who is not selected, to return all classified documents within a specified period of time.

2. The contracting or granting authority, shall notify, through the Commission Security Authority, the competent NSA, DSA or any other competent security authority of the fact that a classified contract or grant agreement has been awarded, and of the relevant data, such as the name of the contractor(s) or beneficiaries, the duration of the contract and the maximum level of classification.

3. When such contracts or grant agreements are terminated, the contracting or granting authority, shall promptly notify, through the Commission Security Authority, the NSA, DSA or any other competent security authority of the Member State in which the contractor or grant beneficiary is registered.

4. As a general rule, the contractor or grant beneficiary shall be required to return to the contracting or granting authority, upon termination of the classified contract or the grant agreement, or of the participation of a grant beneficiary, any EUCI held by it.

5. Specific provisions for the disposal of EUCI during the performance of the classified contract or the classified grant agreement or upon its termination shall be laid down in the SAL.

6. Where the contractor or grant beneficiary is authorised to retain EUCI after termination of a classified contract or grant agreement, the minimum standards contained in this Decision shall continue to be complied with and the confidentiality of EUCI shall be protected by the contractor or the grant beneficiary.

Article 46

Specific provisions for classified contracts

1. The conditions relevant for the protection of EUCI under which the contractor may subcontract shall be defined in the call for tender and in the classified contract.

2. A contractor shall obtain permission from the contracting authority, before sub-contracting any parts of a classified contract. No subcontract involving access to EUCI may be awarded to subcontractors registered in a third country, unless there is a regulatory framework for the security of information as provided for in Chapter 7.

3. The contractor shall be responsible for ensuring that all sub-contracting activities are undertaken in accordance with the minimum standards laid down in this Decision and shall not provide EUCI to a subcontractor without the prior written consent of the contracting authority.

4. With regard to EUCI created or handled by the contractor, the Commission shall be considered to be the originator, and the rights incumbent on the originator shall be exercised by the contracting authority.

Article 47

Visits in connection with classified contracts

1. Where a Commission staff member or contractors' or grant beneficiaries' personnel require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract or grant agreement, visits shall be arranged in liaison with the NSAs, DSAs or any other competent security authority concerned. The Commission Security Authority shall be informed of such visits. However, in the context of specific programmes or projects, the NSAs, DSAs or any other competent security authority may also agree on a procedure whereby such visits can be arranged directly.

2. All visitors shall hold an appropriate security clearance and have a 'need-to-know' for access to the EUCI related to the classified contract.

3. Visitors shall be given access only to EUCI related to the purpose of the visit.

4. More detailed provisions shall be set out in implementing rules.

5. Compliance with the provisions regarding visits in connection with classified contracts, set out in this Decision and in the implementing rules referred to in paragraph 4, shall be mandatory.

Article 48

Transmission and carriage of EUCI in connection with classified contracts or classified grant agreements

1. With regard to the transmission of EUCI by electronic means, the relevant provisions of Chapter 5 of this Decision shall apply.

2. With regard to the carriage of EUCI, the relevant provisions of Chapter 4 of this Decision and its implementing rules shall apply, in accordance with national laws and regulations.

3. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:

(a) security shall be assured at all stages during transportation from the point of origin to the final destination;

(b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;

(c) prior to any cross-border movement of material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, a transportation plan shall be drawn up by the consignor and approved by the NSA, DSA or any other competent security authority concerned;

(d) journeys shall be point to point to the extent possible, and shall be completed as quickly as circumstances permit;

(e) whenever possible, routes should be only through Member States. Routes through States other than Member States should only be undertaken when authorised by the NSA, DSA or any other competent security authority of the States of both the consignor and the consignee.

Article 49

Transfer of EUCI to contractors or grant beneficiaries located in third states

EUCI shall be transferred to contractors or grant beneficiaries located in third States in accordance with security measures agreed between the Commission Security Authority, the Commission department, as the contracting or granting authority, and the NSA, DSA or other competent security authority of the concerned third country where the contractor or grant beneficiary is registered.

Article 50

Handling of information classified RESTREINT UE/EU RESTRICTED in the context of classified contracts or classified grant agreements

1. Protection of information classified RESTREINT UE/EU RESTRICTED handled or stored under classified contracts or grant agreements shall be based on the principles of proportionality and cost-effectiveness.

2. No FSC or PSC shall be required in the context of classified contracts or classified grant agreements involving the handling of information classified at the level of RESTREINT UE/EU RESTRICTED.

3. Where a contract or grant agreement involves handling of information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor or grant beneficiary, the contracting or granting authority shall ensure, after consulting the Commission Security Authority, that the contract or grant agreement specifies the necessary technical and administrative requirements regarding accreditation or approval of the CIS commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation or approval of such CIS shall be agreed between the Commission Security Authority and the relevant NSA or DSA.

