# Record of processing activity

## Management of personal data in the context of crisis management (STAFF)

### 1. General Information

<table>
<thead>
<tr>
<th>Name of the data processing</th>
<th>Management of personal data in the context of crisis management (STAFF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference number:</td>
<td>E015</td>
</tr>
<tr>
<td>Last update:</td>
<td>27/06/2024</td>
</tr>
<tr>
<td>Controller:</td>
<td>European Economic and Social Committee</td>
</tr>
<tr>
<td>Directorate:</td>
<td>Directorate A</td>
</tr>
<tr>
<td>Unit:</td>
<td>MODA</td>
</tr>
</tbody>
</table>
| Contact details:            | Directorate A - Registry and Legislative Planning MODA  
Rue Belliard/Belliardstraat 99-101, 1040 Brussels                        |
| Joint controller (where applicable): | N/A                                          |
| Joint controllership agreement (where applicable): | N/A                                      |
| DPO - contact details:      | EESC Data Protection                                                     |
| Processor(s) (where applicable): | N/A                                          |
| Data Processing Agreement   | N/A                                                                    |

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

| Purpose(s) of the personal data processing | The data collected are processed solely in order to handle crisis situations and ensure business continuity. More specifically, they will be used for:  
• preparation for a crisis situation (exercises);  
• communication to enable the mobilisation of staff members in critical and/or essential and/or necessary roles;  
• appropriate crisis communication with members and secretariat staff in crisis situations;  
• ensuring continuity in the performance of the |
|--------------------------------------------|-------------------------------------------------------------------------|
institution's work, in its management and in its activities that cannot or can only be minimally interrupted;  
- facilitating the process of identifying victims in the event of a disaster.

| Categories of persons whose personal data are processed | • EESC officials  
• Other staff  
• Seconded National Experts  
• Trainees  
For use in connection with the BCM: staff in critical or essential roles and their back-ups, and senior management. |

| Categories of personal data processed | • Surname and first name  
• Home phone number, if available  
• Private mobile phone number, if available  
• Work mobile phone number, if available  
• Private (if available) and work email addresses |

| Recipients of the personal data | Access to personal data is limited to:  
• Directorate A – MODA  
• Directorate L – Security  
• Directorate E – PER  
• DIIT |

| Transfers of personal data to a third country or an international organization | Not applicable. |

| Retention period of the personal data | Personal data are stored for as long as the staff member works for the EESC and for a period of 10 years after leaving the service.  
Data are regularly updated and those which are not or are no longer required for operational purposes will be deleted immediately, as appropriate. |

| General description of security measures, where possible | The data are stored:  
• In electronic storage format, including the RingRing tool, the institution's electronic messaging system, on servers and hard drives, removable memory devices and mobile phone memory.  
• Data are stored on the premises of the EESC and/or with the official and/or on the person of the official.  
Appropriate security measures such as those described below are applied at all times to protect the information (physical protection, encryption, use of passwords, etc.).  
Security measures: Those responsible for accessing private contact data are responsible for taking appropriate precautions to ensure the physical security |
of the data medium and to prevent any unauthorised disclosure or access. Where data are stored on PAPER (HARD COPY), provisions on storage of RESTRICTED UE/EU RESTRICTED documents apply.

Hard copies of documents:

- must be stored in a standard steel case in an office or working area when not in use.
- Must not be left unattended in an office (unless all doors and windows are locked and they cannot be read from outside).
- Must not be left on a desk, table or other freely accessible space that would mean staff from outside the institution (e.g. visitors, cleaners, maintenance staff) would be able to read or remove them.
- Must not be read or left unattended in public places where they could be seen by unauthorised persons (e.g. on trains, planes, in cafés, bars, etc.). may be brought home by the person responsible. They must be placed in a locked container when not in use. They must not be presented to or discussed with people who do not have a justified "need to know".
- May be taken to meetings or on a mission. However, particular attention must be paid to the need to protect them against unauthorised access. Where data are stored on REMOVABLE MEMORY DEVICES, these must be stored under the same conditions as printed documents. Data stored electronically must be protected by passwords, PIN codes or encryption to prevent unauthorised access.

| Data protection notice: | Data Protection Notice available internally |