European Committee of the Regions

Record of processing activity – Working document

Business Continuity Plan

PART 1 - Record	
1. General Information	
Reference number	REI-1
Last update	27/05/2024
Controller	European Committee of the Regions
Directorate	Directorate E
Unit	E.I - Strategic use of resources, smart house
Contact details	businesscontinuity@cor.europa.eu
Joint controller	N/A
Joint controllership arrangement	Available internally
DPO contact details	data.protection@cor.europa.eu
Processor(s)	N/A
Data processing agreement	Available internally
2. Purpose and description of the personal data processing	
Purpose(s) of the personal data processing	The purpose of collecting GSM numbers and private email addresses of relevant staff members is to ensure effective management of and communication within the CoR in times of any threat. GSM numbers and private email addresses of Crisis Management Team members and the staff responsible for priority activities are collected and stored as defined in the Business Continuity Plan. GSM number sand private email addresses of staff members in general are encoded by the staff member in question in Sysper.
Categories of persons whose personal data are processed	All CoR staff members, and those exercising priority activities in the frame of the BCP in particular.
Categories of personal data processed	GSM numbers and private email addresses of staff members of the CoR responsible for priority activities and GSM numbers of staff members of the CoR.
Recipients of the personal data	Pursuant to the Business Continuity Plan framework, following persons are recipient of the data: - Directors and Deputy Directors - Crisis Management Team members - Business Continuity Department - Business Continuity Correspondents - Security officer

Transfers of personal data to a third country or an international organization	No, your personal data are not transferred to a non-EU country or international organisation.
Retention period of the personal data	For members of the Crisis Management Team and for staff responsible for priority activities, data are stored for as long as the staff member has this quality according to the BCP. For staff members in general, the general data storage modalities for personal contact data in Sysper apply.
General description of security measures, where possible	Regarding paper files: Private data is only to be kept in: 1) the "memory card" listing the contact details for the members of the Crisis Management Team (CMT) that is given to the members of this CMT. It has the size of a credit card and is to be carried by the member. 2) before distributing the cards, Unit EI will store them in a locked drawer, the CMT members as well as the BCP Duty Officer (holders of the "memory cards") will sign a confidentiality agreement before receiving the card. 3) a copy of the contact details of the staff in charge of the priority activities in the office and home of the BC Duty Officer and of the Local BC Plans in the offices of the respective Directors. Regarding electronic files: 1) Communication with Crisis Management Team (CMT) members is organised as a rule only via telephone or via the functional BCP mailbox. A specific CoR CMT Signal Group has been created upon unanimous decision by the members of CMT. 2) The data will be stored on the SharePoint-based Convergence Platform. 3) The data printed on "memory cards" will be transmitted to the publication department for its publication. The publication department will consult the data when processing the cards, however they will be asked to destroy all copies afterwards). Communication with staff members in times of crisis is organised as a rule via (professional) e-mail and/or sms texting to private GSM numbers encoded by staff in Sysper.
Data protection notice	Published internally