European Economic and Social Committee

Record of processing activity

User Account Management

European Committee of the Regions

1. General Information

Reference number	J008
Last update:	18/04/2023
Joint controllers:	EESC and CoR
Joint controllership arrangement	EESC-CoR JCA
Directorate/unit:	Directorate IIT
Contact details:	Directorate IIT Rue Belliard, 99-101, 1040 Brussels
DPO - contact details	EESC Data Protection; data.protection@cor.europa.eu
Processor(s)	Not applicable.
Data Processing Agreement	N/A

2. Purpose and description of the personal data processing

Purpose(s) of the personal data processing	User account management for the IT system of the European Economic and Social Committee and the Committee of the Regions (EESC-COR) to enable day-to-day operation of the IT System at the EESC-COR.
Categories of persons whose personal data are processed	All Staff, Statutory or not, within the Committees and having a need for using the Committees' IT System. All Members (including Alternates, Assistants, CCMI Delegates and alternates & their collaborators) and having a need for using the Committees' IT System
Categories of personal data processed	BASIC DATA NEEDED TO CREATE A USER ACCOUNT: - Name

	- Alias (User-name for computer system) - Committee - Office number - Phone number - Unit - E-mail address - Country, Group, Bureau (y/n) for Committee Members - Expiry Date (e.g. end of contract, end of mandate) PASSWORDS: The application to create user accounts sets an initial random password. Users have to change it the first time they logon to the network. After that, the DIIT does not know the password of the users. The DIIT, may on request of the user, reset their password. Users must change their password regularly. LOGFILES: Log-files are used for solving technical problems and for preparing anonymous statistics for trend analysis. The maximum retention time is 6 months. "LAST LOGON" A last "logon report" is generated on demand. This information is used to identify unused accounts. Unused accounts may be suspended or deleted. HELPDESK APPLICATION The Helpdesk register information about technical incidents and problems in a database application. This information is used for problem solving and trend analysis. PRINTING Multifunctional Devices (MFDs) are available which can be used for Printing, Copying and Scanning. Follow me and secure Printing works as follows: - The user prints documents to the virtual print queue (a print server located on the internal network) - These print jobs are saved on the server for 24 hours - The user identifies themselves at the devices of their choice using their service badge or userid and password. Users can edit or delete their own identification data. - The print tasks are visible on the device and ready to print. They are deleted after printing.

	As part of the EMAS programme, a user dashboard is available to see your personal environment report and user statistics (total sheets printed, duplex quota …). User dashboard data is kept for one year. SECURITY INCIDENT HANDLING Security log-files are transferred to a Security Information and Event Management System (SIEM) and are used for security incident handling. The maximum duration of any retention for archival purposes will not exceed 2 years.
Recipients of the personal data	- Services of other Institutions – Information necessary to establish an e-mail directory – Staff of other European Institutions with whom bilateral agreements exist - Administrators of the IT system (technical problem solving and preparation of anonymous statistics), - Competent authorities (on request in the context of an investigation).
Transfers of personal data to a third country or an international organization	None
Retention period of the personal data	ONLINE INFORMATION: Time during which the account is active LOG-FILES: Maximum retention time of 6 months (except Security data)
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.
Data Protection Notice	Data Protection Notice available internally