### Record of processing activity

#### Part 1

<table>
<thead>
<tr>
<th>Name of the data processing</th>
<th>Partnerships with civil society organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created on</td>
<td>04/08/2020</td>
</tr>
<tr>
<td>Last update</td>
<td>26/08/2020</td>
</tr>
<tr>
<td>Reference number</td>
<td>076</td>
</tr>
<tr>
<td>Year</td>
<td>2020</td>
</tr>
<tr>
<td>1. Controller:</td>
<td>European Economic and Social Committee</td>
</tr>
<tr>
<td>2a) Service responsible</td>
<td>D5 CSS</td>
</tr>
<tr>
<td>2b) contact details</td>
<td>D.5 CSS Head of Unit&lt;br&gt;Directorate D</td>
</tr>
<tr>
<td>3. Joint controller</td>
<td>- For partnerships with civil society organisations, it is the partner organisation who manages the entire process of registration of participants and bears full responsibility for the registration data collected.&lt;br&gt;- The EESC collects exclusively the data required by Security to grant access to the organisers and participants.</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></td>
</tr>
</tbody>
</table>
6. Purpose(s) of the data processing

- Data collected for the organisation and management of partnerships with external civil society organisations;
- Data collected for accreditation purposes;
- Data collected for communication (partnership reports/minutes for the website);
- Data collected for statistics and reporting on partnerships.

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

**Partnerships with civil society organisations:**

- General public registering exclusively via partner organisation – the data is collected by the EESC uniquely for accreditation and security purposes;
- EESC members and staff.

8. Description of data categories processed

**Accreditation Data**

Collected for accreditation purposes, according to the internal rules established by the Security service (for all the events with external partners without EU institution badge):

- Name,
- Surname,
- Country of residence,
- Nationality,
- Number of ID card or passport,
- Car number (where relevant).

For additional information please refer to the accreditation privacy statement.

9. Time limit for retaining the data

**Data stored on CSS Unit shared drive**

Partner organisation data are kept as long as follow-up, reporting or evaluation actions are necessary.

**Accreditation**

Data obtained for these purposes are transferred to the Security service and then deleted by the CSS Unit. The Security service retains data for one year, according to the accreditation privacy statement.

**Internet and intranet**

Data published on the Internet and intranet will remain there indefinitely. In case of reports, speeches and presentations written consent is collected before publication. Data subjects may contact the administrator in charge of the event with request to modify or delete any information pertaining to his or her person.

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

No transfer of data is taking place.

12. General description of security measures, where possible

The collected personal data are stored on the EESC’s servers. The access to all personal data as well as all information collected in the context of a partnership is only granted through UserID/Password to a defined population of users: in case of Dynamics – to Dynamics users only, in case of Unit’s share drive – to members of the CSS Unit only.

13. Privacy statement

CSS partnerships

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

(a) necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below)

(b) 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

(c) the data subject has given consent to the processing of his or her personal data for one or more specific purposes

(d) 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)?

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?
By following internal guidelines of the data required by various EESC services implicated in managing the events organised by the Unit, such as data required by the Security to give them access to the EESC premises.

6. How do you rectify inaccurate information?
Website, email and Unit share drive – upon request; only where necessary, records of rectification may be kept (such as minutes, reports, track changes or emails stored).

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?
Data collected for accreditation purposes: 1 year.

9. How do you inform data subjects?
By including the appropriate privacy statement in all official messages, such as invitations, reminders, and newsletters.

10. Access and other rights of persons whose data are processed
Requests from data subjects, regarding access, deletion, correction of data receive a follow-up within 15 days of introducing the request.

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