



European Economic  
and Social Committee

### Record of processing activity Part 1

Name of the data  
processing:

Accreditation

Created on

21/09/2018

Last update

Reference number

009

Year

2018

1. Controller:

European Economic and Social Committee

2.a) Service responsible

SECU

2b) contact details

SECU - Directorate L

[secu@eesc.europa.eu](mailto:secu@eesc.europa.eu)

3. Joint controller

Not applicable

4. DPO: contact details

[data.protection@eesc.europa.eu](mailto:data.protection@eesc.europa.eu)

5. Processor(s) (where  
applicable)

Not applicable

6. Purpose(s) of the data  
processing

Security of buildings and staff and facilitating access to buildings by staff and visitors.

7. Description of the  
categories of persons  
whose data are processed

Officials and other staff of the European institutions, CoR and EESC members, visitors, suppliers, external security guards.

8. Description of data

categories processed

- for VIP guests: last name, first name, role (minister, ambassador, etc.), vehicle registration number
- for external participants: last name, first name, date of birth, nationality and identity card/passport number
- for internal participants (other EU institutions): last name and first name.

9. Time limit for retaining the data

The data will be kept for one year from the date on which the party concerned ceases to be in direct contact with the Committees and no longer requires access to the buildings.

10. Recipients of the data

The two Committees' internal security service, the security guard department, the two Committees' human resources directorates, organisers of events and activities and, subject to prior authorisation from the secretaries-general, the local or federal police and the national security service.

11. Transfers of personal data to a third country or an international organisation

Not applicable.

12. General description of security measures, where possible

The database can only be accessed by means of an individual access code by a limited number of people working for the Committees' security services and those duly accredited.

13. Privacy statement

[Accreditation](#)

## Part 2 Compliance check and risk screening

1.a) Legal basis and reason for processing

- necessary for the performance of a task carried out in the public interest
- (a) or in the exercise of official authority vested in the Union institution or body
  - (b) necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below)
  - (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

2. Are the purposes specified, explicit and legitimate?

Yes

3. Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?

The data will not be processed for any other purpose.

4. Do you really need all the data items you plan to collect?

Yes, all the information requested is necessary.

5. How do you ensure that the information you process is accurate?

The information is provided by the participants themselves.

6. How do you rectify inaccurate information?

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?

9. How do you inform data subjects?

The EESC has drawn up a privacy statement which is published on the security service website.

10. Access and other rights of persons whose data are processed

In order to exercise their rights, the persons concerned may contact the processing department.

( [secu@eesc.europa.eu](mailto:secu@eesc.europa.eu) )

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



No hyperlink inserted

4. Other relevant documents