DECISION (EU) 2016/2387 OF THE GENERAL COURT

of 14 September 2016

concerning the security rules applicable to information or material produced in accordance with Article 105(1) or (2) of the Rules of Procedure

THE GENERAL COURT

Having regard to the Rules of Procedure, and in particular Article 105(11) thereof,

Whereas:

(1) In accordance with Article 105(1) and (2) of the Rules of Procedure, a main party to the proceedings may, on his own initiative or following a measure of inquiry ordered by the General Court, produce information or material pertaining to the security of the European Union or to that of one or more of its Member States or to the conduct of their international relations. Article 105(3) to (10) of those Rules lays down the procedural rules applicable to such information or material.

(2) In view of the sensitive, confidential nature of the information or material concerned, the application of the body of rules established by Article 105 of the Rules of Procedure requires a suitable security framework to be set up in order to ensure a high level of protection for that information or material.

(3) To this end, the security framework must be applied to all information or material produced in accordance with Article 105(1) or (2) of the Rules of Procedure if it is European Union classified information or if the main party producing it has indicated that to communicate it to the other main party would harm the security of the Union or of its Member States or the conduct of their international relations, even when that information or material is not European Union classified information.

(4) In order to guarantee a high level of protection for that information or for that material, the fundamental principles and minimum security rules for the protection of that information or material are based on those applicable for the protection of SECRET UE/EU SECRET classified information according to the rules of the EU institutions on the protection of European Union classified information (EUCI), in particular those adopted by the Council of the European Union, the European Parliament and the European Commission.

(5) Information or material produced in accordance with Article 105(1) or (2) of the Rules of Procedure shall be given a mark specific to the Court of Justice of the European Union, called 'FIDUCIA', which is to determine the security rules applicable to it throughout proceedings before the General Court and, in the event of an appeal, before the Court of Justice. The affixing and removing of this marking shall have no consequences for the classification of information communicated to the General Court.

(6) Access to FIDUCIA information shall be provided in accordance with the need-to-know principle,

HAS DECIDED:

Article 1

Definitions

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

(a) 'security authority' means the authority responsible for the security of the Court of Justice of the European Union designated by the latter, which may delegate, in whole or in part, the performance of the tasks provided for by this decision;

(b) 'FIDUCIA office' means the office of the Court of Justice of the European Union responsible for the management of FIDUCIA information;

(c) 'holder' means a duly authorised person who, on the basis of an established need to know, is in possession of FIDUCIA information and who is, in consequence, required to ensure its protection;

(d) 'document' means any information, whatever its physical form or characteristics;

(e) 'information' means any written or oral information, whatever its medium or author;

(f) 'European Union classified information' (EUCI) means any information or any material identified as such according to the security classification of the European Union under the rules applicable in that respect within the EU institutions, covered by one of the following levels of classification:

— TRÈS SECRET UE/EU TOP SECRET;

— SECRET UE/EU SECRET;

— CONFIDENTIEL UE/EU CONFIDENTIAL;

— RESTREINT UE/EU RESTRICTED.

(g) 'FIDUCIA information' means any information bearing the FIDUCIA mark;

(h) 'handling' of FIDUCIA information means all treatment which FIDUCIA information could undergo during the proceedings before the General Court and until, at the latest, the expiry of the period referred to in the first paragraph of Article 56 of the Statute of the Court of Justice of the European Union. Its registration, consultation, creation, copying, storage, return and destruction are accordingly covered.

Article 2

Purpose and scope

1. This decision shall define the fundamental principles and minimum security rules for the protection of FIDUCIA information in proceedings before the General Court and until, at the latest, the expiry of the period referred to in the first paragraph of Article 56 of the Statute of the Court of Justice of the European Union.

2. Those fundamental principles and minimum security rules shall apply to all FIDUCIA information, and to any use of it, written or oral, and to any copies of it that may be made in accordance with the security rules laid down in this decision.

