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

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

E. COULON

President

M. JAEGER