European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing:	Management of personal data in context of crisis management (Members)
Created on	14/11/2018
Last update	27/08/2019
Reference number	024
Year	2018
1. Controller:	European Economic and Social Committee
2.a) Service responsible	MODA
2b) contact details	Directorate A - MODA (EESC-Businesscontinuity@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	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 or when the sirens and/or e-mail systems are not working; • 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; • arranging for repatriation, if necessary; • facilitating the process of identifying victims in the event of a disaster.

7. Description of the categories of persons whose data are processed	EESC members and their alternates CCMI delegates and their alternates
8. Description of data categories processed	Personal data used in the event of a crisis to communicate and ensure continuity of service: • surname and name • home phone number, if available • private mobile phone number, if available • work mobile phone number, if available • private (if available) and work e-mail addresses For the purposes of crisis management and, if necessary, arranging repatriation, we need to be able to locate the venues of meetings that EESC members are attending as part of their work for the Committee. This information can be obtained by means of a report extracted from Agora. The Business Objects report Business Continuity / BC – Members localisation processes the following personal data: the full name and mobile telephone number of the member; the name of the assistant responsible for the meeting; the name of the administrator responsible for the meeting; and the telephone number (office extension) of the administrator responsible.
9. Time limit for retaining the data	Personal data are retained for the purposes listed in point 6 for the duration of the term of office of the members, alternates and delegates at the EESC. Data are updated by members, alternates and delegates themselves or by the Registry at the request of members, alternates or delegates. Data which are not or no longer required for operational purposes will be deleted immediately, as appropriate.
10. Recipients of the data	Access to personal data shall be limited to: • Directorate A – MODA (except the Data Protection Officer) • Directorate A – Registry • Directorate L – Security • Directorate L/IT (for the maintenance and operation of the SendSMS tool). For the Business Objects report Business Continuity/BC – Members localisation, intended to facilitate repatriation, access is limited to: • The crisis management team (CMT) • The secretary-general's secretariat • Directorate A – MODA (except the Data Protection Officer).
11. Transfers of personal data to a third country or an international organisation	Not applicable
12. General description of security measures, where possible	

1. The data will be stored in the institution's electronic messaging system, and on servers and hard drives on the EESC premises.
2. 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 must be applied at all times to protect the information (physical protection, encryption, use of passwords, etc.).

Security measures: Those responsible for accessing private contact data shall be 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 (paper copy), provisions on storage of RESTREINT UE/EU RESTRICTED documents shall apply:
Paper copies of documents:

1. must be stored in a standard steel case, either in an office or working area, when not in use.
2. must not be left unattended in an office (unless all doors and windows are locked and they cannot be read from outside).
3. must not be left on a desk, table or other freely accessible space that would mean staff from outside the institutions (e.g. visitors, cleaners, maintenance staff) would be able to read or remove them.
4. 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.).
5. may be brought home by the person in charge. 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".
6. 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.

13. Privacy statement

Business Continuity (MEMBERS)

Part 2
Compliance check and risk screening

1.a) Legal basis and reason for processing

- [x] (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
- [ ] (b necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below)
- [ ] (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 ☐ (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)?	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?	The personal data will be extracted from AGORA to ensure business continuity management in general and for the SendSMS tool in particular. EESC members, alternates and delegates CCMI and their alternates will be able to insert and update their telephone number via the Members' Portal and choose the desired option. The software allows to define mobile phone numbers for specific purposes on the Members' Portal. In Agora the following values are defined: 1. mobile phone number for password resets; 2. mobile phone number for work and representation; 3. mobile phone number to receive SMS notifications from the entrance hall; 4. mobile phone number for security, crisis management and business continuity. In order to be contacted in the event of a crisis, members, alternates and delegates should enter their mobile phone number in the relevant column.
6. How do you rectify inaccurate information?	Members, substitutes alternates and delegates may change or delete their GSM numbers in the Members' Portal or request the Registry to change or delete them from the AGORA database. In the event that a member, alternate or delegate requests the modification or deletion of data in AGORA they will be corrected or deleted by the Registry within 15 days.
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	Not applicable

longer, can you split the storage periods?	
9 How do you inform data subjects?	The EESC has drawn up a privacy statement, which is published on the members' portal. Whenever a notice is sent on the subject, the link to the Privacy Statement will be included in the message. The link to the privacy statement is sent whenever members are requested to insert/update their personal data.
10. Access and other rights of persons whose data are processed	Data subjects may contact the controller to exercise their rights. Any queries will be dealt with within fifteen working days.
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)	Click here to insert a hyperlink
2. Where are your information security measures documented?	Click here to insert a hyperlink
3. Links to other documentation	Click here to insert a hyperlink
4. Other relevant documents	

Save Cancel