PRESIDENT DECISION No. 10/2019
of 18 February 2019

Regarding Data Protection
at the European University Institute (EUI)

THE PRESIDENT OF THE EUI,

having regard to the Convention setting up a EUI, and in particular Article 7 thereof,

having regard to the Protocol on the Privileges and Immunities of the EUI,

having regard to the Headquarters Agreement between the Government of the Italian Republic and the EUI, and in particular Article 3 thereof,

having regard to Regulation (EU) No 1725/2018 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC,

having regard to the Regulation (EU) No 679/2016 (General Data Protection Regulation) and, in particular to its Article 45 providing for its 'soft enforcement' by means of requiring 'adequate safeguards' for transfer of data, carried out by the EUI,

after consulting the Data Protection Committee,

whereas,

an effective system of protection of personal data requires in particular the establishment of rights for data subjects and obligations for those who process personal data,

a sound data protection policy provides the individual with legally enforceable rights, specifies the data processing obligations of Controllers within the EUI and better defines the role and function of the Data Protection Officer,

President's Decision No 40 of 27 August 2013 regarding data protection at the EUI and President's Decision No 11 of 13 February 2014 adopting implementing rules concerning the Data Protection Officer need to be revised in order to ensure adequacy with EU rules on data protection.

Therefore, the current revision improves, in particular, the following aspects of data protection:

- legal remedies in case of infringements of data subjects' rights;
- rules and technical measures for data security and security breaches;
- definition and protection of sensitive personal data in case of transfers to third parties.

HAS DECIDED AS FOLLOWS:

I. GENERAL PROVISIONS

Article 1

Purpose & scope

1. This Decision aims at protecting the fundamental right of protection of personal data of natural persons with respect to the processing of personal data by the EUI.

2. It applies to all processing operations of personal data by the EUI and by Processors acting on behalf of the EUI, which are carried out in the exercise of the EUI's activities whether wholly or partially by automated means, or in any other manner.

Article 2

Definitions

1. For the purposes of this Decision:

    a) "Personal data" means any information relating to identified or identifiable natural persons ('data subjects'); "identifiable persons" can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity;

    b) "Sensitive data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health and data relating to sexual orientation or activity;

    c) "Processing of personal data" ('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, transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

    d) "Controller" is the EUI as such or one of its organisational entities who determine the purposes and means of the processing of personal data.

    e) "Processor" means a natural or legal person who processes personal data on behalf of the Controller;

    f) "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) external to the EUI and processes personal data for the EUI or on behalf of the EUI;

    g) "The data subjects' consent" means any freely given, specific, informed and unambiguous indication of agreement to personal data being processed.

h) “Personal data breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data transmitted, stored or otherwise processed.

Article 3

Purposes of processing operations

Personal data can be processed by the EUI only for institutional purposes, as defined by the EUI Convention or other legal instruments adopted on the basis thereof, such as 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.

Article 4

Principles relating to data processing

1. Personal data are:

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

b) processed fairly and lawfully;

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

d) accurate and 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 were collected or for which they are further processed;

f) processed in line with data subjects’ rights, including the right to be forgotten, as referred to in Article 16 below;

g) processed under the responsibility and liability of the Controller, who ensures and demonstrates for each processing operation 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) data subjects have given their consent, or

    b) processing is necessary to

        i. perform an institutional task of the EUI or other tasks carried out in the public interest on the basis of the EUI Convention or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority of the 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 Articles 4, 5 and 8, personal data collected exclusively for ensuring the security or the control of the processing systems or operations are not used for any other purpose, with the exception of the prevention, investigation, detection and prosecution of serious criminal offences.

Article 6

Conditions for consent

1. Where processing is based on consent, the Controller shall be able to demonstrate that the data subjects have consented to the processing of their personal data.

2. When the processing has multiple purposes, informed and specific consent must be given for each of them.

3. Data subjects have the right to withdraw the consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, data subjects shall be informed of this consequence.

