PRESIDENT'S DECISION No 11/2014

of 13 February 2014

adopting implementing rules concerning the Data Protection Officer on the basis of the President's Decision No 40/2013 regarding Data Protection at the European University Institute (EUI Data Protection Policy)

The President of the European University Institute (EUI),

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

Having regard to President's Decision No 40/2013 of 27 August 2013 regarding Data Protection at the European University Institute (EUI Data Protection Policy) and its accompanying Annex I,

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, and in particular Article 24(8) and the Annex thereof,

Having regard to 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 Commission's Decision 2008/597/EC of 3 June 2008 adopting implementing rules concerning the Data Protection Officer pursuant to Article 24(8) of Regulation (EC) No 45/2001,

Having regard to EUI President's Decision No 67 of 16 December 2013 appointing a Data Protection Officer (DPO) at the EUI from 1 January 2014,

After consulting the EUI's Data Protection Committee,

Whereas:

(1) EUI President's Decision No 40/2013, sets out the EUI's Data Protection Policy and provides for the appointment of a Data Protection Officer.

(2) By analogy to Regulation 45/2001 and the relevant practises of the EU institutions and bodies, further implementing rules concerning the Data Protection Officer are deemed necessary to be adopted by the EUI, taking into account the provisions of the EUI's Decision 40/2013 and its accompanying Annex I. The implementing rules shall in particular concern the tasks, duties and powers of the Data Protection Officer and shall specify the modalities of co-operation between the DPO and the actors involved in the governance of data protection (including the Data Protection Committee).

HAS DECIDED AS FOLLOWS:

SECTION 1

GENERAL PROVISIONS

Article 1
Definitions

For the purpose of the present Decision the definitions provided for by the EUI's Decision 40/2013 shall apply. In particular:

- "Controller", as defined in Article 2(c) of Decision 40/2013 and for the purpose of the present decision, shall mean the Head of the EUI's organisational entity who alone or jointly with others has determined the purposes and means of the processing of personal data by the EUI. This refers in practise to the Secretary General or to the appointed by him Director of Service or Head of Department, Unit, Programme or Centre of the EUI.
- "Processor", as defined in Article 2(d) of Decision 40/2013 and for the purposes of the present decision, shall mean a natural or legal person within the EUI structure responsible for processing personal data on behalf of the Controller.

Article 2
Scope

The present Decision defines the rules and procedures for implementation of the function of Data Protection Officer (hereinafter referred to as the "DPO") within the European University Institute (hereinafter referred to as the "EUI"). It also sets out the modalities of co-operation between the DPO and the actors involved in the governance of data protection (including the Data Protection Committee).

SECTION 2

THE DATA PROTECTION OFFICER

Article 3
Appointment and Status

1. The President of the EUI shall appoint the DPO.
2. The term of office of the DPO shall be between two and five years, renewable once.
3. The DPO shall act in an independent manner with regard to the internal application of the provisions of Decision 40/2013 and may not receive any instructions with respect to the performance of his duties.
4. The DPO shall be selected on the basis of personal and professional qualities and, in particular, expert knowledge of data protection. In addition to the requirements of Decision 40/2013, the DPO should also have a sound knowledge of the EUI's structure and administrative rules and procedures. It is desirable to have a good knowledge of information systems, principles and methodologies. The DPO must have the capacity to demonstrate sound judgement and the ability to maintain impartial and objective stance in accordance with the EUI's Staff Regulations.

5. The selection of the DPO shall not be liable to result in a conflict of interests between his or her duty as DPO and any other official duties, in particular to the application of the provisions of Decision 40/2013.

6. Without prejudice to the provisions of Decision 40/2013 concerning his or her independence and obligations, the DPO shall report directly to the Secretary General of the EUI who according to Article 17 of the same Decision is overall responsible for the general implementation of the Institute's activity in the field of Data Protection under the President's guidance. This reporting obligation shall be taken into account in the context of the performance appraisal of the staff member appointed as DPO, for which the Secretary General shall ensure equal and fair treatment.

7. The EUI will provide the DPO as far as possible and taking into account the available resources, with the staff and resources necessary to carry out his or her duties.

8. The DPO shall not suffer any prejudice on account of the performance of his or her duties.

9. The DPO may be dismissed from his post by the President upon a proposal from the Secretary General having obtained the consent of the Data Protection Committee (DPC), if he no longer fulfils the conditions required for the performance of his duties.

10. Without prejudice to the relevant provisions of Decision 40/2013, the DPO shall be subject to the rules and regulations applicable to the administrative staff members of the EUI.

Article 4
Tasks and Duties

Without prejudice to the tasks as described in Decision 40/2013 and in its Annex I, the DPO shall contribute to creating a culture of protection of personal data within the EUI by raising general awareness of data protection issues while maintaining a just balance between the principles of protection of personal data and transparency.

The DPO shall also perform the following tasks and accomplish the following duties:

1. Give advice to the President and the Secretary General of the EUI and the Controllers on matters concerning the application of data protection provisions in the EUI, either on request, or on his own initiative.

