## Record of processing activity
## Part 1

| | |
|---|---|
| Name of the data processing | Unified Communication |
| Created on | 27/05/2020 |
| Last update | 15/09/2020 |
| Reference number | 085 |
| Year | 2020 |
| 1. Controller: | European Economic and Social Committee |
| 2.a) Service responsible | L3 IT |
| 2b) contact details | helpdesk@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 | To enable internal unified communication for Committees' staff.<br><br>Unified Communication provides an integrated set of communication and collaboration tools to all Committee staff. It comprises video conferencing, instant messaging and document sharing facilities in a single tool, based on the Microsoft Skype for Business (SfB) software. |
| 7. Description of the categories of persons whose data are processed | Staff (statutory & non-statutory) of the EESC and COR |

| | |
|---|---|
| 8. Description of data categories processed | The Committees' solution for Unified Communication, Skype for Business, is part of the Microsoft Office software suite and integrated with other components of the platform, notably Outlook. While primarily only keeping lofiles for its internal operations, it uses a variety of other personal data items already present in the environment and shared between its various components. Overall, the personal data handled in Unified Communications consists of:<br><br>• Username<br>• Name & Surname<br>• Email address (office)<br>• Contact details – office telephone number, office address<br>• Location – a free text field that is by default empty.<br>• Calendar information (from Outlook) – meeting details , availability<br>• Recordings of audio/video meetings (optional for meeting/conference organisers)<br>• Instant messaging conversation details including content of messages exchanged (the messages are stored like emails in Outlook)<br>• Current availability for communication purposes status information (e.g. busy/away/in a call/don not disturb/offline since etc). This information can also be set manually.<br>• Presence indicator during a call ("In a call."). This information can also be set manually.<br>• Log-files are used for solving technical problems and preparing anonymous statistics for trend analysis. These logs do not contain the content of messages or communications |
| 9. Time limit for retaining the data | • As long as the data subject is a Committee staff member<br>• After deletion from the user directory, 6 months (maximum backup rotation time) |
| 10. Recipients of the data | Other users of the system. Log-files: - administrators of the system (daily operations), - competent authorities in the context of investigations. |
| 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 | [Unified Communication](Unified Communication) |

## Part 2
## Compliance check and risk screening

| | |
|---|---|
| 1.a) Legal basis and reason for processing | ☑ (a) 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<br><br>☐ (b) necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below)<br><br>☐ (c) 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<br><br>☐ (d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes<br><br>☐ (e) necessary in order to protect the vital interests of the data subject or of another natural person<br><br>[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)? | N.A. |
| 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? | Information provided by HR & Registry units. |
| 6. How do you rectify inaccurate information? | Directly in the IT systems |
| 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? | N.A. |
| 9 How do you inform data subjects? | |

- Information on the unified communication 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

- 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 system is published on the intranet

| | |
|---|---|
| 10. Access and other rights of persons whose data are processed | What regards incorrectly encoded data in the Address Book; Data Subjects may exercise their rights by sending an e-mail to the "Helpdesk IT" functional mailbox. Other data is under the control of the users. |
| 11. Does this process involve any of the following? | ☐ (a) data relating to health, (suspected) criminal offences or other special categories of personal data<br>☐ (b) evaluation, automated decision-making or profiling<br>☐ (c) monitoring data subjects<br>☐ (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<br><br>Organisational Security measures<br><br>http://jsnet.eesc.europa.eu/en/dl/it/services/index%20of%20service%20topics/sec_mgmt.pdf<br><br>Technical security measures<br><br>http://jsnet.eesc.europa.eu/EN/dl/it/Services/Index%20of%20Service%20Topics/Technical%20Security%20Measures.pdf |
| 3. Links to other documentation | No hyperlink inserted |
| 4. Other relevant documents | |

The basic decisions regarding the IT system (acceptable use, internet & information security), privacy statements and information notes regarding personal data & information security:

http://jsnet.eesc.europa.eu/EN/dl/it/Rules/Pages/default.aspx

Service overview on the Intranet:

http://jsnet.eesc.europa.eu/EN/dl/it/Services/Pages/Videoconferencing.aspx