CHAPTER 7

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

Article 51

Basic principles

1. Where the Commission or one of its departments determines that there is a need to exchange EUCI with another Union Institution, agency, body or office, or with a third State or international organisation, the necessary steps shall be undertaken to establish an appropriate legal or administrative framework to that effect, which may include security of information agreements or administrative arrangements concluded in accordance with the relevant regulations.

2. Without prejudice to Article 57, EUCI shall only be exchanged with another Union Institution, agency, body or office, or with a third State or international organisation, provided such an appropriate legal or administrative framework is in place, and that there are sufficient guarantees that the Union Institution, agency, body or office, or the third State or international organisation concerned applies equivalent basic principles and minimum standards for the protection of classified information.

Article 52

Exchange of EUCI with other Union institutions, agencies, bodies and offices

1. Before entering into an administrative arrangement for the exchange of EUCI with another Union Institution, agency, body or office, the Commission 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 EUCI and security of Communication and Information Systems (CIS), which guarantee an equivalent level of protection of EUCI as that afforded in the Commission.

(c) marks classified information which it creates, as EUCI.

2. The Directorate-General Human Resources and Security shall, in close cooperation with other competent Commission departments, be the lead service within the Commission for the conclusion of administrative arrangements for the exchange of EUCI with other Union institutions, agencies, bodies or offices.

3. Administrative arrangements shall as a general rule take the form of an Exchange of Letters, signed by the Director-General for Human Resources and Security on behalf of the Commission.

4. Before entering into an administrative arrangement on the exchange of EUCI, the Commission Security Authority shall conduct an assessment visit aimed at assessing the regulatory framework for protecting EUCI and ascertaining the effectiveness of measures implemented for protecting EUCI. The administrative arrangement shall enter into force, and EUCI shall be exchanged, 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.

5. Within the Commission, the EUCI registry managed by the Secretariat General shall, as a general rule, be the main point of entry and exit for classified information exchanges with other Union institutions, agencies, bodies and offices. However, where on security, organisational or operational grounds it is more appropriate for protecting EUCI, local EUCI registries established within Commission departments in accordance with this Decision and its implementing rules, shall operate as the point of entry and exit for classified information regarding matters within the competence of the Commission departments concerned.

6. The Commission Security Expert Group shall be informed of the process of concluding administrative arrangements pursuant to paragraph 2.

Article 53

Exchange of EUCI with Member States

1. EUCI may be exchanged with and released to 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 I.

2. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the European Union, the Commission shall 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 Annex I.

Article 54

Exchange of EUCI with third States and international organisations

1. Where the Commission determines that it has a long-term need to exchange classified information with third States or international organisations, the necessary steps shall be undertaken to establish an appropriate legal or administrative framework to that effect, which may include security of information agreements or administrative arrangements concluded in accordance with the relevant regulations.

2. Such security of information agreements and administrative agreements referred to in paragraph 1 shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are equivalent to those laid down in this Decision.

3. The Commission may enter into administrative arrangements in accordance with Article 56 where the classification level of EUCI is as a general rule no higher than RESTREINT UE/EU RESTRICTED.

4. Administrative arrangements for the exchange of classified information referred to in paragraph 3 shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are equivalent to those laid down in this Decision. The Commission Security Expert Group shall be consulted on the conclusion of security of information agreements or administrative arrangements.

5. The decision to release EUCI originating in the Commission to a third State or international organisation shall be taken by the Commission department, as originator of this EUCI within the Commission, 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 the Commission, the Commission department which holds this classified information, shall first seek the originator's written consent to release. If the originator cannot be established, the Commission department, which holds this classified information, shall assume the former's responsibility after consulting the Commission Security Expert Group.

Article 55

Security of information agreements

1. Security of information agreements with third states or international organisations are concluded in accordance with Article 218 TFEU.

2. Security of information agreements shall:

(a) establish the basic principles and minimum standards governing the exchange of classified information between the Union and a third State or international organisation;

(b) provide for technical implementing arrangements to be agreed between the competent security authorities of the relevant Union institutions and bodies and the competent security authority of the third State or international organisation in question. Such arrangements shall take account of the level of protection provided by the security regulations, structures and procedures in place in the third State or international organisation concerned;

(c) provide that prior to the exchange of classified information under the agreement, it shall be ascertained that the receiving party is able to protect and safeguard classified information provided to it in an appropriate manner.

3. The Commission shall, when a need to exchange classified information is determined according to Article 51(1), consult the European External Action Service, the General Secretariat of the Council and other Union institutions and bodies, where appropriate, in order to determine whether a recommendation according to Article 218(3) TFEU should be submitted.

