European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing:	Management of personal data in the context of crisis management (staff)
Created on	14/11/2018
Last update	
Reference number	023
Year	2018
1. Controller:	European Economic and Social Committee
2.a) Service responsible	MODA
2b) contact details	Direction 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 (drills); • 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; • facilitating the process of identifying victims in the event of a disaster.

7. Description of the categories of persons whose 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.
8. Description of data categories processed	• last name 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
9. Time limit for retaining the 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.
10. Recipients of the data	Access to personal data is limited to: • Directorate A – MODA (except the Data Protection Officer) • Directorate L – Security • Directorate E – PER • Directorate L - IT (for the maintenance and operation of the SendSMS tool)
11. Transfers of personal data to a third country or an international organisation	Not applicable
12. General description of security measures, where possible	

The data are stored:

1. In electronic storage format, including the SendSMS tool, the institution's electronic messaging system, on servers and hard drives, removable memory devices and mobile phone memory.
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 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 RESTREINT UE/EU RESTRICTED documents apply:
Hard copies of documents:

1. must be stored in a standard steel case 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 institution (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 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".
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 (STAFF)

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 ☐ (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	Article 55 of the Staff Regulations of Officials of the European Communities
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?	Staff members may update their phone number via Sysper Dir. E/STA: the Individual Rights team in unit E.3-STA processes current staff members' personal data by amending the last name, address, civil status, family members, etc. on the basis of documents provided by the staff member. Dir. E/PER: the Recruitment team in unit E.3-PER enters the personal data of all new staff members whose details are not yet included in the COMREF database. Dir. E/FOR: trainees enter their own mobile phone numbers in Sysper, under the supervision of the person responsible for traineeships in unit E.3-FOR
6. How do you rectify inaccurate information?	Staff members can change or delete their mobile phone numbers in Sysper at any time. The data will be updated in COMREF within 24 hours. Should a staff member ask that data in COMREF be amended or deleted (because they are incorrect or obsolete or because that person no longer works for the institution), they will be corrected or deleted 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 longer, can you split the storage periods?	No
9 How do you inform data	

subjects?	Staff members are informed about the processing process by means of the privacy statement, which is available on the intranet.
10. Access and other rights of persons whose data are processed	Data subjects may contact the controller to exercise their rights. Questions will be dealt with within 15 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)	No hyperlink inserted
2. Where are your information security measures documented?	No hyperlink inserted
3. Links to other documentation	No hyperlink inserted
4. Other relevant documents	