## 1. General Information

<table>
<thead>
<tr>
<th>Reference number</th>
<th>J007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last update:</td>
<td>18/04/2023</td>
</tr>
<tr>
<td>Joint controllers:</td>
<td>EESC and CoR</td>
</tr>
<tr>
<td>Joint controllership arrangement</td>
<td>EESC-CoR JCA</td>
</tr>
<tr>
<td>Directorate/unit:</td>
<td>Directorate IIT</td>
</tr>
</tbody>
</table>
| Contact details:       | Directorate IIT  
Rue Belliard, 99-101, 1040 Brussels |
| DPO - contact details  | EESC Data Protection; data.protection@cor.europa.eu |
| Processor(s)           | Not applicable |
| Data Processing Agreement | n/a |

## 2. Purpose and description of the personal data processing

| Purpose(s) of the personal data processing | To enable use of the telephone system at the EESC-COR.  
Measuring the capacity used and estimating the required capacity in the future,  
Follow-up on telephone charges for budgetary reasons and for cost-control,  
Billing of private telephone calls,  
Solving technical problems. |
| Categories of persons whose personal data are processed | All staff, statutory or not, within the Committees and having a need for using the Committees' telephone system.  
All Members (including alternates, assistants & CCMi delegates and alternates) and having a need for using the Committees' telephone system. |
| Categories of personal data processed | The first set of data is composed of records known as "call data records". These records contain the number of the calling party (if available), the number of the called party, the date and time of the beginning and end of the communication, the cost of the communication (if it is an external call) and the number of the code if a service or private code was used to establish the communication.

A second set of data is composed of the data provided by the telecommunications operators for the purposes of billing. This billing data contains the detailed list of calls with data similar to those contained in the call data records.

A third group of data is composed of the data stored on the telephone set of the user.

A fourth group of data is composed of that communicated by the internal user to the external world.

A fifth group of data is composed of telephone directories containing all staff. |
| Recipients of the personal data | The persons responsible for recovery orders are informed of the amounts to be recovered from salaries in the case of private calls (i.e. only the amount to be recovered per user & no details of individual calls).

The DIIT and its hierarchy for anonymous reports relating to the infrastructure.

Competent persons working within the DIIT for ad-hoc reports relating to the telephone switchboard (e.g. follow-up of queries relating to usage of private or service codes or the use of service gsm's).

The COR administration for reporting related to the COR gsm regulation.

The EESC administration for reporting related to the EESC gsm regulation. |
<table>
<thead>
<tr>
<th>Transfers of personal data to a third country or an international organization</th>
<th>Not applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retention period of the personal data</td>
<td>The data stored in electronic format (in the &quot;call data records&quot;) are retained for a maximum period of 6 months. The data obtained from the telecommunications operators and used as the basis for billing are kept for the same duration as the financial files. Global bills (no personal data) from the operators are included in the financial files. The financial files for fixed telephony contain no information permitting direct identification of the data subject. The financial files for the use of service gsm's contain no information permitting direct identification of the data subject. The financial files relating to the recovery of private use of the service gsm contains a list of all dialled numbers and data related to roaming (if any). Anonymous data is kept indefinitely</td>
</tr>
<tr>
<td>General description of security measures, where possible</td>
<td>In order to protect personal data, a number of technical and organisational measures have been put in place. These include appropriate measures to address online security, physical security, risk of data loss, alteration or unauthorised access, taking into consideration the risk represented by the processing and the nature of the data being protected.</td>
</tr>
<tr>
<td>Data Protection Notice</td>
<td>Data Protection Notice available internally</td>
</tr>
</tbody>
</table>