Article 3

Rules governing lodging and return

For the purpose of setting up the security framework provided for by this decision:

— the main party shall inform the General Court Registry of the day on which the information or material is lodged in accordance with Article 105(1) or (2) of the Rules of Procedure;

— the main party, accompanied by a representative of the Registry, shall be required to lodge the information or material provided pursuant to Article 105(1) or (2) of the Rules of Procedure with the FIDUCIA office during the hours the Registry is open to the public;

— the main party producing the information or material in accordance with Article 105(1) or (2) of the Rules of Procedure shall be required to remove it from the FIDUCIA office in the presence of a representative of the Registry if that party does not authorise its disclosure in accordance with Article 105(4) of those Rules, as soon as it is withdrawn in accordance with Article 105(7) of those Rules or as soon as the period referred to in the first paragraph of Article 56 of the Statute of the Court of Justice of the European Union has expired, unless an appeal has been brought within that period;

— if, within the period referred to in the first paragraph of Article 56 of the Statute of the Court of Justice of the European Union, an appeal is brought against the decision of the General Court, the information or material produced in that case in accordance with Article 105(1) or (2) of the Rules of Procedure shall be made available to the Court of Justice. To that end, as soon as the Registrar of the General Court is informed of the existence of that appeal, he shall send a letter to the Registrar of the Court of Justice, informing him of the fact that the information or material concerned is available to the Court of Justice. The Registrar of the General Court shall simultaneously notify the security authority of the fact that the information or material concerned must be made available to the Court of Justice, without that information or material being physically moved. That notification shall be registered by the FIDUCIA office. The main party that produced that information or that material shall be required to remove it from the FIDUCIA office, in the presence of a representative of the Registry of the Court of Justice, as soon as the decision disposing of the appeal has been served, save where the case is referred back to the General Court for a ruling;

— in the event that the case is referred back to the General Court, the Court of Justice shall make the information or material concerned available to the General Court as soon as the decision disposing of the appeal has been served. To that end, the Registrar of the Court of Justice shall send a letter to the Registrar of the General Court informing him of the fact that the information or material concerned is available to the General Court. The Registrar of the Court of Justice shall simultaneously notify the security authority of the fact that the information or material concerned must be made available to the General Court, without that information or material being physically moved. That notification shall be registered by the FIDUCIA office. The main party that produced that information or that material shall be required to remove it from the FIDUCIA office, in the presence of a representative of the Registry of the General Court, as soon as the period referred to in the first paragraph of Article 56 of the Statute of the Court of Justice of the European Union has expired, unless an appeal has been brought within that period.

Article 4

FIDUCIA marking

1. All information or material produced in accordance with Article 105(1) or (2) of the Rules of Procedure shall be given a FIDUCIA mark by the FIDUCIA office.

2. Any information reproducing, in whole or in part, the content of information or material produced in accordance with Article 105(1) or (2) of the Rules of Procedure, and every copy of such information or material, shall likewise be given a FIDUCIA mark by the FIDUCIA office.

3. Documents and registers drawn up by the FIDUCIA office in accordance with this decision whose unauthorised disclosure could harm the security of the Union or that of one or more of its Member States or the conduct of their international relations shall also be given a FIDUCIA mark by the FIDUCIA office.

4. The FIDUCIA mark shall be placed visibly on all FIDUCIA information pages and media.

5. The affixing and removing of the FIDUCIA mark, on the conditions set out in Annex III, shall have no consequences for the classification of information communicated to the General Court.

Article 5

Protection of FIDUCIA information

1. The protection of FIDUCIA information shall be equivalent to that given to SECRET EU/EU SECRET EUCI in accordance with the rules on the protection of EUCI applicable within the EU institutions.

2. The holder of any FIDUCIA information shall be responsible for protecting it in accordance with this decision.

Article 6

Security risk management

1. The risks threatening FIDUCIA information shall be managed as a process of risk analysis aimed at determining known security risks, defining security measures making it possible to reduce those risks to an acceptable level in accordance with the fundamental principles and minimum standards set out in this decision, and applying those measures. The effectiveness of such measures shall be continuously evaluated by the security authority.

2. Security measures for protecting FIDUCIA information throughout the proceedings before the General Court and until, at the latest, the expiry of the period referred to in the first paragraph of Article 56 of the Statute of the Court of Justice of the European Union shall be commensurate with, in particular, the form in which the information or material concerned is presented and its volume, the environment and structure of the FIDUCIA office premises and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.

