European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing:	Microsoft Office 365
Created on	28/04/2021
Last update	28/04/2021
Reference number	100
Year	2021
1. Controller:	European Economic and Social Committee
2.a) Service responsible	L3 IT
2b) contact details	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	The IT Unit is operating the future collaboration platform of the Committee which is based on the cloud-based solution Office 365 (“Office 365 platform") provided by Microsoft. This enables the members and staff of the Committee to work on any corporate or in certain cases on private devices and facilitates collaboration with internal and external stakeholders.

7. Description of the categories of persons whose data are processed	EESC-COR Members & officials External to the organisation All collaborators are granted access to use the Office 365 platform as guests with limited rights.
8. Description of data categories processed	The Office 365 platform distinguishes between the following data categories: 1. Identification data 2. Content data 3. Service generated data 4. Diagnostic data 1) Identification data contains personal data necessary for the proper identification of the user and the corresponding user account, including exhaustively: 1. Username, Email address and account status 2. User personal data (last name, first name) 3. Function-related data (Unit, Telephone numbers) This information is copied to all Office 365 data centres around the globe used to provide the service that allows global access and access control to the Committee's environment in Office 365. 2) Content data includes any content uploaded to the Office 365 platform by its users, such as documents, and multimedia (e.g. video recordings). Such data is stored by the user in Office 365 but not otherwise processed by the service 3) Diagnostic data (also known as telemetry data) is related to the data subjects' usage of office client software. The IT Unit has applied technical measures to disable sharing of diagnostic data with external parties, including Microsoft. 4) Service generated data contains information related to the data subjects' usage of online services, most notably the user IP address, creation time, site URL and user email address. This data is generated by events that are related to user activity in Office 365. Event data like account logins will allow to monitor all activity in the cloud environment of each user. Any of these categories may contain personal data. The operation of this platform requires the processing of data categories by Microsoft, for the following specific purposes: 1. Providing the Office 365 service to the Committees: ◦ Identification data, Content data, Service generated data 2. Technical support to IT teams for issues with Office 365 ◦ Identification data, Service generated data

- Identification data, Service generated data

3. Prevention, detection and resolution of security events (e.g. cyber-attack)
    - Identification data, Service generated data
4. Assistance to data subjects in exercising their rights in relation to data processed within Office 365
    - Identification data, Service generated data

The operation of this platform requires the processing of data categories by the IT Unit, for the following specific purposes:

1. Set-up, configuration and maintenance of Office 365 capabilities
    - Identification data, Service generated data
2. Administration of the rights allocated to a user account
    - Identification data
3. End-user support for issues with Office 365
    - Identification data, Service generated data, Diagnostic data
4. Prevention, detection and resolution of security events (e.g. cyber-attack)
    - Identification data, Service generated data
5. Assistance to data subjects in exercising their rights in relation to data processed within Office 365
    - Identification data, Service generated data

The above-mentioned processing of personal data by the IT Unit and/or Microsoft is done to provide the cloud component of Digital Workplace services.

In addition to this, Microsoft has been granted permission to process personal information for internal business functions in the context of providing the Office 365 service (exhaustive list):

1. Billing and Account Management
    - Identification data, Service generated data
2. Compensation
    - Identification data, Service generated data
3. Internal Reporting and Business Modelling
    - Identification data, Service generated data
4. Combatting fraud, Cybercrime, and Cyberattacks
    - Identification data, Service generated data
5. Improving Core Functionality of Accessibility, Privacy and Energy Efficiency
    - Service generated data
6. Mandatory Financial Reporting and Compliance with Legal Obligations
    - Identification data, Service generated data

Note that processing of personal data for profiling, advertising or marketing is explicitly prohibited.