4. No EUCI shall be exchanged by electronic means unless explicitly provided for in the security of information agreement or technical implementing arrangements.

5. Within the Commission, the EUCI registry managed by the Secretariat-General shall, as a general rule, be the main point of entry and exit for classified information exchanges with third States and international organisations. However, where on security, organisational or operational grounds it is more appropriate for protecting EUCI, local EUCI registries established within Commission departments in accordance with this Decision and its implementing rules, shall operate as the point of entry and exit for classified information regarding matters within the competence of the Commission departments concerned.

6. In order to assess the effectiveness of the security regulations, structures and procedures in the third State or international organisation concerned, the Commission shall, in collaboration with other Union institutions, agencies or bodies, participate in assessment visits, in mutual agreement with the third State or international organisation concerned. Such assessment visits shall evaluate:

(a) the regulatory framework applicable for protecting classified information;

(b) any specific features of the security policy and the way in which security is organised in the third State or international organisation which may have an impact on the level of classified information that may be exchanged;

(c) the security measures and procedures actually in place; and

(d) security clearance procedures for the level of EUCI to be released.

Article 56

Administrative arrangements

1. Where a long-term need exists in the context of a Union political or legal framework to exchange information classified as a general rule no higher than RESTREINT UE/EU RESTRICTED with a third State or international organisation, and where the Commission Security Authority, after consulting the Commission Security Expert Group, has established, in particular, that the party in question does not have a sufficiently developed security system for it to be possible to enter into a security of information agreement, the Commission may decide to enter into an administrative arrangement with the relevant authorities of the third State or international organisation in question.

2. Such administrative arrangements shall as a general rule take the form of an Exchange of Letters.

3. An assessment visit shall be conducted prior to the conclusion of the arrangement. The Commission Security Expert Group shall be informed of the outcome of the assessment visit. Where there are exceptional reasons for exchanging classified information urgently, EUCI may be released provided every attempt is made to conduct an assessment visit as soon as possible.

4. No EUCI shall be exchanged by electronic means unless explicitly provided for in the administrative arrangement.

Article 57

Exceptional ad hoc release of EUCI

1. Where no security of information agreement or administrative arrangement is in place, and where the Commission or one of its departments determines that there is an exceptional need in the context of an Union political or legal framework to release EUCI to a third State or international organisation, the Commission Security Authority shall, to the extent possible, verify with the security authorities of the third State or international organisation concerned that its security regulations, structures and procedures are such that EUCI released to it will be protected to standards no less stringent than those laid down in this Decision.

2. The decision to release the EUCI to the third State or international organisation concerned, shall, after consultation of the Commission Security Expert Group, be taken by the Commission on the basis of a proposal by the member of the Commission responsible for security matters.

3. Following the Commission's decision to release EUCI and subject to prior written consent of originator, including the originators of source material it may contain, the competent Commission department shall forward the information concerned, which shall bear a releasability marking indicating the third State or international organisation to which it has been released. Prior to or upon actual release, the third party in question shall undertake in writing to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in this Decision.

CHAPTER 8

FINAL PROVISIONS

Article 58

Replacement of previous decision

This Decision shall repeal and replace Commission Decision 2001/844/EC, ECSC, Euratom ([1]).

Article 59

Classified information created before the entry into force of this Decision

1. All EUCI classified in accordance with Decision 2001/844/EC, ECSC, Euratom shall continue to be protected in accordance with the relevant provisions of this Decision.

2. All classified information held by the Commission on the date that Decision 2001/844/EC, ECSC, Euratom entered into force, with the exception of Euratom classified information, shall:

(a) if created by the Commission, continue to be considered to have been reclassified RESTREINT UE by default, unless its author had decided to give it another classification by 31 January 2002 and had informed all addressees of the document concerned;

(b) if created by authors outside the Commission, retain its original classification and thus be treated as EUCI of the equivalent level, unless the author agrees to declassification or downgrading of the information.

Article 60

Implementing rules and security notices

1. As necessary, the adoption of the implementing rules for this decision will be the subject of a separate empowerment decision of the Commission in favour of the Member of the Commission responsible for security matters, in full compliance with the internal rules of procedure.

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

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

Article 61

Entry into force

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

Done at Brussels, 13 March 2015.

For the Commission

The President

Jean-Claude JUNCKER

([1]) Commission Decision 2001/844/EC,ECSC,Euratom of 29 November 2001 amending its internal Rules of Procedure (OJ L 317, 3.12.2001, p. 1).