3. The internal contingency plan of the Court of Justice of the European Union shall take account of the necessity of protecting FIDUCIA information in the event of emergency in order to prevent unauthorised access or disclosure or loss of integrity or availability.

4. Preventative and recovery measures to minimise the impact of major failures or incidents on the handling and storage of FIDUCIA information shall be included in the internal contingency plan of the Court of Justice of the European Union.

Article 7

Personnel security measures

1. Access to FIDUCIA information may be granted only to persons who:

— have a need to know it,

— subject to paragraph 2 of this Article, have been authorised to have access to FIDUCIA information, and

— have been briefed on their responsibilities.

2. The Judges of the General Court shall, by reason of their office, be deemed authorised to have access to FIDUCIA information.

3. The procedure designed to determine whether an official or other servant of the Court of Justice of the European Union, having regard to his loyalty, trustworthiness and reliability, may be authorised to have access to FIDUCIA information is laid down in Annex I.

4. Before being given access to FIDUCIA information and thereafter at regular intervals, all the persons concerned shall be briefed on their responsibilities as regards the protection of FIDUCIA information in accordance with this decision and shall acknowledge their responsibilities in writing.

Article 8

Physical security

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

2. Physical security measures shall be designed to prevent surreptitious or forced entry into the FIDUCIA office premises by an intruder, to deter, impede and detect unauthorised acts and to enable a distinction to be drawn between persons with and without authority to have access to FIDUCIA information in accordance with the need-to-know principle. Such measures shall be determined on the basis of a risk management process.

3. Physical security measures shall be put in place for the FIDUCIA office premises in which FIDUCIA information is handled and stored. These measures shall be designed to ensure protection equivalent to that afforded to SECRET UE/EU SECRET EUCI in accordance with the rules on the protection of EUCI applicable within the EU institutions. No FIDUCIA information may be stored or consulted outside the FIDUCIA office premises created for that purpose within an area that has itself been secured.

4. Only approved equipment or devices in conformity with the rules on the protection of EUCI applicable within the EU institutions shall be used for protecting FIDUCIA information.

5. Provisions for implementing this Article are set out in Annex II.

Article 9

Management of FIDUCIA information

1. 'Management of FIDUCIA information' means the application of administrative measures designed to protect FIDUCIA information throughout the proceedings before the General Court and until, at the latest, the expiry of the period referred to in the first paragraph of Article 56 of the Statute of the Court of Justice of the European Union, and to control it in order to help deter and detect deliberate or accidental compromise or loss of such information.

2. Measures for the management of FIDUCIA information relate to, in particular, the registration, consultation, creation, copying, storage, return and destruction of FIDUCIA information.

3. On reception, and before any handling, FIDUCIA information shall be registered by the FIDUCIA office.

4. The FIDUCIA office premises shall be subject to regular inspection by the security authority.

5. Provisions for implementing this Article are set out in Annex III.

Article 10

Protection of FIDUCIA information handled electronically

1. The communication and information systems (computers and peripheral devices) used in the handling of FIDUCIA information shall be situated in the FIDUCIA office premises. They shall be isolated from any computerised network.

2. Security measures shall be implemented in order to protect the information technology equipment used for the handling of FIDUCIA information against the compromise of that information by unintentional electromagnetic emanations (security measures equivalent to those in place for SECRET UE/EU SECRET EUCI in accordance with the rules on the protection of EUCI applicable within the EU institutions).

3. The communication and information systems shall be subject to accreditation issued by the security authority which shall satisfy itself that they comply with the rules on the protection of EUCI applicable within the EU institutions.

4. Provisions for implementing this Article are set out in Annex IV.

Article 11

Security in the event of external action

1. 'Security in the event of external action' means the application of measures designed to ensure the protection of FIDUCIA information by contractors required to carry out work in connection with the maintenance of communication and information systems isolated from the computerised network or when action has to be taken that entails the urgent removal of FIDUCIA information to a place of safety.

2. The security authority may entrust the performance of tasks involving or entailing, under the contract, access to FIDUCIA information to contractors registered in a Member State.

3. The security authority shall ensure that the minimum security standards laid down in this decision and mentioned in the contract are observed when contracts are granted.

