European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing	Multifactor Authentication using Azure Multi-Factor Authentication
Created on	07/8/2020
Last update	23/10/2020
Reference number	083
Year	2020
1. Controller:	European Economic and Social Committee
2.a) Service responsible	L3 IT
2b) contact details	IT Unit, Head of Unit, helpdesk@eesc.europa.eu
3. Joint controller	
4. DPO: contact details	data.protection@eesc.europa.eu
5. Processor(s) (where applicable)	Microsoft Ireland, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.
6. Purpose(s) of the 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).

7. Description of the categories of persons whose data are processed	EESC-COR Members & officials.
8. Description of data categories 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.
9. Time limit for retaining the data	Time during which the user account is active.
10. Recipients of the 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.
11. Transfers of personal data to a third country or an international organisation	None
12. 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 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.
13. Privacy statement	Multifactor authentication
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	Necessary for the management and functioning of the institution (as per recital 22, second sentence)
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)?	N.A.

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?	Information directly provided by the users.
6. How do you rectify inaccurate information?	Directly in the IT systems
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?	N.A.
9 How do you inform data subjects?	• Information on the multifactor authentication system is available on the intranet. • The principal IT publication for end-users is the "IT Guide". • Regular reminders are sent by e-mail concerning relevant issues from the "IT helpdesk". • A privacy statement is published on the intranet • The decision on acceptable use of the Committees' computer system is published on the intranet
10. Access and other rights of persons whose data are processed	What regards incorrectly encoded data in the Multifactor Authentication system; Data Subjects may exercise their rights by sending an e-mail to the "Helpdesk IT" functional mailbox. Other data is under the control of the users.
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 Organisational Security measures http://jsnet.eesc.europa.eu/en/dl/it/services/index%20of%20service%20topics/sec_mgmt.pdf Technical security measures http://jsnet.eesc.europa.eu/EN/dl/it/Services/Index%20of%20Service%20Topics/Technical%20Security%20Measures.pdf
3. Links to other documentation	No hyperlink inserted
4. Other relevant documents	The basic decisions regarding the IT system (acceptable use, internet & information security), privacy statements and information notes regarding personal data & information security: http://jsnet.eesc.europa.eu/EN/dl/it/Rules/Pages/default.aspx Specific multifactor authentication policy: http://team.eesc.europa.eu/sites/IT/Shared%20Documents/Operational%20Policy%20for%20Multifactor%20Authentication.pdf Service overview on the Intranet: http://jsnet.eesc.europa.eu/EN/dl/it/Services/Pages/MFA.aspx Information from the Data Processor: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-data-residency