Article 7

Data retention for administrative purposes

1. Administrative data concerning researchers, fellows, and members of the staff may be retained by the EUI only as long as required for institutional purposes.

2. Data retention and disposal at the EUI shall be managed by the Records Management service (RAME) under the provisions of President's Decision No. 12/2002. Retention schedules shall be indicated on the EUI website.

Article 8

Processing of sensitive data

1. Processing of sensitive data, as defined in Article 2 b), is prohibited.

2. Paragraph 1 does not apply where:

    a) data subjects have given their 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 data subjects are physically or legally incapable of giving their consent;

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

    e) processing of the data is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of care or treatment or the management of health-care services, pursuant to contract with a health professional subject to the obligation of professional secrecy.

3. Processing of data relating to criminal convictions may be carried out only if expressly authorised by regulatory measures adopted by the competent EUI authorities. Those measures shall contain appropriate specific safeguards and must be notified to the Data Protection Officer.

Article 9

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, administrative inquiries, or disciplinary proceedings.

2. The identification of the user connected to a log entry may only be provided in case of an administrative inquiry or disciplinary action by the EUI or upon a motivated request by a judicial or a law-enforcement authority. The identification of the user is subject to the prior-authorisation of the Secretary General after consulting the Data Protection Officer and, if deemed necessary, the Data Protection Committee.

3. 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.

4. 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.

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

Article 10

Individual e-mail accounts

1. Institutional e-mail accounts assigned to individuals may be accessed only when needed for security purposes, administrative inquiries, or disciplinary proceedings or following a motivated request by judicial authorities. Access requires the prior authorisation of the Secretary General, after consulting the Data Protection Officer.

   Content of folders and individual e-mails labelled clearly as private can be accessed only with the express and unambiguous consent of the holders of the accounts or of their heirs, or if the conditions of Article 5(1) b) ii) or iv) are fulfilled.

2. If holders of individual e-mail accounts or their heirs are permanently unable to access the account and to give consent, the Secretary General may exceptionally nominate a trusted member of the EUI to access the e-mail account if required by the interests of the EUI. A copy of the nomination indicating the nature of information required and the purpose of such access is sent to the Data Protection Officer and to the staff members concerned or, alternatively, their heirs.

   Access to the information required will be performed in the presence of the Data Protection Officer. The information may be copied on electronic storage medium as far as required by the interests of the service.

   The responsible for the account shall forward professional e-mails to a member of the EUI designated by the Secretary General. After the information has been retrieved, the Secretary General shall notify the staff members concerned or their heirs (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 11

Security of processing

1. The security of personal data shall be safeguarded through adequate technical and organisational measures according to the EUI's Data Security Policy, such as pseudonymisation or encryption of personal data.

   The level of security is appropriate to the risks represented by the processing and the nature of the personal data concerned.

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

2. Where personal data are processed by automated means, measures are taken with the aim of:

   a) preventing any unauthorised person from gaining access to systems processing personal data and from any processing of data;

   a) ensuring that authorised users of a data-processing system can only access personal data covered by their access rights;

   b) recording which personal data have been processed, when and by whom;

c) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the EUI;

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

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

3. Data subjects shall be informed in a timely manner about security risks and any security breaches potentially affecting them.

Article 12

Confidentiality of processing

Persons employed or contracted by the EUI, who act as Processors on behalf of the EUI, shall process personal data, and in particular sensitive data, only on instructions from the Controller and in full compliance with EUI's data protection policy. Processors are bound by the duty of confidentiality.

Article 13

Notification of a personal data breach

1. The Controller shall notify any personal data breach to the EUI's Data Protection Officer, no later than 72 hours after having become aware of it. Any delays must be motivated.

2. The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach.

3. The notification shall at least:

a) state the nature and likely consequences of the personal data breach, as well as, the categories and approximate number of data subjects and personal data records concerned;

b) explain the remedial actions taken and, where appropriate, measures to mitigate the effects of the personal data breach.

4. In duly justified cases, the information may be provided in phases without delay.

5. The Controller shall document in detail any personal data breaches, comprising at least the facts relating to the breach, its effects and the remedial actions taken.

Article 14

Communication of a personal data breach to the data subject

1. The Controller shall communicate the personal data breach to the data subjects concerned without undue delay.

2. The communication to the data subjects shall:

a) state the nature and likely consequences of the personal data breach;

b) explain the remedial actions taken and, where appropriate, measures to mitigate the effects of the personal data breach;

c) provide the name and contact details of the EUI's Data Protection Officer.

3. The communication to the data subject is not required if:

a) the controller has implemented appropriate technical and organizational measures to the personal data affected by the security breach;

b) the controller has taken effective remedial actions;

c) it would involve disproportionate effort. In such a case, the communication is made through an equally effective manner, such as a public communication.

III. RIGHTS OF DATA SUBJECTS

Article 15

Information provided to data subjects

1. Controllers provide the data subjects with any information necessary for effectively exercising their rights under this Decision, such as:

a) the identity and the contact details of the Controller and the DPO;

b) the legal basis for the processing operation;

c) the purpose of the processing;

d) the time-limits for storing the data;

e) where applicable, the fact that the Controller intends to transfer personal data to a third party and the reference to the appropriate safeguards as stated in Article 17 below;

f) the possibility to ask for review according to Article 27.

2. If data subjects provide data themselves, the Controller specifies which data are optional and the consequences of not providing them.

3. If data are provided by third persons or institutions, the Controller provides the data subject with the information mentioned in paragraph 1 of this Article. This information must be provided when the personal data are collected or, if disclosure to a third party is envisaged, no later than the data are first disclosed. Any further information provided to the data subject has to respect professional secrecy.

Article 16

Individual rights

1. Data subjects enjoy the following rights concerning their personal data:

    a) to be informed whether, how, by whom and for which purpose they are processed;

    b) to ask for their rectification, in case they are inaccurate or incomplete;

    c) to demand their erasure in case the processing is unlawful or no longer lawful ('right to be forgotten');

    d) to block their further processing whilst the conditions under letters b) and c) of this Article are verified.

2. Requests under this Article are addressed to the Controller who shall reply within 30 working days.

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

Article 17

Transfer of personal data to third parties

1. Personal data may be transferred between the EUI and third parties including Contracting States, only for institutional purposes, and only when all parties of the transfer have in place adequate safeguards for the protection of personal data. Transfers are allowed under the following conditions:

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

    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 18

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 EUI - according to the following provisions:

    a) concerning the Archival Holdings of EU Institutions, the HAEU acts as 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 Regulation (EU) 1725/2018;

b) concerning the private archival deposits, the HAEU acts as 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 EUI, the HAEU acts as Processor for the EUI and applies data protection according to the present Decision.

2. The HAEU provides appropriate safeguards, including technical and organisational measures, for the rights and freedoms of the data subjects, listed under Article 16 of this Decision. The HAEU may provide derogations from the rights, subject to the safeguards, when such rights are likely to render impossible or seriously impair the achievement of the specific purposes of the HAEU.

3. 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, following an authorisation by 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 the 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 EUI to reconsider its position.

   Within 30 working days from receipt of the confirmatory application, the EUI 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 according to Article 27 of this Decision.

Article 19

Processing for research purposes

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

2. Such data may be publicly disclosed only if:

   a) the data subjects have given their consent according to Article 6, or

   b) the data subjects have made the data public.

3. Distribution shall be excluded or limited when this is required by data subjects' interests.

V. GOVERNANCE OF DATA PROTECTION AT THE EUI

Article 20

General overview of governance structure

1. The Secretary General is overall responsible for the implementation of the EUI's data protection policy.

2. Controllers are responsible, for fair and lawful processing of the data under their control. The Controllers can seek the DPO's advice on all questions related to their tasks.

3. Processors process personal data on instructions from the Controller.

4. The Data Protection Officer (DPO) ensures respect for data protection principles within the EUI. For this purpose, the DPO advises the senior management of the EUI and the Controllers and is responsible for providing information, raising awareness, monitoring compliance and assisting in the handling of complaints in the field of data protection. The DPO enjoys full independence in the exercise of those tasks.

5. The Data Protection Committee (DPC) assists, on its own initiative or upon request, the President, the Secretary General and the DPO in fundamental issues related to EUI's data protection policy.

Article 21

Tasks, responsibilities and liabilities of the Secretary General and of Controllers

1. The Secretary General shall be overall responsible for the general implementation of the EUI's activity in the field of data protection under the President's guidance. The Secretary General can nominate the Controllers in the EUI's organisational entities.

2. Controllers determine the purpose and means of the processing of personal data.

   Controllers shall have in particular the following responsibilities:

   a) manage data protection inside their respective organisational units and implement the requirements in accordance with the principles set out in sections I, II, III and IV of the present Decision;

   b) identify the Processors and notify them of the scope of the processing operations they are permitted to accomplish;

   c) implement appropriate technical and organisational measures to ensure, verify and demonstrate compliance. Controllers keep a record of processing activities under their responsibility;

   d) 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 processed. Such measures shall be taken to prevent any personal data breach. Controllers give the Processors instructions for the notification of security breaches, in accordance with Article 13 of this Decision;

   e) carry out privacy impact assessments;

f) review personal data complaints in cooperation with the Data Protection Officer, according to Article 27 below.

3. Controllers maintain those responsibilities in cases of external processing.

4. Controllers are liable towards the EUI and towards the data subjects for breaches of their responsibilities.

5. Controllers may delegate certain tasks to Delegated Controllers. Delegated Controllers act under the Controller's authority and responsibility.

Article 22

External processing of personal data on behalf of Controllers

1. The carrying out of a processing operation by an external Processor shall be governed by a contract or another binding legal act (see Annex I to this Decision) stipulating in writing that the Processor:

a) processes the data only on instructions from the Controller;

b) respects the data protection rules of this Decision;

c) has committed to confidentiality and security according to the EUI's data security policy;

d) provides adequate technical and organisational security measures.

Article 23

The Data Protection Officer

1. The Data Protection Officer (DPO) ensures respect for the provisions of this Decision.

The DPO can be either a staff member or work based on a service contract.

The DPO may fulfil other tasks and duties, provided these do not result in a conflict of interest.

The DPO is appointed by the President, after consultation of the Secretary General, 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.

The DPO's mandate can be renewed by the President.

The DPO's mandate may be withdrawn by the President after consultation of the Data Protection Committee.

2. The DPO's duties are executed in an independent manner and without receiving any instructions.

3. The DPO may be consulted by the EUI management, the Controllers and the Staff Committee on matters concerning the interpretation or application of the present Decision. The DPO shall advise on the application of data protection provisions. The

DPO shall also make recommendations for the practical improvement of all aspects of data protection at the EUI.

4. The DPO presents a yearly report on the status of data protection at the EUI and an intermediate report if deemed necessary.

5. Upon request by data subjects, the DPO may ask the Controller for any relevant information on the processing of the personal data.

   Controllers and Processors shall assist in the performance of the DPO's duties.

6. The DPO may perform assessments concerning compliance with the EUI's data protection policy. The President and the Secretary General shall ensure the follow-up on the findings of those assessments. Upon authorization granted by the President, the DPO can address compliance problems by means of an investigation. In performing such investigations, the DPO can access the relevant data, verify the corresponding processing operations and all offices, data-processing installations and data carriers.

7. The DPO distributes information and promotes awareness on data protection and data security, in close cooperation with the Controllers and the Data Security Officer.

8. The DPO and the DPO's staff shall not divulge information or documents obtained in the course of their duties.

Article 24

The Data Protection Committee

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 three 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 three years;

   e) a researcher nominated by the Researcher Representatives for a period of two 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 25

Tasks of the DPC

1. The DPC assists the President, the Secretary General and the Data Protection Officer in fundamental issues concerning compliance of the processing of personal data by the EUI with the present Decision.

2. The DPC adopts its internal rules of procedure.

Article 26

Voting rules of the DPC

1. The DPC takes its decisions by a simple majority of the votes cast, 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.

VI. REMEDIES

Article 27

Review procedures

1. Data subjects may request the Controller to review acts or omissions infringing their rights under the EUI's data protection rules. Such requests for review have to be made in writing within 15 working days either after the alleged violation occurred or after the data subject could have obtained knowledge thereof. They should be sent simultaneously to the EUI's Data Protection Officer (DPO).

2. The Controller replies to the request for review within one month. The reply takes into account the position expressed by the DPO. The Controller has to motivate the rejection of a request for review and of a substantial deviation from the advice received by the DPO. The absence of a reply within one month constitutes an implied rejection.

3. Data subjects may submit a motivated written complaint to the President against the Controller's rejection decision. The motivated complaint must be lodged within three months either after receipt of the express rejection or, in case of an implied rejection, the expiry of the deadline of one month.

   The President consults the DPO before replying to a complaint. The President's motivated decision is communicated to the data subject within two months from the

date on which the complaint was received. The absence of a reply within this deadline constitutes an implied rejection.

4. Data subjects may apply to the Organ of First Instance for judicial review of the rejection of their complaint. Such applications must be lodged within three months either after the express rejection of the complaint or the expiry of the deadline of two months for the reply in case of an implied rejection.

   The Organ of First Instance can confirm, annul or reverse the decision taken by the President.

Article 28

Sanctions

Any failure to comply with the obligations pursuant to this Decision, whether intentionally or through negligence, renders the members of the EUI community concerned liable to disciplinary action, in accordance with the rules and procedures laid down in the Staff Regulations, the conditions of employment applicable to other servants, the conditions of employment for teaching staff (CETS), the rules adopted on the basis thereof and the EUI's disciplinary regulation.

VII. FINAL PROVISIONS

Article 29

Derogations

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

2. The President, following a motivated request by the Secretary General and after having obtained the favourable opinion of the DPO, can adopt such derogations. It shall be made known to all concerned data subjects.

Article 30

Entry into force and publication

1. This Decision enters into force on the day of its adoption. It replaces President Decision 40/2013 regarding data protection at the EUI and President Decision 11/2014 adopting implementing rules concerning the Data Protection Officer.

2. This Decision will be published on the EUI's Intranet. It will also be communicated to the High Council and to all Data Controllers at the EUI.

Done at Florence, on 18 February 2019

The President,

(signed)

Renaud Dehousse

ANNEX

Implementing Article 22 concerning external processing of personal data on behalf of Controllers

1. The Controller must ensure that external processors implement appropriate technical and organisational measures for the protection of the rights of the data subjects in compliance with EUI rules on data protection.

2. A contract or another binding legal act must govern the processing by an external processor.

   The contract or other legal act must set out in writing:

   i) subject-matter and duration of the processing;

   ii) nature and purpose of the processing;

   iii) type of personal data and categories of data subjects;

   iv) obligations and rights of the controller.

3. The contract or other legal act must stipulate that the processor:

   a) processes the personal data only on documented instructions from the controller;

   b) is committed to confidentiality or are under an appropriate statutory obligation of confidentiality;

   c) deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies;

   d) makes available to the controller all information necessary to demonstrate compliance with the obligations and contributes to audits.

4. The processor shall not engage another processor without prior specific or general written authorisation of the controller, the same data protection obligations apply as between the controller and the processor. A contract or other legal act must impose those obligations on that other processor. The initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. When a processor is not a Union institution or body, its adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate sufficient guarantees.

6. The contract or the other legal act referred to in this Annex may be based, on standard contractual clauses laid down by the European Commission or the European Data Protection Supervisor.

7. If a processor exceeds the instructions as defined under paragraph 3(a), the processor shall be considered to be a controller in respect of that processing for all purposes of the EUI’s data protection policy.