4. Members of a contractor's staff may have access to FIDUCIA information only if they have been authorised for that purpose by the security authority on the basis of personnel security clearance issued by the National Security Authority or any other competent security authority in accordance with national laws and regulations.

5. Provisions for implementing this Article are set out in Annex V.

Article 12

No digital transmission, communication or exchange of FIDUCIA information

1. FIDUCIA information shall in no circumstances be transmitted digitally.

2. The General Court shall not send FIDUCIA information to the institutions, bodies, offices or agencies of the Union, or to the Member States, or to the other parties to the proceedings or to any third party.

Article 13

Breaches of security and compromise of FIDUCIA information

1. A breach of security is an act or omission by an individual that is contrary to the security rules laid down in this decision.

2. Compromise occurs when, as a result of a breach of security, FIDUCIA information has been disclosed in whole or in part to persons who are not, or are not deemed to be, authorised persons.

3. Any breach or suspected breach of security shall be reported forthwith to the security authority.

4. Where it is established, or where there are reasonable grounds to assume, that FIDUCIA information has been compromised or lost, the security authority, liaising closely with the President and the Registrar of the General Court, shall take all appropriate measures in accordance with the applicable provisions in order to:

(a) inform the main party that produced the information or material concerned;

(b) request the competent authority to commence an administrative investigation;

(c) assess the potential damage caused to the security of the Union or to that of one or more of its Member States or to the conduct of their international relations;

(d) prevent any recurrence; and

(e) inform the competent authorities of the steps taken.

5. Any person responsible for a breach of the security rules laid down in this decision shall be liable to disciplinary action in accordance with the applicable provisions. Any person responsible for compromise or loss of FIDUCIA information shall be liable to disciplinary and/or legal action in accordance with the applicable provisions.

Article 14

Organisation of security within the General Court

1. The FIDUCIA office shall put in hand the protection of FIDUCIA information in accordance with this decision.

2. The security authority shall be responsible for the proper application of this decision. For that purpose, the security authority shall:

(a) apply the security policy of the Court of Justice of the European Union and review it at regular intervals;

(b) supervise the implementation of this decision by the FIDUCIA office;

(c) where appropriate, cause an investigation to be carried out, on the conditions laid down in Article 13, of any compromise or loss, or suspected compromise or loss, of FIDUCIA information;

(d) periodically inspect the security arrangements intended to ensure the protection of FIDUCIA information on FIDUCIA office premises.

Article 15

Practice rules for implementation

Practice rules for the implementation of this decision shall be laid down by the security authority in agreement with the Registrar of the General Court.

Article 16

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 Luxembourg, 14 September 2016.

Registrar	*President*
E. COULON	M. JAEGER

ANNEX I

PERSONNEL SECURITY MEASURES

1. This Annex sets out provisions for implementing Article 7 of this decision.

2. The Registrar of the General Court shall be responsible for identifying, so far as concerns him and in so far as strictly necessary, the posts necessitating access to FIDUCIA information and therefore requiring the officials or other servants occupying the posts concerned within the General Court to be authorised to have access to FIDUCIA information.

3. With a view to the grant of authority to have access to FIDUCIA information, the FIDUCIA office shall send the security questionnaire, filled in by the official or other servant concerned, to the National Security Authority of the Member State of which the person concerned is a national or to any other competent national authority, identified in the rules on the protection of EUCI applicable within the EU institutions ('the competent NSA'), and request a security investigation for a SECRET UE/EU SECRET level of classification.

4. At the end of the security investigation, acting in accordance with the laws and regulations in force in the Member State concerned, the competent NSA shall notify the FIDUCIA office of the conclusions of the investigation in question.

5. When the result of the security investigation is that the competent NSA is certain that nothing adverse is known that would call into question the loyalty, trustworthiness or reliability of the person concerned, the competent appointing authority ('the appointing authority') may authorise that person to have access to FIDUCIA information.

6. When the completed security investigation does not lead to the certainty referred to in paragraph 5, the appointing authority shall inform the person concerned. In such a case, the FIDUCIA office, acting on the instructions of the appointing authority, may ask the competent NSA for any further clarification it is in a position to offer in accordance with its national laws and regulations. If the outcome of the security investigation is confirmed, authorisation shall not be granted for access to FIDUCIA information.