2. Be consulted by the President or the Secretary General of the EUI, any of the Controllers concerned, the Staff Committee or any individual on any matter concerning the interpretation or application of Decision 40/2013.

3. Investigate -either on his own initiative or on the request of the President or the Secretary General of the EUI, a Controller or any individual concerned- matters and occurrences directly related to DPO tasks and duties and report back to the person who commissioned the investigation, in accordance with the procedure described in Article 11 hereof.

4. Maintain an inventory ("Data Protection Registry") of all processing operations on personal data of the EUI into which the Controllers introduce their respective processing operations.

5. Help the Controllers to assess the risks of the processing operations under their responsibility.
6. Prior-check with the DPC if any processing operation is likely to present any specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes as the ones described in Article 10 of this Decision.
7. Respond to the requests of the DPC and work together with the DPC on the subject of data protection either on his own initiative or on the request of the DPC.
8. Submit each year a "Data Protection Status Report" for the EUI to the President and the Secretary General. The report shall be made available to the EUI's administrative and teaching staff as well as to the EUI's researchers through the internal website of the Institute.
9. Cooperate with the DPOs of other institutions and bodies of the European Union or other international organisations in particular by exchanging experience and sharing know-how and participating in the dedicated networks of DPOs.
10. Represent the EUI on any data protection issue, upon request by the Secretary General or the President, and without prejudice to the independence of the DPO.

Article 5
Powers

In performing his tasks and duties and without prejudice to the powers conferred by Decision 40/2013, the DPO may:

1. Make recommendations to the President of the EUI or to the Controllers on the issues concerning the practical improvement of the data protection policy at the EUI.
2. Bring to the attention of the Secretary General and to the President any failure of a staff member or controller to comply with the obligations of Decision 40/2013 and suggest that an administrative investigation be launched with a view to possible application of Article 26 of Decision 40/2013.
3. Handle queries and complaints, in compliance with Decision 40/2013.
4. Have access at all times, in the performance of his or her duties, to the data forming the subject matter of processing operations on personal data and to all offices, data-processing installations and data carriers.
5. Have access to necessary training with regard to the legal and technical aspects of data protection.
6. Regularly attend the meetings with the DPOs of other institutions and bodies of the European Union or other international organisations if such possibility arises.

SECTION 3

RULES AND PROCEDURES

Article 6
Controllers

1. Without prejudice to the provisions of Decision 40/2013 concerning their obligations, Controllers shall:

   a) Ensure that all processing operations involving personal data within their area(s) of responsibility comply with the EUI's Data Protection Policy;

   b) Prepare without delay notifications to the DPO for all existing processing operations which have not yet been notified, using the relevant notification forms. The form shall be printed, signed by the controller and submitted to the DPO. The notification shall contain all information required by Article 9 of the present Decision;

   c) Notify the DPO in due time about processing operations which are likely to present specific risks under Article 10 of the present Decision bearing in mind that the prior checking procedure with the DPO and the DPC if appropriate, can last up to two months and the operation cannot be implemented before the DPO and DPC if appropriate, have communicated their opinion;

   d) Immediately inform the DPO about any change affecting the information referred to in paragraphs (b) and (c);

   e) In relation to processing operations and inquiries or investigations conducted by the DPO, answer the request of the DPO for information and grant him access to the relevant personal data within 5 working days of receipt of such request;

   f) Where appropriate, consult the DPO on the conformity of processing operations, in particular in the event of doubt as to conformity.

2. A Controller may delegate certain parts of his or her tasks to other persons acting as a Delegated Controllers under the Controller's authority and responsibility.

Article 7
Processors

1. Processors within the EUI, required to process personal data on behalf of Controllers, shall act only on the Controllers' instructions and process such personal data in strict compliance with Decision 40/2013, and any other applicable legislation and implementing provisions on data protection.

2. Formal contracts shall be concluded with external processors; such contracts shall contain the specific requirements mentioned in Article 18 of Decision 40/2013.

