

Declaration of confidentiality

Administrative and Teaching staff as well as trainees are bound by professional secrecy and confidentiality concerning information and personal data on the EUI, its staff members, researchers and external parties they obtain directly or indirectly during their engagement with the EUI or in connection with it.

I, the undersigned: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, personnel number **\_\_\_\_\_\_\_\_\_\_\_\_**, having the status of **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** confirm that I remain bound by the obligations incumbent upon administrative/teaching staff/trainees and in particular the duty of integrity and discretion. Therefore I will refrain from any use or disclosure of confidential information obtained during my engagement at the EUI or in connection with it. I will also fully respect the obligations of protection of personal data as provided for by the applicable rules on data protection at the EUI.

Date: Signature:

**ANNEX**

**Abstracts from EUI’s President’s Decision No.40 of 27 August 2013**

**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.

**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 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.

**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.

**Abstracts from the Service Rules of Administrative Staff applicable to Permanent Staff Members and Conditions of Employment of Other Servants of the European University Institute (EUI)**

*Article 17*

1. A staff member shall refrain from any unauthorised disclosure of information received in the line of duty, unless that information has already been made public or is accessible to the public.

2. A staff member shall continue to be bound by this obligation after leaving the service.

**Abstracts from the Conditions of Employment of Teaching Staff of the European University Institute (EUI)**

*Article 2*

1. A full-time contract holder,…., shall carry out his duties and conduct himself solely with the interests of the Institute in mind. He shall abstain from any action or behaviour which may reflect adversely upon his position or affect his ability to perform his duties

**Abstracts from President’s Decision No. 39 of 27 August 2013 laying down the provisions governing traineeships at the European University Institute**

***Rights and Duties of trainees***

*Article 8*

4. Trainees shall observe the traineeship programme and rules and the EUI’s in-house working rules, especially those on security and confidentiality. They shall also comply with the data protection rules currently in force at the EUI.