7. Authorisation of access to FIDUCIA information shall be valid for a period of five years. It shall be withdrawn when the person concerned leaves the post necessitating access to FIDUCIA information or if the appointing authority considers that there are grounds for withdrawal of authorisation.

8. Authorisation of access to FIDUCIA information may be renewed in accordance with the procedure set out in paragraphs 3 to 5.

9. The FIDUCIA office shall keep a record of authorisations of access to FIDUCIA information.

10. If it is brought to the FIDUCIA office's knowledge that a risk to security is posed by a person holding authorisation for access to FIDUCIA information, the FIDUCIA office shall give notice of this to the competent NSA and the appointing authority may suspend access to FIDUCIA information or withdraw the authorisation of access to that information.

11. In an emergency, the appointing authority may, after consulting the competent NSA and subject to the results of preliminary checks to ascertain that no adverse information is known, grant temporary authorisation of access to FIDUCIA information to the officials and other servants concerned. Such temporary authorisation shall be valid until the end of the procedure referred to in paragraphs 3 to 5, but may not, however, exceed a period of six months from the date on which the request for a security investigation is made to the competent NSA.

12. Before being granted access to FIDUCIA information, the persons holding that authorisation shall follow a training programme in order to enable them to discharge their responsibility for handling FIDUCIA information. Authorisation of access to FIDUCIA information shall not become effective until that training has been completed and responsibility has been acknowledged in writing.

ANNEX II

PHYSICAL SECURITY

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 8 of the decision. It lays down minimum requirements for the physical protection of the FIDUCIA office premises in which FIDUCIA information is handled and stored.

2. Physical security measures shall be designed to prevent unauthorised access to FIDUCIA information by:

   (a) ensuring that FIDUCIA information is properly handled and stored;

   (b) enabling a distinction to be drawn between persons with and without authorisation to have access to FIDUCIA information, in accordance with the need-to-know principle;

   (c) deterrence, by preventing and detecting unauthorised acts; and

   (d) preventing or delaying surreptitious or forced entry into the FIDUCIA office premises.

3. Physical security measures shall be chosen in the light of an appraisal of the threats posed to FIDUCIA information. These measures shall take into consideration the environment and structure of the FIDUCIA office premises. The security authority shall determine the degree of security to be attained for every one of the following physical measures:

   (a) a perimeter barrier defending the boundaries of the area to be protected;

   (b) an intrusion detection system connected to the security command post of the Court of Justice of the European Union;

   (c) an access control system exercised by electronic or electro-mechanical means, and operated by a member of the security staff;

   (d) security staff trained, supervised and holding authorisation to have access to FIDUCIA information;

   (e) closed-circuit video-surveillance system operated by security staff and connected to the intrusion detection and access control systems;

   (f) security lighting allowing effective surveillance directly, or indirectly through a video-surveillance system;

   (g) any other appropriate physical measures designed to deter unauthorised access or to detect it, or to prevent consultation or loss of, or damage to, FIDUCIA information.

II. PREMISES IN WHICH FIDUCIA INFORMATION IS STORED AND CONSULTED

Creation of physically protected premises for storage and consultation

4. Secured premises shall be created for the purpose of storage and consulting FIDUCIA information. FIDUCIA information may be stored and consulted only in FIDUCIA office premises which comply in all respects with the rules on the protection of EUCI applicable within the EU institutions.

5. Within those premises, FIDUCIA information shall be kept in security containers also complying in all respects with the rules on the protection of EUCI applicable within the EU institutions.

6. No communications system (telephone or other electronic device) may be brought into the FIDUCIA office premises.

7. The FIDUCIA office meeting room shall be protected against eavesdropping. Electronic security inspections of them shall be carried out at regular intervals.

Access to storage and consultation premises

8. Access to the FIDUCIA office premises shall be controlled by an identification security door under video surveillance.

9. Persons who have been authorised to have access to FIDUCIA information and persons deemed to be so authorised may gain access to the FIDUCIA office premises in order to consult FIDUCIA information on the conditions laid down in Article 7(1) and (2) of this decision.

