European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing	Traineeships
Created on	11/09/2018
Last update	
Reference number	002
Year	2018
1. Controller:	European Economic and Social Committee
2.a) Service responsible	E1 FOR
2b) contact details	EESC-trainee@eesc.europa.eu
3. Joint controller	Not applicable
4. DPO: contact details	data.protection@eesc.europa.eu
5. Processor(s) (where applicable)	Not applicable
6. Purpose(s) of the data processing	Processing of traineeship applications The processing of personal data aims at managing the traineeships applications administratively (confirming receipt of the application, informing applicants of the outcome of their application, etc.) and at facilitating the internal selection procedure of the trainees recruited by the EESC. Processing of data may also occur for administrative and financial audit purposes. A medical health certificate is asked of the selected candidates in order to confirm aptitude to work in an office environment, and a police statement is requested in order to confirm that they have not been convicted of serious offences.

7. Description of the categories of persons whose data are processed	Any person applying for a traineeship at the EESC
8. Description of data categories processed	The data collected in the framework of a traineeship application concern personal data (name, first name, gender, nationality, date and place of birth), contact data (email address, address, telephone), academic and/or professionnal credentials (completed and/or ongoing studies, previous employment and/or traineeship experience) and other relevent information (langage skills, IT skills,etc…). Only preselected candidates have to send: - a copy of ID/passport - a copy of diploma(s) - a proof of health insurance (if applicable). Selected candidates have to send in addition: - a medical certificate - a police statement proving that the selected candidates have not been convicted of serious offences.
9. Time limit for retaining the data	The data of pre-selected candidates are kept for up to 2 years after the official starting date of the traineeshop period. This period is necessary to deal with any possible complaints to the Ombudsman. After this time anonymised data will be kept for historical and statistical purposes. The personal data of persons effectively recruited for a traineeship will be kept in the Traineeship Office for 5 years after the official starting date of the traineeship in question for financial audit purposes and in order to allow proper exchange of information among traineeship offices of other EU institutions. As having been a paid trainee for at least six weeks in any EU institution is an exclusion criterion for traineeships application at other EU institutions, bodies and agencies (see Article 1.2.4. of the decision 201/19 A; other EU institutions apply similar rules), it is important to keep these data for a reasonably long time after the actual traineeship period. In case of questions from other institutions within a reasonable period, the traineeship office must be able to give correct answers. Beyond this period, data will only be stored anonymously for statistical purposes.
10. Recipients of the data	The personal data compiled in this framework are disclosed solely and exclusively to the staff members in charge of the EESC Traineeship Office. Traineeship advisors within the respective departments responsible for (pre-) selecting the EESC trainees only have access to pseudonymized data, until the pre-selection process is completed. The personal data obtained will not be disclosed to any third parties, unless insofar this would be necessary for the purposes indicated above. Under no circumstances will the personal data be disclosed for direct marketing purposes.
11. Transfers of personal data to a third country or an international organisation	No transfers of personal data will be made to a third country or international organisation.
12. General description of security measures, where possible	

1. Data available in electronic format

In order to safeguard the personal data against any possible misuse or unauthorised access, the digital information is registered in a database with restricted access codes for the above mentioned data recipients only.

The public web interface (the on-line application form) is the DMZ, and a dedicated web service is connected to the database and to an internal server behind the firewall. The URL's of the web service are not published. In other words: they cannot be seen from the outside (the Internet).

Data sent to the database via the public web application are transferred without any interference: no changes can be made to the form before it reaches the database.

The staff members in charge of the Traineeship Office have full operational access to the database (including the possibility to modify personal data upon the applicant's explicit request). Access for the traineeship advisors responsible for (pre-) selecting the trainees is limited to selection and consultation purposes only; these data are pseudonymized, until the pre-selection process is completed.

The database and the business logic of the application are established behind a firewall and they are only accessible via a web interface. Both the administrative interface (restricted to the Traineeship Office) and the consultative interface of the application (available to the Traineeship Office and to the traineeship advisors responsible for (pre-) selecting the trainees), use Windows authentication to authorise the respective access to data.

Applicants can consult the status of their traineeship request on-line, via an individual username/password protection code communicated to the applicant upon registration of his/her traineeship application. The data displayed on this consultative web page are of a non-personal character: only the traineeship period to which the application relates and the current status of the application (registered, valid, pre-selected or non-selected, etc.) are revealed.

2. Data available in paper format

Paper format information including medical health certificates and police statements are locked in secured offices, attributed to the Traineeship Office and – later on – to the Human Resources Directorate's Archives.

13. Privacy statement	Traineeship

Part 2
Compliance check and risk screening

1.a) Legal basis and reason for processing

- [x] (a) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body
- [x] (b necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below)
- [x] (c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

	☑ (d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes ☐ (e) necessary in order to protect the vital interests of the data subject or of another natural person [Tick (at least) one of the boxes]
1b) Legal basis	Decision Nº 201/19A laying down rules on traineeships at the EESC.
2. Are the purposes specified, explicit and legitimate?	Yes. The processing of personal data aims at managing the applications administratively (confirming receipt of the application, informing applicants of the outcome of their application, etc.) and at facilitating the internal selection procedure of the trainees recruited by the EESC. Processing of data may also occur for administrative and financial audit purposes (e.g. to enter EU-buildings when visiting other EU-Institutions). A medical health certificate is asked of the selected candidates in order to confirm aptitude to work in an office environment, and a police statement is requested of them in order to confirm that they have not been convicted of serious offences.
3. Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?	There is no incompatibility. When information is processed for others purposes, those purposes are linked to the initial purpose (i.e. payment of the grant).
4. Do you really need all the data items you plan to collect?	Yes, all the personal data processed are necessary.
5. How do you ensure that the information you process is accurate?	Each information provided by the candidates is checked against supporting documents.
6. How do you rectify inaccurate information?	The trainee must inform the traineeships office about data to be corrected. The correction is done by the traineeships office.
7. Are they limited according to the maxim "as long as necessary, as short as possible"?	Yes
8. If you need to store certain information for longer, can you split the storage periods?	Yes. Retention periods are split
9 How do you inform data subjects?	The processing is described in Decision 201/19A of July 2019 and on every means of communication at our disposal. Applicants are informed of their rights regarding the personal data processed in the framework of the EESC's traineeship programme by way of a specific privacy statement on the EESC's Internet website.
10. Access and other rights of persons whose data are processed	In order to exercise their rights, data subjects can contact the controller. Questions will be answered within 15 working days.

11. Does this process involve any of the following?	☑ (a) data relating to health, (suspected) criminal offences or other special categories of personal data ☐ (b) evaluation, automated decision-making or profiling ☐ (c) monitoring data subjects ☐ (d) new technologies that may be considered intrusive
Part 3 **Linked documentation**	
1. Links to threshold assessment and DPIA (where applicable)	No hyperlink inserted
2. Where are your information security measures documented?	No hyperlink inserted
3. Links to other documentation	Privacy statement FR version
4. Other relevant documents	