<table>
<thead>
<tr>
<th>Name of the data processing</th>
<th>EESC plenary session recordings and voting system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created on</td>
<td>19/11/2018</td>
</tr>
<tr>
<td>Last update</td>
<td>08/10/2020</td>
</tr>
<tr>
<td>Reference number</td>
<td>021</td>
</tr>
<tr>
<td>Year</td>
<td>2018</td>
</tr>
<tr>
<td>1. Controller:</td>
<td>European Economic and Social Committee</td>
</tr>
<tr>
<td>2a) Service responsible</td>
<td>A1 GRE</td>
</tr>
<tr>
<td></td>
<td>A2 CIP</td>
</tr>
<tr>
<td></td>
<td>A3 INF</td>
</tr>
<tr>
<td>2b) contact details</td>
<td><a href="mailto:greffeinfo.doconly@eesc.europa.eu">greffeinfo.doconly@eesc.europa.eu</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:audiovisualhelpdesk@eesc.europa.eu">audiovisualhelpdesk@eesc.europa.eu</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:webeesc@eesc.europa.eu">webeesc@eesc.europa.eu</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:eesc-social-media@eesc.europa.eu">eesc-social-media@eesc.europa.eu</a></td>
</tr>
<tr>
<td>3. Joint controller</td>
<td></td>
</tr>
<tr>
<td>4. DPO: contact details</td>
<td><a href="mailto:data.protection@eesc.europa.eu">data.protection@eesc.europa.eu</a></td>
</tr>
<tr>
<td>5. Processor(s) (where applicable)</td>
<td>External companies that do the recordings, videos, take photographs and are in charge of the voting system.</td>
</tr>
<tr>
<td>6. Purpose(s) of the data processing</td>
<td></td>
</tr>
</tbody>
</table>
EESC plenary session recordings are made for transcription, communication and publicity reasons, as well as for historical purposes.

Video recordings are published on social media.

Plenary sessions are broadcasted livestream.

Members' correspondence e-mail addresses (= non-confidential) are used for voting purposes.

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

EESC members (only members' correspondence addresses are processed = non-confidential), EESC staff and trainees, contractors' staff involved in the organisation of plenary sessions, invited speakers, guests, interpreters and any other persons present in the plenary session room. For social media platforms, this includes the users of such platforms.

**8. Description of data categories processed**

Sound, visual, audiovisual and live recordings carried out by the Committee, irrespective of the medium in which they are stored. Live recordings shall mean recordings of webcast meetings in part or in whole. EESC members' correspondence e-mail addresses (= non-confidential) are used for remote voting purposes.

**9. Time limit for retaining the data**

The minutes drawn up on the basis of these recordings shall be stored in the Committee's archive and transferred to the Historical Archives of the European Union after a period of thirty years in accordance with the rules.

Audio recordings are stored for thirty years in accordance with the EESC Bureau Decision 236/10 A.

Debates declared confidential (in camera) shall not be recorded unless otherwise decided by the Assembly and shall be so for transcription purposes only. Such recordings shall be destroyed as soon as the relevant minutes are approved and, at the latest, six months after the date of the meeting.

Members' correspondence e-mail addresses are stored in their personal file in the Agora database for the duration of the whole term of office, and are afterwards stored indefinitely and might be used for historical purposes.

**10. Recipients of the data**

The EESC Rules of Procedure provide that plenary sessions of the Committee and meetings of the sections shall be public. Therefore the data is accessible to the EESC members, staff and to general public. EESC members' correspondence e-mail addresses (= non-confidential) shall be made available to the external company in charge of the voting system.
11. Transfers of personal data to a third country or an international organisation

N/A

12. General description of security measures, where possible

Recordings are stored on shared drives to which only a restricted number of staff members have access. Members’ correspondence e-mail addresses are stored in the Agora database, which is restricted to staff given access rights by IT with a password, and central management is provided by the Registry Unit.

13. Privacy statement

Plenary Session

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

EESC Bureau Decision No 206/17 A of 17 October 2017 establishing the Rules on the Recording of Activities Undertaken by the European Economic and Social Committee

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 personal data are not used for any other purpose.

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

Yes, all data are necessary.

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

Members have access to their data via the Members’ Portal and may check their accuracy at all times.

6. How do you rectify inaccurate information?

Rectifications are made by the Registry and Legislative Planning Unit at the request of the member or following a change affecting the member’s term of 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. Please see details under point 9, part 1.

9. How do you inform data subjects?

In accordance with paragraph 1, Article 10 of Decision 006/17 A, all members of the Committee and its staff are informed of the rules on the recording activities as soon as they take up office.

Plenary session participants are informed that the meeting will be recorded following the procedure set out in Decision No 206/17 A. This information is provided in the convocation to the plenary session.

In addition, participants are informed via a privacy statement.

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

In order to exercise their rights, data subjects can contact the service responsible. 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

No hyperlink inserted

4. Other relevant documents