10. The security authority may in exceptional cases issue access authorisation to persons without FIDUCIA authorisation if it is essential that they should enter the FIDUCIA office premises, provided that access to those premises does not involve access to FIDUCIA information which is to remain protected from sight in security containers. Those persons may gain access only if they are accompanied, and continuously watched, by a member of the FIDUCIA office with authorisation for access to FIDUCIA information.

11. All access to FIDUCIA office premises shall be recorded in an access logbook. This logbook shall be kept at a work station in those premises. The communication and information system used for this purpose shall be compatible with the security requirements laid down in Article 10 of, and Annex IV to, this decision.

12. The protection measures governing the written use of FIDUCIA information shall apply in the case of oral use of that information.

III. CONTROL OF KEYS AND COMBINATIONS USED TO PROTECT FIDUCIA INFORMATION

13. The security authority shall define procedures for managing keys and combination settings for the FIDUCIA office premises and security containers. Such procedures shall protect against unauthorised access.

14. Combination settings shall be committed to memory by the smallest possible number of persons needing to know them. Combination settings for security containers storing FIDUCIA information shall be changed;

(a) on receipt of a new container;

(b) when there is a change in personnel knowing the combination;

(c) when compromise has occurred or is suspected;

(d) when a lock has undergone maintenance or repair;

(e) at least every 12 months.

15. Technical equipment intended for the physical protection of FIDUCIA information shall comply with the rules on the protection of EUCI applicable within the EU institutions. The security authority shall be responsible for the observance of these rules.

16. Technical equipment shall be periodically inspected and maintained at regular intervals. Maintenance shall take account of the inspection results in order that the best possible operation of the equipment may be guaranteed.

17. At every inspection the efficiency of the various security measures and of the security system as a whole is to be reappraised.

ANNEX III

MANAGEMENT OF FIDUCIA INFORMATION

I. INTRODUCTION

1. This Annex sets out provisions for implementing Article 9 of the decision. It lays down the administrative measures designed to protect FIDUCIA information throughout the proceedings before the General Court and until, at the latest, the expiry of the period referred to in the first paragraph of Article 56 of the Statute of the Court of Justice of the European Union, and to control it in order to help deter and detect deliberate or accidental compromise or loss of such information.

II. REGISTER OF FIDUCIA INFORMATION

2. A register of FIDUCIA information shall be created. This register shall be kept, by the FIDUCIA office, at a work station situated in the FIDUCIA office premises. The communication and information system used to keep this register shall be compatible with the security requirements laid down in Article 10 of, and Annex IV to, this decision.

III. REGISTRATION OF FIDUCIA INFORMATION

3. For the purposes of this decision, registration for security purposes ('registration') means the application of procedures keeping track of the life-cycle of FIDUCIA information, including its destruction.

4. Registration of FIDUCIA information shall be the responsibility of the FIDUCIA office.

5. The FIDUCIA office shall automatically give a FIDUCIA mark to information or material produced in accordance with Article 105(1) or (2) of the Rules of Procedure. The FIDUCIA office shall register FIDUCIA information in the FIDUCIA information register.

6. The FIDUCIA office shall draw up a report annexed to the FIDUCIA information register, specifying the circumstances in which information is received. The information shall then be handled according to the rules laid down in the previous paragraph.

7. FIDUCIA information shall be registered, in accordance with paragraphs 5 and 6 above, in the FIDUCIA information register without prejudice to the procedural registration performed by persons within the Registry authorised to have access to FIDUCIA information.

IV. MANAGEMENT OF FIDUCIA INFORMATION

Marking

8. When EUCI or any other information, in respect of which it has been indicated that its communication would harm the security of the Union or that of one or more of its Member States or the conduct of their international relations, is produced under Article 105(1) or (2) of the Rules of Procedure, it shall be given the FIDUCIA mark by the FIDUCIA office.

9. The FIDUCIA mark shall be clearly and correctly indicated in every part of the document, irrespective of the form in which the information is presented, whether the format is paper, audio, electronic or other.

Creation of FIDUCIA information

10. Only a person authorised to have access to FIDUCIA information or a person deemed to be so authorised may create FIDUCIA information, as specified in Article 4(2) to (3) of this decision.

