	Record of processing activity **Multifactor Authentication using Azure MFA**	

1. General Information

Reference number	J017
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)	Microsoft Ireland, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.
Data Processing Agreement	n/a

2. Purpose and description of the personal data processing

Purpose(s) of the personal data processing	Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their mobile phone. By requiring a second form of authentication, security is increased as this additional factor isn't something that's easy for an attacker to obtain or duplicate. Multifactor authentication is enabled for webmail and Terminal Services Gateway (TSG).
Categories of persons whose personal data are processed	EESC-COR Members & officials.

Rue Belliard/Belliardstraat 101 | 1040 Bruxelles/Brussel | BELGIQUE/BELGIË | Tel. +32 22822211

www.cor.europa.eu | @EU_CoR | /european.committee.of.the.regions | /european-committee-of-the-regions | @EU_regions_cities

Categories of personal data processed	Overall, the personal data handled by Multifactor Authentication consists of directory entries: - Name - Alias (User-name for computer system) - Committee - Office number - Phone number - Unit - E-mail address - Country, Group, Bureau (y/n) for Committee Members - Second factor Information for the second factor is mandatory to use the service. While the second factor isn't necessarily based on the phone number as provided by Sysper/Agora for staff and members respectively, these numbers, if present, are used to pre-populate the corresponding field in the second factor setup. Users can change it to another phone number or move to an authentication method not using phone numbers at all.
Recipients of the personal data	Access to your personal data is provided to the EESC-COR staff responsible for carrying out this processing operation and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements. The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law. For services related to Multifactor Authentication, Microsoft acts as data processor. Contact details: Microsoft Ireland, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.
Transfers of personal data to a third country or an international organization	None
Retention period of the personal data	Time during which the user account is active.
General description of security measures, where possible	All personal data in electronic format are stored on the servers of the EESC-COR and its contractors based on its service. The EESC-COR actively configures customer data location (at rest) of

Rue Belliard/Belliardstraat 101 | 1040 Bruxelles/Brussel | BELGIQUE/BELGIË | Tel. +32 22822211

www.cor.europa.eu | @EU_CoR | /european.committee.of.the.regions | /european-committee-of-the-regions | @EU_regions_cities

	the service. The service is offered from data centres in EU Member States, respectively Ireland or the Netherlands. No content data will be stored outside the EU territory. Push notifications are an exception. Any log files generated by using Multifactor Authentication Services can be analysed in the US, and while EESC-COR cannot technically avoid this, strong contractual safeguards apply to this data. Any data in transit is protected by strong encryption. 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

Rue Belliard/Belliardstraat 101 | 1040 Bruxelles/Brussel | BELGIQUE/BELGIË | Tel. +32 22822211

www.cor.europa.eu | @EU_CoR | /european.committee.of.the.regions | /european-committee-of-the-regions | @EU_regions_cities