



European Economic  
and Social Committee

### Record of processing activity Part 1

Name of the data  
processing

Telephony

Created on

04/09/2018

Last update

11/09/2020

Reference number

015

Year

2018

1. Controller:

European Economic and Social Committee

2.a) Service responsible

L3 IT

2b) contact details

[helpdesk@eesc.europa.eu](mailto:helpdesk@eesc.europa.eu)

3. Joint controller

Not applicable

4. DPO: contact details

[data.protection@eesc.europa.eu](mailto:data.protection@eesc.europa.eu)

5. Processor(s) (where  
applicable)

Not applicable

6. Purpose(s) of the 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.

7. Description of the categories of persons whose 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.

8. Description of data categories 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.

9. Time limit for retaining the data

- The data stored in electronic format (in the "call data records") 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 contains 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

10. Recipients of the 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 IT unit and its hierarchy for anonymous reports relating to the infrastructure.
- Competent persons working within the IT unit 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.

11. Transfers of personal data to a third country or an international organisation **None**

12. General description of security measures, where possible **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.**

13. Privacy statement [Telephony](#)

## 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)
- processing is necessary for the performance of a contract to which the
- (c) 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 that these are not incompatible with the initial purpose(s)?

**Not applicable**

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

**Yes, all the processed data are necessary.**

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

**Automated processing**

6. How do you rectify inaccurate information?

**Not applicable**

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?

**Not applicable**

9 How do you inform data subjects?

Information on the telephone system is available on the intranet. This information is mentioned (with indication of the location):

- in the documentation provided to the new officials during the "welcome" sessions
- in the documentation provided to all users (Members & staff)

The principal IT publication for end-users is the "IT Guide". Regular reminders are sent by e-mail concerning relevant issues from the "IT Helpdesk".

A privacy statement is published on the intranet. The decision on acceptable use of the committees' computer (includes telephones) system is published on the intranet

In addition, the following information specific to the telephone system:

- List of reports generated from the "call data records" (as described in point 9);
- The identification of the calling number is communicated to the outside when a user at the Committees calls an external number;
- There is no centralised recording of calls. The users can record calls in which they participate by connecting a recorder to a port at the back of the telephone set
- The user can erase the number of the caller which is stored in the memory of the telephone set once the call is finished;
- If the user does not wish the calling number to appear on the screen of their telephone set in their absence, they can divert the phone to their voice-mail;
- If the user does not wish their private number to appear when their phone is forwarded to their private number during teleworking, a specific shortcut is used to hide their private number
- The telephone directory of the institution is not public.

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

Data subjects can exercise their rights by addressing themselves to the Data Controller identified in the privacy statement (IT, Head of Unit).

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

**Organisational Security measures**

[http://jsnet.eesc.europa.eu/en/dl/it/services/index%20of%20service%20topics/sec\\_mgmt.pdf](http://jsnet.eesc.europa.eu/en/dl/it/services/index%20of%20service%20topics/sec_mgmt.pdf)

**Technical security measures**

<http://jsnet.eesc.europa.eu/EN/dl/it/Services/Index%20of%20Service%20Topics/Technical%20Security%20Measures.pdf>

3. Links to other documentation

[Telephony service overview on the intranet](#)

4. Other relevant documents