11. All FIDUCIA information created shall be registered by the FIDUCIA office in the FIDUCIA information register.

12. All FIDUCIA information created shall be subject to all the rules on the handling of FIDUCIA information as laid down in this decision and in the annexes thereto.

Removal of the FIDUCIA mark

13. FIDUCIA information shall lose its mark in two cases:

(a) when the main party that produced the FIDUCIA information authorises its communication to the other main party, the information originally communicated and all information created on the basis thereof shall lose its FIDUCIA mark;

(b) when FIDUCIA information is returned to the main party that produced it.

14. The FIDUCIA office shall remove the FIDUCIA mark and record that removal in the FIDUCIA information register.

15. Removal of the FIDUCIA mark shall not mean that EUCI has been declassified.

V. COPIES OF FIDUCIA INFORMATION

16. FIDUCIA information shall not be copied unless this is essential. In that case, copies shall be made by the FIDUCIA office which shall number and register them.

17. Copies shall be subject to all the security rules laid down in this decision and in the annexes thereto.

VI. DESTRUCTION OF FIDUCIA INFORMATION

18. When information or material produced in accordance with Article 105(1) or (2) of the Rules of Procedure is returned to the main party that produced it, all information reproducing, in whole or in part, the content of that information or material, and any copies made, shall be destroyed.

19. The destruction of FIDUCIA information referred to in paragraph 18 shall be carried out by the FIDUCIA office, using methods complying with the rules on the protection of EUCI applicable within the EU institutions, in order to prevent that information being reconstructed in whole or in part.

20. The destruction of FIDUCIA information referred to in paragraph 18 shall be performed in the presence of a witness authorised to have access to FIDUCIA information.

21. The FIDUCIA office shall draw up a destruction certificate.

22. The destruction certificate shall be annexed to the FIDUCIA information register. A copy shall be sent to the main party that produced the document concerned.

ANNEX IV

PROTECTION OF FIDUCIA INFORMATION HANDLED ELECTRONICALLY

1. This Annex sets out provisions for implementing Article 10.

2. FIDUCIA information may be handled only on electronic equipment (work stations, printers, photocopiers) that is not connected to the computerised network and is placed in the FIDUCIA office premises.

3. All electronic equipment used in the handling of FIDUCIA information shall comply with the rules on the protection of EUCI applicable within the EU institutions. The security of this equipment shall be ensured throughout its life-cycle.

4. All possible connections to the internet and to other tools (LAN, WLAN, Bluetooth etc.) shall be permanently deactivated.

5. Work stations shall be equipped with appropriate anti-virus protection. Anti-virus updates shall be performed using a dedicated CD-ROM or USB stick.

6. The memories of printers and photocopiers shall be erased before any maintenance operation.

7. Only cryptographic products approved in accordance with the rules on the protection of EUCI applicable within the EU institutions shall be used to handle the requests for investigations referred to in Annex I.

ANNEX V

SECURITY IN THE EVENT OF EXTERNAL ACTION

1. This Annex sets out provisions for implementing Article 11.

2. Contractors may gain access to FIDUCIA information only in connection with the maintenance of the communication and information systems isolated from the computerised network or when action has to be taken that entails the urgent removal of FIDUCIA information to a place of safety.

3. The security authority shall draw up guidelines for external action covering, in particular, security clearances for the contractors' staff, and also the content of the contracts referred to in this Annex.

4. Documents relating to the tendering procedures and maintenance contracts for the communication and information systems isolated from the computerised network shall be given the FIDUCIA mark when they contain information whose unauthorised disclosure could harm the security of the Union or that of one or more of its Member States or the conduct of their international relations. The security aspects letter annexed to the contract shall contain provisions requiring the contractor to comply with the minimum standards laid down in this decision. Failure to comply with those minimum standards may constitute sufficient grounds for termination of the contract.

5. The contract involving action having to be taken that entails the urgent removal of FIDUCIA information to a place of safety shall include the number of security guards who are to have personnel security clearance. It shall be silent with regard to the procedures to be put in hand. This contract shall not be given the FIDUCIA mark.

6. The contractor may not sub-contract the activities defined in the call for tenders and in the contract involving or entailing access to FIDUCIA information.