| **Record of processing activity**  
**Part 1** |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name of the data processing:</strong></td>
</tr>
<tr>
<td><strong>Created on</strong></td>
</tr>
<tr>
<td><strong>Last update</strong></td>
</tr>
<tr>
<td><strong>Reference number</strong></td>
</tr>
<tr>
<td><strong>Year</strong></td>
</tr>
<tr>
<td><strong>1. Controller:</strong></td>
</tr>
<tr>
<td><strong>2.a) Service responsible</strong></td>
</tr>
</tbody>
</table>
| **2b) contact details** | A3 MEM – Members’ Working Conditions  
Rue Belliard/Belliardstraat 99, 1040 Bruxelles/Brussel, BELGIUM  
Members’ Statute sector  
_STATUTDESMEMBRESCESE@EESC.EUROPA.EU |
| **3. Joint controller** | |
| **4. DPO: contact details** | data.protection@eesc.europa.eu |
| **5. Processor(s) (where applicable)** | |
| **6. Purpose(s) of the data processing** | The data are processed with a view to preparing a file enabling the ethical committee to establish whether a beneficiary (EESC member, delegate, alternate or expert) has infringed the ethical standards set out in the Code of Conduct. The ethical committee submits to the Committee president a duly substantiated report containing recommendations for a decision, which may include penalties if necessary. |
## 7. Description of the categories of persons whose data are processed

Anyone (EESC member, delegate, alternate or expert or staff member)

## 8. Description of data categories processed

**Data relating to:**

1. the behaviour, action or failure to act on the part of the persons under investigation;
2. the legal definition of such action or failure to act with regard to the Code of Conduct and to other obligations by which the persons in question are bound;
3. the individual responsibility of the persons concerned;

any penalties imposed on the persons concerned.

## 9. Time limit for retaining the data

Files that are considered not to be cases following the preliminary assessment will be stored for five years dating from the decision not to open an investigation. The length of this period of storage is justified by the need to detect possible instances of repeat infringements. A single instance would not give rise to the opening of an administrative investigation, but an investigation could be launched if several such instances were to recur over time.

When the investigations (in accordance with Article 12 of the Code of Conduct) have been closed, the files are kept by the ethical committee secretariat in electronic format on the confidential drive of the MEM unit, Members’ Statute sector. Access to this drive is limited solely to persons belonging to the sector, for a period of ten years from the date on which the investigation was closed.

## 10. Recipients of the data

In principle, personal data are not transferred between units and persons at the EESC.

Nonetheless, as provided for in Article 9(2)(a) of the Code of Conduct, personal data could be transferred to the EESC’s Legal Service and, for administrative reasons, to the EESC’s Translation Directorate and Coordination / Cross-cutting interinstitutional issues department.

Should it prove necessary, files could also be forwarded – in part or in their entirety – to other bodies of the European Union or to other official bodies: the European Data Protection Supervisor, the European Anti-Fraud Office (OLAF), the Court of Justice of the European Union (CJEU), the European Ombudsman and the Court of Brussels.
11. Transfers of personal data to a third country or an international organisation

Personal data will not be transferred to third countries or to international organisations.

12. General description of security measures, where possible

No hard copy confidential file is either kept or circulated during processing. The electronic version of the file is saved on a shared drive, with access limited to staff directly responsible for handling these requests, with the exception of investigators. Confidential documents are communicated to the members of the ethical committee via encrypted messaging and if necessary are password protected. Confidential documents are sent, marked as confidential, to the Translation Directorate so that the members of the ethical committee can examine them in a language with which they are sufficiently familiar.

13. Privacy statement

Privacy statement Ethical Committee

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 or in the exercise of official authority vested in the Union institution or body
- necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below)
- 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
- the data subject has given consent to the processing of his or her personal data for one or more specific purposes
- 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

Article 9 of the Code of Conduct of EESC members

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)?

yes

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?

The data are provided by the persons concerned in the course of the investigation.

6. How do you rectify inaccurate information?

At the request of the person concerned, prior to the approval of the investigation documents.

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

9. How do you inform data subjects?

Privacy statement

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.

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