Article 8
Rights of data subjects

1. The Data Protection Registry kept by the DPO pursuant to Article 19 of Decision 40/2013 shall serve as an index of all processing operations relating to personal data in the EUI. The register shall be accessible through the internal website of the EUI and in paper format. Data subjects may make use of the information contained in the register to exercise their rights under Articles 11 and 12 of Decision 40/2013.
2. Data subjects will be informed by the Controllers about their rights, in particular as specified in Article 11 and Article 12 of Decision 40/2013.
3. Further to their right to be appropriately informed about any processing of their personal data, data subjects may approach the relevant Controller to exercise their rights pursuant to Decision 40/2013, as specified below:
    a) These rights may only be exercised by the data subject or their duly authorised representative. Such persons may exercise any of these rights free of charge.
    b) Requests to exercise these rights shall be addressed in writing to the relevant controller. The Controller shall only consider the request if the requester's identity and, if relevant, their entitlement to represent the data subject have been appropriately verified. The controller shall without delay and in any case within 30 working days from receipt of the request, inform the data subject in writing of whether or not the request has been accepted. If the request has been rejected, the controller shall include the grounds for the rejection.
    c) The controller shall, by paying due attention to the urgency of the request, grant access pursuant to Article 12 of Decision 40/2013 by enabling the data subject to consult the data on-site or to receive a copy thereof, according to the applicant's preference.
    d) Data subjects may contact the DPO in the event that the Controller does not respect the relevant time limit for paragraphs (b). In the event of obvious abuse by a data subject in exercising his rights, the Controller may refer the data subject to the DPO. If the case is referred to the DPO, the DPO will decide on the merits of the request and the appropriate follow-up. In the event of disagreement between the data subject and the Controller, both parties shall have the right to consult the DPO.
4. The data subjects shall notify the DPO at the moment of lodging a complaint with the Controller pursuant to Article 24 of Decision 40/2013.

Article 9

Notification to the DPO

1. The Controller shall give prior notice to the DPO of any processing operation or set of such operations intended to serve a single purpose or several related purposes.
2. The information to be given shall include:

a) the name and address of the Controller and an indication of the organisational parts of the EUI or external organisation or body entrusted with the processing of personal data for a particular purpose;

b) the purpose or purposes of the processing;

c) a description of the category or categories of data subjects and of the data or categories of data relating to them;

d) the legal basis of the processing operation for which the data are intended;

e) the recipients or categories of recipient to whom the data might be disclosed;

f) a general indication of the time limits for blocking and erasure of the different categories of data;

g) proposed transfers of data to third countries or international organisations, if applicable;

h) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 10 of Decision 40/2013 to ensure security of processing.

3. Any change affecting information referred to in paragraph 2 shall be notified promptly to the DPO.

Article 10

Prior-checking by the Data Protection Committee

1. Processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes shall be subject to prior checking by the Data Protection Committee. In case of doubt as to the need for prior checking, the DPO shall consult the DPC.
2. The following processing operations are likely to present such risks:

    a) processing of data relating to health and to suspected offences, offences, criminal convictions or security measures;

    b) processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct;

    c) processing operations allowing linkages not provided for pursuant to the EUI regulatory framework between data processed for different purposes;

    d) processing operations for the purpose of excluding individuals from a right, benefit or contract.

3. The prior checks shall be carried out by the DPC following receipt of a notification from the DPO.
4. The DPC shall deliver his or her opinion within two months following receipt of the notification. This period may be suspended until the DPC has obtained any further information that may have requested. When the complexity of the matter so requires, this

period may also be extended for a further two months, by decision of the DPC. This decision shall be notified to the Controller prior to expiry of the initial two-month period.

If the opinion has not been delivered by the end of the two-month period, or any extension thereof, it shall be deemed to be favourable.

If the opinion of the DPC is that the notified processing may involve a breach of any provision of Decision 40/2013, the DPC shall where appropriate make proposals to avoid such breach.

5. The DPC shall keep a register of all processing operations that have been notified to it pursuant to this article. The register shall be open to public inspection.
6. EUI processing operations which fall under a similar framework to that of the EU institutions or bodies and have been notified and prior-checked by the European Data Protection Supervisor (EDPS), will not have to be prior-checked by the DPC. The DPO shall be able to base his/her assessment on the opinion delivered by the EDPS.
7. Without prejudice to the regulatory framework of Decision 40/2013, the DPO and the DPC will take into account also the opinions, recommendations and working papers of the Working Party on the Protection of Individuals with regard to the processing of personal data set up under Art.29 of Directive 95/46/EC (Art.29 Working Party).

Article 11

Investigation Procedure

1. The requests for an investigation mentioned in Article 4(3) hereof shall be addressed to the DPO in writing. Within 15 working days upon receipt, the DPO shall send an acknowledgment of receipt to the person who commissioned the investigation, and verify whether the request is to be treated as confidential. In the event of obvious misuse of the right to request an investigation, the DPO shall not be obliged to report back to the requester.
2. The DPO shall request a written statement on the matter from the Controller who is responsible for the data-processing operation in question. The Controller shall provide his response to the DPO within 15 working days. The DPO may wish to receive complementary information from him and/or other parties within 15 days.
3. The DPO shall report back to the person who commissioned the investigation no later than three months following its receipt. This period may be suspended until the DPO has obtained any further information that he or she may have requested.
4. If the requester of the investigation is an individual, or if the requester acts on behalf of an individual, the DPO must, to the extent possible, ensure confidentiality governing the request, unless the data subject concerned gives his/her unambiguous consent for the request to be handled otherwise.
5. No one shall suffer prejudice on account of a matter brought to the attention of the DPO alleging a breach of the provisions of Decision 40/2013.

SECTION 4

FINAL PROVISIONS

Article 12
Entry into Force

This Decision enters into force on the date of its adoption.

Done at Florence, 13 February 2014

The President,

(signed)

Joseph H.H. WEILER