9. Time limit for retaining the data

1. Data category Identification Data
    - Identification data is stored for as long as the user account is active
2. Data category Service generated data (log files)
    - Up to six months
3. Data category Content data in Office 365 and any personal data included therein
    - Up to 180 days upon expiration/termination of the subscription
4. Data category Diagnostic data
    - Up to five years

10. Recipients of the data

Within the EESC-COR:

- IT Unit Office 365 administrators
- IT Unit Security Team members

IT Unit Office 365 administrators and IT Security Team members can view identification data, diagnostic data and service generated data. They can access identification data, diagnostic data and service generated data in view of investigating issues for a specific user. For the most part they access aggregated data without any mention of personal data.

Outside the EESC-COR

Microsoft's personnel managing the databases on Microsoft cloud servers and their sub-processors' personnel on a need-to-know basis.

A list of sub-processors that has been agreed upon. Microsoft commits to have in place written agreements with all sub-processors that are at least as restrictive in terms of data protection and security as their data processing agreement with the Committees. The activities of all sub-processors are in scope of third-party audits.

Microsoft's personnel may access service generated data on a need-to-know basis. Microsoft's sub processors that provide services to Microsoft may access service generated data on a need-to-know basis.

11. Transfers of personal data to a third country or an international organisation

Data is transferred to countries outside the EU or EEA Yes

If users access the Office 365 service from outside the EU/EEA, personal data may be transferred to a corresponding location in order to provide the service. To enable the global service provisioning of Office 365, Microsoft copies identification data to all Office 365 data centres around the globe used to provide the service. This copied identification data remains under the control of Microsoft and is used to verify the user authentication details and grant access to Office 365 resources of the Committee. Service generated data is not necessarily processed outside of the EU. Microsoft is authorised to transfer it to Microsoft Corp., located in the USA, and the network of sub-processors. This type of data contains information on the usage of the service. The data is aggregated before being transferred but may contain identifiable information.

Data is transferred to international organisation(s) No

12. General description of security measures, where possible	

There are appropriate measures in place to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

Access Control: Azure Multifactor Authentication (MFA) will act as the primary authentication solution, linking access to the cloud environment and to on premise authentication. Azure MFA supports Multi Factor Authentication (MFA), allowing several options such as phone calls or use of Mobile App (Microsoft Authenticator)

In terms of confidentiality, Data Loss Prevention (DLP) rules can be created at the Office365 Security & Compliance Center.

With the Customer Lockbox feature of Office 365, the IT Unit controls how and when Microsoft engineers may access the data to give support.

Microsoft's Office 365 solutions provide the administrator with the ability to audit user interaction with Office 365 systems, safeguarding the ability of the IT Unit's incident response team to investigate personal data breaches and security incidents. The functionalities also include access of the administrator to third-party ISO, SOC, and other audit reports, as well as Audited Controls, which provides details about the various controls that have been tested and verified by third-party auditors of Office 365.

Log Analytics is a key service Microsoft provides to grant administrators a detailed view of the infrastructure of the organizations.

Cloud Application Security (CAS) is a critical component used for the identification of breaches but also to block activities and remediate issues before they arise

Office 365 Security & Compliance Center has a feature called Secure Score, used to measure an organisation's position and to help to improve its security posture at Office365.

Microsoft, as a cloud service provider, has adopted several capabilities to test technical and organisational measures (Security Assessment and Authorization). These include port scanning and remediation, perimeter vulnerability scanning, operating system patches, network level isolation/breach boundaries, Distributed Denial of Services (DDoS) detection and prevention, just-in-time access, live site penetration testing, and multi-factor authentication for service access.

Furthermore, Office 365 offers a tool called Attack Simulator to run realistic attack scenarios, including phishing, brute force password attacks or spray attacks, an attempt to try commonly used passwords against a list of user accounts.

Microsoft's solutions including Office 365 are audited regularly and Microsoft submits self-assessments to the third-party auditors and Microsoft is being audited.

13. Privacy statement	Privacy Statement Office 365

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 17, 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 Office 365 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 Office 365 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 Service overview on the Intranet: http://jsnet.eesc.europa.eu/EN/dl/it/Services/Pages/Videoconferencing.aspx Information from the Data Processor: https://docs.microsoft.com/en-us/microsoft-365/enterprise/o365-data-locations?ms.officeurl=datamaps&view=o365-worldwide