ANNEX I

EQUIVALENCE OF SECURITY CLASSIFICATIONS

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgium	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	nota (1) below
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	Streng geheim	Geheim	VS (2) — Vertraulich	VS — Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	Secreto	Reservado	Confidencial	Difusión Limitada
France	Très Secret Défense	Secret Défense	Confidentiel Défense	nota (3) below
Croatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	'Szigorúan titkos!'	'Titkos!'	'Bizalmas!'	'Korlátozott terjesztésű!'
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
United Kingdom	UK TOP SECRET	UK SECRET	No equivalent ([5])	UK OFFICIAL — SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([2]) Germany: VS = Verschlusssache.

([3]) France does not use the classification 'RESTREINT' in its national system. France handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([4]) Sweden: the security classification markings in the top row are used by the defence authorities and the markings in the bottom row by other authorities.

([5]) The UK handles and protects EUCI marked CONFIDENTIEL UE/EU CONFIDENTIAL in accordance with the protective security requirements for UK SECRET.

ANNEX II

LIST OF ABBREVIATIONS

Acronym	Meaning
CA	Crypto Authority
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CIS	Communication and Information Systems handling EUCI
DSA	Designated Security Authority
EUCI	EU Classified Information
FSC	Facility Security Clearance
IA	Information Assurance
IAA	Information Assurance Authority
IDS	Intrusion Detection System
IT	Information Technology
LSO	Local Security Officer
NSA	National Security Authority
PSC	Personnel Security Clearance
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
RCO	Registry Control Officer
SAA	Security Accreditation Authority
SAL	Security Aspects Letter
SCG	Security Classification Guide
SecOPs	Security Operating Procedures
TA	TEMPEST Authority
TFEU	Treaty on the Functioning of the EU

ANNEX III

LIST OF NATIONAL SECURITY AUTHORITIES

BELGIUM

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Tel. Secretariat: +32 25014542
Fax +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULGARIA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tel. +359 29333600
Fax +359 29873750
E-mail: dksi@government.bg
Website: www.dksi.bg

CZECH REPUBLIC

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel. +420 257283335
Fax +420 257283110
E-mail: czech.nsa@nbu.cz
Website: www.nbu.cz

DENMARK

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel. +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel. +45 33325566
Fax +45 33931320

GERMANY

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Tel. +49 30186810
Fax +49 30186811441
E-mail: oesIII3@bmi.bund.de

ESTONIA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Tel. +372 7170113 0019, +372 7170117
Fax +372 7170213
E-mail: nsa@mod.gov.ee

GREECE

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Tel. +30 2106572045
+ 30 2106572009
Fax +30 2106536279, +30 2106577612

SPAIN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tel. +34 913725000
Fax +34 913725808
E-mail: nsa-sp@areatec.com

FRANCE

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP
Tel. +33 171758177
Fax + 33 171758200

CROATIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia
Tel. +385 14681222
Fax + 385 14686049
Website: www.uvns.hr

IRELAND

National Security Authority
Department of Foreign Affairs
76 — 78 Harcourt Street
Dublin 2
Tel. +353 14780822
Fax +353 14082959

ITALY

Presidenza del Consiglio dei Ministri
D.I.S. — U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Tel. +39 0661174266
Fax +39 064885273

CYPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Tel. +357 22807569, +357 22807643,
+357 22807764
Fax +357 22302351
E-mail: cynsa@mod.gov.cy

LATVIA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Tel. +371 67025418
Fax +371 67025454
E-mail: ndi@sab.gov.lv

LITHUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)
Gedimino 40/1
LT-01110 Vilnius
Tel. +370 706 66701, +370 706 66702
Fax +370 706 66700
E-mail: nsa@vsd.lt

LUXEMBOURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tel. +352 24782210 central
+ 352 24782253 direct
Fax +352 24782243

HUNGARY

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 (1) 7952303
Fax +36 (1) 7950344

Postal address:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel. +356 21249844
Fax +356 25695321

NETHERLANDS

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Tel. +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tel. +31 703187060
Fax +31 703187522

AUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tel. +43 1531152594
Fax +43 1531152615
E-mail: ISK@bka.gv.at

POLAND

Agencja Bezpieczeństwa Wewnętrznego — ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Tel. +48 22 58 57 944
Fax +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tel. +351 213031710
Fax +351 213031711

ROMANIA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA — ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tel. +40 212245830
Fax +40 212240714
E-mail: nsa.romania@nsa.ro
Website: www.orniss.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Fax +386 14781399
E-mail: gp.uvtp@gov.si

SLOVAKIA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Fax +421 263824005
Website: www.nbusr.sk

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. 16055890
Fax +358 916055140
E-mail: NSA@formin.fi

SWEDEN

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Tel. +46 84051000
Fax +46 87231176
E-mail: ud-nsa@foreign.ministry.se

UNITED KINGDOM

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Fax +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)

Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN