PRESIDENT'S DECISION No. 40

of 27 August 2013

Regarding Data Protection at the European University Institute

(EUI Data Protection Policy)

THE PRESIDENT OF THE EUROPEAN UNIVERSITY INSTITUTE,

Having regard to the Convention setting up a European University Institute, and in particular Article 7 thereof,

Having regard to the Protocol on the Privileges and Immunities of the European University Institute,

Having regard to the Headquarters Agreement between the Government of the Italian Republic and the European University Institute, and in particular Article 3 thereof,

Having regard to the Directive 95/46/EC 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,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data,

Having regard to the 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,

Having regard to the relevant European Conventions and EU legislation

After consulting the Data Protection Committee,

Whereas,

The current Decision No 32 of the President of 27 November 2008 regarding Data Protection at the European University Institute needs to be revised in order to be even more aligned with European legislation and practices of the European Union Institutions,

It is necessary to update the current Data Protection Policy in order to make it better respond to recent trends and developments both in the legislative as well as in the ICT fields,

A fully-fledged system of protection of personal data requires the establishment of rights for data subjects and obligations for those who process personal data,

A sound Data Protection Policy is necessary to provide the individual with legally enforceable rights, to specify the data processing obligations of the controllers within the EUI and to better define the role and function of the advisory Data Protection Committee,

HAS DECIDED AS FOLLOWS:

I. GENERAL PROVISIONS

Article 1

Purpose & Scope

1. This Decision has the purpose to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data by the EUI.

2. It applies to the processing of personal data by the EUI and by processors acting on behalf of the EUI, which are carried out in the exercise of the Institute's activities wholly or partially by automated means, or in the context of a filing system.

Article 2

Definitions

1. For the purposes of this Decision:

a) "Personal data" means any information relating to an identified or identifiable natural person hereinafter referred to as 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

b) "Processing of personal data" hereinafter referred to as 'processing' means any operation or set of operations which is performed upon personal data, whether or not

by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

c) "Controller" is the EUI or the Service or Unit of Department or any other organisational entity who alone or jointly with others determines the purposes and means of the processing of personal data on behalf of the EUI. In practise, this means that the Controller can be the Secretary General or the Director of Service /Head of the Unit or Department of the EUI;

d) "Processor" means a natural or legal person within the EUI structure who processes personal data on behalf of the Controller;

"External processor" is a natural or legal person, public authority, agency or any other body (e.g. organisational entity of an event, Settlements Office of the Joint Sickness Insurance Scheme) which is external to the EUI and processes personal data on behalf of the EUI;

e) "The data subject's consent" means any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

Article 3

Purposes of processing operations

1. Personal data can be processed by the EUI only for institutional purposes. These include educational activities, administrative and accounting activities, activities of academic and scientific research, safety and security purposes, and any other activities pertaining to the functioning and operations of the EUI both internally as well as with external partners.

2. The EUI shall not store or process data for commercial purposes, and in particular shall not mail commercial advertising material or perform any market research.

Article 4

Principles relating to data processing

1. Personal data shall be:

a) processed fairly and lawfully;

b) collected for specified, explicit and legitimate institutional purposes, and not further processed in a way incompatible with those purposes;

c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Decision.

II. CRITERIA FOR LEGITIMATE DATA PROCESSING

Article 5

Lawfulness of processing

1. Personal data may be processed only if

   a) the data subject has unambiguously given his or her consent or

   b) processing is necessary to

      i. perform an institutional task of the EUI or a task carried out in the public interest on the basis of the EUI Convention or other legal and regulatory instruments adopted on the basis thereof or in the legitimate exercise of official authority in the EUI or body or in a third party to whom the data are disclosed,

      ii. comply with a legal obligation to which the Controller is a subject,

      iii. perform a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract, or

      iv. protect the vital interests of the data subject or of a third party.

2. Without prejudice to Article 4, 5 and 7, personal data collected exclusively for ensuring the security or the control of the processing systems or operations shall not be used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences.

Article 6

Data retention

1. Personal data shall be stored for no longer than it is required for the processing purposes for which it was collected.

2. However, administrative data concerning researchers, fellows, and members of the staff may be retained by the EUI as long as it is needed for institutional purposes. The administrative data retained beyond the completion of the specific purpose for which they were collected but they have to be maintained for the purposes of proof will be deleted if the data subject objects to their retention.

3. Data retention and disposal at the EUI shall be managed by the Records Management service (RAME) under the provisions of Presidential Decision 12/2002. Retention schedules shall be indicated on the EUI website at

http://www.eui.eu/ServicesAndAdmin/RAME/ClassificationSchemesUsed.aspx

Article 7

Processing of special categories of data

1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, is prohibited.

2. Paragraph 1 does not apply where:

a) the data subject has given his or her explicit consent to the processing of those data,

b) processing is necessary for complying with the specific rights and obligations of the Controller in the field of employment law,

c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent,

d) processing relates to data which are manifestly made public by the data subject or are necessary for the establishment, exercise or defence of legal claims,

e) processing is carried out in the course of the legitimate activities with appropriate safeguards by a non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of this body or to persons who have regular

contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects,

f) processing of the data is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, on condition that these data are processed by a health professional subject to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

3. Processing of data relating to offences, criminal convictions or security measures may be carried out only if authorized by the EUI Convention or other legal and regulatory instruments adopted on the basis thereof or, by a President's reasoned Decision after notification to the Data Protection Officer and if necessary, also to the Data Protection Committee, subject to appropriate specific safeguards.

Article 8

Processing of data logs, e-mails and traffic data

1. Internet navigation logs and data pertaining to the video footage recorded in the video surveillance system of the EUI may be collected only for security purposes or administrative inquiries and/or disciplinary proceedings.

The identification of the user connected to a log entry may only be provided subject to the prior-authorization of the Secretary General after consulting the Data Protection Officer and if necessary, also the Data Protection Committee, on the basis of an administrative inquiry and/or disciplinary action by the EUI or upon a request by a judicial or a law-enforcement authority.

However, the log data concerning access to electronic resources that are licensed to the EUI may be used to identify users who have violated the terms of use for such electronic resources upon request by the competent Controller.

2. Identification-card logs may be collected only for security purposes. However, identification-card logs of the staff may also be used for registering working times.

3. Data pertaining to phone traffic may be collected only for billing purposes.

Article 9

Individual e-mails accounts

1. Institutional e-mail accounts assigned to individuals may be accessed only when needed for security purposes or administrative inquiries and/or disciplinary proceedings or when required by judicial authorities. Access requires the prior authorization of the Secretary General of the EUI, after consulting the Data Protection Officer and if necessary, also the Data Protection Committee.

2. Exceptionally, when the interests of the service so require and the holder of an individual email account is permanently unable to access the account, due to circumstances such as serious illness, forced absence or death, the Secretary General may nominate a trusted member of the Institute for accessing the account. A copy of the nomination indicating also the nature of information required as well as the purpose of such access will be sent to the Data Protection Officer and if necessary, also to the Data Protection Committee and to the absent staff member (or his/her heirs).

Access to the information required will be performed in the presence of the Data Protection Officer. The information may be copied in electronic means.

The responsible for the account shall forward professional emails to a member of the Institute designated by the Secretary General. After the information has been retrieved, the Secretary General shall notify the absent staff member (with a copy to the Data Protection Officer) indicating the date, time and purpose of the access, as well as the information consulted and/or retrieved.

Article 10

Confidentiality & Security

1. A person employed within the EUI or contracted by the EUI and acting as processor on behalf of the Institute, and who has access to personal data, shall be bound by the duty of confidentiality and shall not process them except on instructions from the controller, unless required to do so by national, Community or international law.

2. Having regard to the state of the art and the cost of their implementation, the security of personal data shall be safeguarded through adequate technical and organizational measures, according to the EUI's Data Security Policy.

The purpose will be to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be processed.

Such measures shall be taken in particular to prevent any unauthorized disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.

3. Where personal data are processed by automated means, measures shall be taken as far as possible and as appropriate in view of the risks in particular with the aim of:

(a) preventing any unauthorised person from gaining access to computer systems processing personal data;

(b) preventing any unauthorised reading, copying, alteration or removal of storage media;

(c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;

(d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities;

(e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers;

(f) recording which personal data have been communicated, at what times and to whom;

(g) ensuring that it will subsequently be possible to check which personal data have been processed, at what times and by whom;

(h) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting Institute;

(i) ensuring that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation;

(j) designing the organisational structure within the Institute in such a way that it will meet the special requirements of data protection.

4. Data subjects shall be informed about security risks and any security breaches potentially concerning their data shall be communicated to them.

III. RIGHTS OF DATA SUBJECTS

Article 11

Information to Data Subjects

1. The Controller shall provide the data subject from whom data relating to himself/herself are collected with information about:

- the identity of the Controller,
- the legal basis of the processing operation,
- the purpose of the processing,
- the time-limits for storing the data,
- the recipients of the data,
- the rights as listed in art. 12, and
- any further information in so far as such information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing.

2. When data is to be provided by the data subject, the Controller shall specify what pieces of data are optional, and what the consequences of not providing them are.

3. If the data has not been provided by the data subject, the Controller shall at the time of undertaking the recording of personal data or, if disclosure to a third party is envisaged, no

later than the time when the data are first disclosed, provide the data subject with at least the information under paragraph 1 above where he or she already has it. Any further information provided to the data subject can also refer to the origin of the data, except where the controller cannot disclose this information for reasons of professional secrecy.

4. Paragraph 1, 2, and 3 do not apply when providing the data subject with the information would be impossible, would require a disproportionate effort, or would be contrary to established academic practices.

Article 12

Individual rights

1. Data subjects have the following rights:

a) to obtain a confirmation whether or not their data are processed, and information on the categories of data that are being processed, in what ways, and for what purposes as well as the recipients or categories of recipients to whom the data are disclosed

b) to obtain communication of their personal data undergoing processing and of any available information as to their source,

c)to knowledge of the logic involved in any automated decision process concerning him or her

d) to the rectification of inaccurate or incomplete personal data,

e) to the erasure of data of which processing by the EUI is unlawful,

f) to block the processing of data of which they contest the accuracy, until accuracy is checked.

2. Requests concerning the rights in this Article can be addressed to the Controller who shall reply within 30 working days.

IV. TRANSFER OF PERSONAL DATA AND SPECIAL PROCESSING OPERATIONS BY THE EUI

Article 13

Transfer of personal data to third parties

1. Subject to the requirements of paragraph 2, personal data may be transferred between the EUI and third parties, such as member states, public authorities, institutions and companies only for institutional purposes, and only when all parties of the transfer have in

place adequate safeguards for the protection of privacy compatible with Directive 95/46/EC".

2. Personal data may be transferred to recipients subject to national law adopted for the implementation of Directive 95/46/EC by a President's reasoned Decision after notification to the Data Protection Officer and if necessary, also to the Data Protection Committee, subject to appropriate specific safeguards

a) as long as the data are necessary for the legitimate performance of tasks covered by the competence of the recipient and

b) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority or

c) if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.

Article 14

Processing by the Historical Archives of the European Union (HAEU)

1. The Historical Archives of the European Union (HAEU) protects personal data in its archival collections - Archival Holdings of EU Institutions, private archival deposits, and Historical Archives of the European University Institute - according to the following provisions:

a) concerning the Archival Holdings of EU Institutions, the HAEU acts as data processor for the depositing EU Institutions and applies data protection in accordance with the control mechanisms of the depositing Institutions and complying with Council Regulation No. 354/83 as subsequently amended, concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community , and with EC Regulation No. 45/2001;

b) concerning the private archival deposits, the HAEU acts as data processor for the depositing organisation or individual and applies data protection according to provisions in the respective deposit agreement and in line with the present Presidential Decision;

c) concerning the Historical Archives of the European University Institute, the HAEU acts as data processor for the European University Institute and applies data protection according to the present Presidential Decision.

2. i) The documents in private archival collections deposited at the HAEU shall be made accessible to the public by decision of the Director of the archives, with authorization of the depositing institution or individual. However, the Director of the archives may exclude or limit access to those documents or to parts of them when necessary to protect overriding interests of data subjects or of institutions that are originators of the documents. Any

person having been refused access to a document on data protection grounds may address a confirmatory application to the Secretary General of the EUI asking the Institute to reconsider its position.

ii) Within 30 days from receipt of the confirmatory application, the Institute shall either grant access to the document requested or, in a written reply, state the reasons for the total or partial refusal. In the event of a confirmation of the total or partial refusal, the applicant may make a complaint to the Data Protection Committee as described under Article 24.

Article 15

Processing for research purposes

1. Personal data collected by the EUI for research purposes can be processed only for the scientific objectives for which they were collected.

2 Such data may be publicly disclosed only if:

a) the data subject has given consent or

b) the publication of personal data is necessary to present research findings or to facilitate research; or

c)the data subject has made the data public.

3. Distribution shall be excluded or limited when this is required by overriding interests or fundamental rights of the data subject.

V. THE GOVERNANCE OF DATA PROTECTION

Article 16

General overview of governance structure

1. The Secretary General has overall responsibility for the implementation of the Data Protection Policy, including the appointment of controllers, in accordance with Article 17.

2. Controllers have responsibility, in accordance with Articles 17 and 18, for the fair and lawful processing of the data under their control and the notification of any processing operation to the Data Protection Officer and if necessary also, to the Data Protection Committee.

3. The Processor shall process personal data on behalf of the controller and shall act only on instructions of the controller.

4. The Data Protection Officer (DPO) shall ensure in an independent way in accordance with Article 19 respect for data protection principles within the Institute. In addition to an advisory function, the main tasks of the DPO will consist in the provision of information and raising awareness, monitoring of compliance and assisting in the handling of complaints and queries and related investigation functions.

5. The Data Protection Committee (DPC) monitors the application of the provisions of this Decision and any related data protection policy instruments and provides advice or makes recommendations for improvement of the Institute's Data Protection Policy, in accordance with Article 23. It can also review complaints submitted to the Controller regarding a breach of data protection principles, in accordance with Article 24.

Article 17

Tasks and responsibilities of the Secretary General and of Controllers

1. The Secretary General shall be overall responsible for the general implementation of the Institute's activity in the field of Data Protection under the President's guidance. The Secretary General may, after consulting the Data Protection Committee and notifying the DPO, issue guidelines and operational policy-related instruments for the implementation of the EUI's Data Protection policy. The Secretary General appoints the Controllers.

2. The Controller determines the purpose and means of the processing of personal data and must ensure that personal data is processed fairly and lawfully in compliance with the EUI Data Protection Policy.

Controllers shall have -amongst others- the following responsibilities:

- manage data protection inside their respective Units and shall implement data quality requirements in accordance with the principles set out under Article 4 of the present Decision;

- give prior notification to the Data Protection Officer of any new processing, unless a processing only consists of operations pertaining to usual administrative and/or academic practices, such as the organisation of conferences or the processing and assessment of scientific works;

- identify the persons in charge of each processing ("processors") and shall notify them as to the scope of the processing operations they are permitted to accomplish;

- inform and allow the Data Subjects to exercise their rights;

- implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. Such measures shall be taken to prevent any unauthorised disclosure or access, accidental or unlawful destruction, accidental loss or alteration and to prevent all other unlawful forms of processing.

The Data Controller remains responsible even where the personal data are processed by an external processor.

Article 18

Processing of personal data on behalf of controllers

1. The carrying out of a processing operation by way of an external processor shall be governed by a binding contract or legal act stipulating in particular that:

a) the processor shall act only on instructions from the controller; and

b) the processor shall comply with the data protection rules of this Decision;

c) the processor shall ensure confidentiality and security according to the EUI's Data Security Policy.

2. The parts of the contract or the legal act relating to data protection and the requirements relating to confidentiality and security measures shall be in writing or in another equivalent form.

3. Resort to an external processor shall be allowed only on the condition that the processor provides sufficient guarantees in respect of technical and organizational security measures and ensures compliance with those measures.

Article 19

The Data Protection Officer (DPO)

1. The Data Protection Officer shall ensure that the provisions of this Decision are applied and that Controllers and data subjects are informed of their rights and obligations pursuant to this Decision.

That person shall thus ensure that the rights and freedoms of the data subject are unlikely to be adversely affected by the processing operations.

The DPO may be consulted by the EUI, a controller, the Staff Committee or any individual on any matter concerning the interpretation or application of the present Decision. The DPO may advise, on request or on his/her own initiative, the EUI and the controllers on the application of data protection provisions. The DPO may also make recommendations for the practical improvement of data protection at the EUI.

2. The DPO may be asked to provide advice, or may spontaneously provide advice, in various contexts. The most common instances where the DPO will give advice are when the EUI:

- Considers any new information systems or processing operations;
- Prepares notifications;

- Prepares replies to requests from data subjects for access, rectification, blocking, or erasure;
- Prepares replies to complaints from data subjects and to requests from staff within the meaning of Article 1 of the Common Provisions for teaching and administrative staff of the Institute if they are linked to DP issues;
- Prepares any rules having impact on DP;
- Discusses any legal, practical or technical issues having impact on DP

Advice may be given orally or in writing, as appropriate.

3. The DPO shall provide the President and the Secretary General with a yearly report on the status of Data protection compliance at the EUI. An intermediate report in the middle of the year may also be provided if requested by the EUI or if the DPO deems it appropriate.

4. The DPO shall maintain a Data Protection Registry, which identifies and describes all processing operations communicated to the DPO by the Controllers. Upon requests from the data subjects, the DPO shall provide them with the information in the Registry concerning processing of their data.

5. Upon requests by the data subjects, the DPO shall ensure that they obtain from the controller confirmation and any applicable related information as to whether or not their personal data undergoing are being processed.

6. The DPO may perform investigations concerning compliance with the present Decision.

7. The DPO shall distribute information and promote awareness on data protection and data security.

Article 20

Appointment of the DPO

1. The DPO is appointed by the President, for a period of between two and five years, being selected on the basis of personal and professional qualities and, in particular, expert knowledge of data protection.

2. With respect to the performances of his/her duties, the DPO is independent and may not receive any instructions.

Article 21

The Data Protection Committee (DPC)

1. The Data Protection Committee (DPC) includes the following members:

a) The Internal Auditor;

b) A Professor from the Law Department nominated for a period of 3 years by the Executive Committee upon the proposal of the Head of the Law Department;

c) The Dean of Graduate Studies;

d) A member of staff nominated by the Staff Committee for a period of 3 years;

e) A researcher nominated by the Researcher Representatives for a period of 2 years.

f) A staff member with knowledge of data protection.

2. An alternate member is designated for each full member. The alternate of the Internal Auditor is the Director of the Historical Archives of the European Union; the alternate of the Dean of Graduate Studies is a departmental Director of Graduate Studies, to be nominated by the Executive Committee for a period of three years. Alternates may take part in the work of the DPC.

3. The members of the DPC nominate its President.

4. The members of the DPC, together with their alternates, perform their duties in complete independence. They do not receive any instructions as to the performance of their duties. They respect the secrecy of the information that comes to their knowledge in the course of their work for the DPC.

5. The President of the DPC may invite the DPO and/or the Legal Advisor as well as a staff member with relevant technological expertise to participate in the meetings of the DPC.

Article 22

Voting rules of the DPC

1. The DPC takes its decisions by a simple majority of the votes casts, not including abstentions. However, the favourable vote of at least one third of the members of the DPC having the right to vote is required.

2. Alternates may vote in substitution of the corresponding members when the latter are unable to attend.

Article 23

Tasks of the DPC

1. The DPC monitors the application of the provisions of this Decision and of any other legal or regulatory act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by the EUI, and advises the EUI and data subjects on all matters concerning the processing of personal data.

The DPC may either on request by the EUI or on its own initiative make recommendations for improvement and implementation of the Institute's Data Protection Policy.

2. The DPC reviews complaints by data subjects as described under Article 24 below.

3. On the request of the President, the Secretary General or the DPO, the DPC may investigate specific instances of data processing and give opinions on all questions concerning implementation of the present Decision.

4. The DPC adopts its internal rules of procedure.

Article 24

Data protection complaints

1. Data subjects may address complaints to the Controller with simultaneous notification to the DPO regarding a breach of data protection principles. The Controller shall respond within 30 days and take action if needed.

2. In case the data subject is not satisfied with the response to the complaint or he or she obtains no timely response, the data subject may refer the complaint to the DPC.

3. The DPC shall make a reasoned recommendation within 90 days on the actions to be taken with respect to the complaint.

4. Where the DPC takes the view that an investigation of a complaint is necessary which would involve hearings of the parties, witnesses or experts, or the carrying out an immediate verification of the processing operations in question, it should notify the President and may request an Administrative Inquiry to be carried out.

I. FINAL PROVISIONS

Article 25

Derogations

1. Derogations from the provisions of this Decision may be made in exceptional cases, for meeting overriding institutional needs of the EUI, having regard to the interests and fundamental rights of the data subjects.

2. Such a derogation can be adopted by the President following a justified request by the Secretary General, after having obtained the favourable opinion of the DPO and if necessary also of the DPC. It shall be made known to all concerned data subjects.

Article 26

Sanctions

Any failure to comply with the obligations pursuant to this Decision, whether intentionally or through negligence on his or her part, renders the staff member concerned liable to

disciplinary action, in accordance with the rules and procedures laid down in the Staff Regulations or in the conditions of employment applicable to other servants.

Article 27

Final measures

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

2. This Decision shall replace the President's Decision 32/2008 regarding Data Protection at the EUI.

3. This Decision shall be published on the EUI's Intranet and Internet sites. It shall be forwarded to the High Council and notified to all Directors of Service and Heads of Departments and Units, without delay.

Done at Florence, on 27 August 2013

The President,

(signed)

Marise CREMONA

ANNEX I

The role of the Data Protection Officer in ensuring compliance with the present Decision

1. The Data Protection Officer may make recommendations for the practical improvement of data protection policy to the EUI and advise the Institute and the controller concerned on matters concerning the application of data protection provisions. Furthermore he or she may, on his or her own initiative or at the request of the EUI, the controller, the Staff Committee concerned or any individual, investigate matters and occurrences directly relating to his or her tasks and which come to his or her notice, and report back to the person who commissioned the investigation or to the controller.

2. The Data Protection Officer may be consulted by the EUI, by any controller or processor, by the Staff Committee and directly by any individual, on any matter concerning the interpretation or application of this Regulation.

3. No one shall suffer prejudice for bringing to the attention of the competent Data Protection Officer a matter alleging that a breach of the provisions of this Decision has taken place.

4. Every controller and processor shall be required to assist the Data Protection Officer in performing his or her duties and to give information in reply to questions in compliance with this Decision. In performing his or her duties, the Data Protection Officer shall have access at all times to the data forming the subject-matter of processing operations and to all offices, data-processing installations and data carriers.

5. To the extent required and as far as possible given the structure of the EUI, the Data Protection Officer shall be relieved of other activities. The Data Protection Officer and his or her staff shall be required not to divulge information or documents which they obtain in the course of their duties.

6. Without prejudice to the specific provisions of this Decision and of its accompanying Annex I, the DPO of the EUI shall be inspired in the conduct of his tasks and duties by the *EDPS position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001* as well as by the document prepared by the Network of Data Protection Officers of the EU institutions and bodies titled: *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001*available under:

http://ec.europa.eu/anti_fraud/documents/data-protection/dpo/edps_dpo_paper_en.pdf

and

http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf