



European Economic  
and Social Committee

### Record of processing activity Part 1

Name of the data processing

Created on

Last update

Reference number

Year

1. Controller: European Economic and Social Committee

2.a) Service responsible

2b) contact details  
The Secretary General's team ("Team SG"), acting on behalf of the EESC.  
[team-sg@eesc.europa.eu](mailto:team-sg@eesc.europa.eu)

3. Joint controller

4. DPO: contact details [data.protection@eesc.europa.eu](mailto:data.protection@eesc.europa.eu)

5. Processor(s) (where applicable)

6. Purpose(s) of the data processing  
The purpose is twofold:  
1) To guide members on the interpretation and implementation of the provisions of the Code of Conduct of members  
2) To assess alleged breaches of the Code of Conduct for Members.

7. Description of the categories of persons whose data are processed  
1) Members that are concerned by the procedures laid out under Article 7 of the EESC Code of conduct and for which the Advisory Committee is responsible  
2) third parties that are heard by the Advisory Committee

8. Description of data categories processed

Any data relevant to the case:

(1) the behavior, action or inaction of persons under investigation;

(2) the legal qualification of these actions or inactions with regard to the Code of Conduct;

(3) the individual responsibility of the persons concerned, including their financial responsibility;

(4) sanctions, if any, to be imposed on the persons concerned. These personal data are contained:

- in electronic/paper files (written enquiry reports, written testimonies or minutes of hearings, exchanges of emails, etc.) that are necessary for the examination of the case.

- in Video/Audio recordings: hearings with third parties can only be recorded with the explicit consent of the persons concerned.

9. Time limit for retaining the data

Files are kept in paper version in the archives of the Team SG (in a protected safe) but also in electronic version on a confidential drive "shr-advisory-committee-cese" whose access is limited to the three members of Team SG:

- electronic/paper files (written enquiry reports, written testimonies or minutes of hearings, exchanges of emails, etc.) shall be kept by the Advisory Committee members and secretariat only for the examination of the case. Copies held by the members shall be subsequently destroyed and one single copy will be kept by the secretariat:

- for a period of five (5) years if the case was closed without further action. This retention period is justified by the need to detect possible cases of recidivism, which in isolation would not give rise to the opening of a new procedure but which could do so if they were repeated over a period of time;
- for a period of ten (10) years if sanctions were adopted. This retention period is justified in the light of the obligation to take into account, in the event of a new procedure, a possible recidivism as well as the past conduct of the member concerned.

- Video/Audio recordings are used for transcription purposes and are subsequently deleted.

10. Recipients of the data

All relevant files are transmitted to all members of the Advisory Committee for their deliberations.

Those files may be transmitted for the follow-up of the "breach procedure" to the President, to the enlarged presidency and to the Bureau. They can also be transmitted to the competent internal administrative services responsible for the management of these files (Legal Service, Data Protection Officer, Secretary general team). Any transmission is done on a strictly need-to-know basis and depending on the need to ensure the confidentiality of persons.

Without prejudice of the rights of defense of the alleged offender, the Advisory Committee guarantees the anonymity of all whistleblowers, witnesses and alleged victims. Their identity can only be revealed with their explicit consent.

11. Transfers of personal data to a third country or an international organisation  
No transfers will take place.

12. General description of security measures, where possible

13. Privacy statement  
[Advisory Committee on Conduct of Members](#)

## 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  
N/A

that these are not incompatible with the initial purpose(s)?	
4. Do you really need all the data items you plan to collect?	Yes
5. How do you ensure that the information you process is accurate?	N/A
6. How do you rectify inaccurate information?	N/A
7. Are they limited according to the maxim "as long as necessary, as short as possible"?	N/A
8. If you need to store certain information for longer, can you split the storage periods?	N/A
9 How do you inform data subjects?	Privacy statements
10. Access and other rights of persons whose data are processed	<p>Data subjects have the right to request access to their personal data. Also, they have the right to request rectification or erasure or restriction of the processing of their personal data.</p> <p>Data subjects can direct their queries to: <a href="mailto:team-sg@eesc.europa.eu">team-sg@eesc.europa.eu</a></p> <p>The query will be dealt with within fifteen (15) working days.</p> <p>Data subjects can also contact the Data Protection Officer: <a href="mailto:data.protection@eesc.europa.eu">data.protection@eesc.europa.eu</a></p> <p>If the data subjects consider that their rights under Regulation EU 2018/1725 have been infringed as a result of the processing of your personal data by the EESC, they have the right to lodge a complaint to the European Data Protection Supervisor : <a href="mailto:edps@edps.europa.eu">edps@edps.europa.eu</a></p>
11. Does this process involve any of the following?	<input type="checkbox"/> (a) data relating to health, (suspected) criminal offences or other special categories of personal data <input type="checkbox"/> (b) evaluation, automated decision-making or profiling <input type="checkbox"/> (c) monitoring data subjects <input type="checkbox"/> (d) new technologies that may be considered intrusive
<b>Part 3 Linked documentation</b>	
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