Audio and Video Communication and Collaboration services

Last update of this record		29/04/2021 (first version) - 05 /10/2022 (minor update - typos)
Reference number		ESMA40-133-1118
Nr.	Item	Record Information
1	Name of the Controller	Head of ICT Unit <itdpo@esma.europa.eu>
1,1	Address of the Controller	ESMA, 201-203 rue de Bercy, 75012 Paris - France
1,2	ESMA Parts Entrusted with Processing	ESMA/RES/ICT/CMS (Corporate Mgmt. Systems)
1,3	Processors (If any)	Microsoft NV/SA Da Vincilaan 3 Corporate Village 1935 Zaventem Belgium
2	Name and contact details of DPO	Data Protection Officer (ESMA) dpo@esma.europa.eu
3	Name and contact details of joint controller (where applicable)	Not applicable
4	Name and contact details of processor (where applicable)	Microsoft NV/SA Da Vincilaan 3 Corporate Village 1935 Zaventem Belgium
5	Purpose of the processing	ESMA processes personal data provided in connection with the use of Microsoft Teams for communication and collaboration purposes — namely for the organisation of internal and external meetings as well as conversation chats —in accordance with Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions and bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (hereinafter referred to as 'Regulation no. 1725/2018' or 'EUDPR'). As specified by the Online Services Terms, Microsoft, as a data processor, processes ESMA's personal Data only to provide the requested services to the users, the data controller, including purposes compatible with providing those services. Microsoft will not use ESMA's Data or information derived from it for any other purpose, including but not limited to advertising or similar commercial purposes.
6	Description of categories of persons whose data ESMA processes and list of data categories	Statutory and Non-statutory staff that have been granted an ESMA user account, stakeholders that have been granted an ESMA-EXT user account and external stakeholders included in Teams used for the exchange of information. The categories/types of personal data processed are the following: - Content: your meetings and conversations chats, voicemail, shared files, recordings and transcriptions; - Profile data: data that is shared within the ESMA (e.g. e-mail address, profile picture); - Image and/or video: should the meeting be recorded; - Call history: a detailed history of the phone calls you make, which allows you to go back and review your own call records; - Call quality data: details of meetings and call data are available to the ESMA system administrators. This allows the Authority's administrators to diagnose issues related to poor call quality and service usage; - Support/Feedback data: information related to troubleshooting tickets or feedback submission to Microsoft; and - Diagnostic and service data: diagnostic data related to service usage. Diagnostic data might contain personal data. On discretionary basis, ESMA will grant access to Microsoft Technical Support Teams to diagnostic data to perform problem troubleshooting. Thus, the Service Provider will not have permanent access to clear text personal data. This information will only be used to perform root cause analysis and problem determination/solution and do not for other purposes.
7	Time limit for keeping the data	1) Chat messages will be kept for 6 months and then will be erased; 2) Channel Messages: the retention period is 2 years (this retention period is required in order to keep the necessary ESMA's business information during a useful timeframe); 3) For content data (files, recordings), ESMA intention is to implement a 10 years retain and erasure policy.

8	**Recipients of the data**	The personal data is disclosed, under the need to know basis, to the following recipients: • Personal data being part of the content of the communication: video and audio exchanges among ESMA staff and external participants using Microsoft Teams (the personal data content might be determined by the sender and recipient); • Personal Data required to provide the Service: ESMA's processors, including Microsoft and Microsoft's processors involved in the data processing necessary to provide the service. **No other third parties will have access to your personal data, except if required by law:** https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-office365?view=o365-worldwide **Data sharing with third-party sub processors:** Microsoft shares data with third parties acting as their sub processors to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Customer Data, Support Data, or Personal Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Contract. All third-party sub processors with which Customer Data from Microsoft's Core Online Services is shared are included in the Online Services Subcontractor list. All third-party sub processors that may access Support Data (including Customer Data that customers choose to share during their support interactions) are included in the Microsoft Commercial Support Contractors list. https://aka.ms/Online_Serv_Subcontractor_List https://aka.ms/servicesapprovedsuppliers **Data sharing with independent third-parties:** Microsoft will not disclose Customer Data or Support Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data or Support Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data or Support Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.
9	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**	As described in the Data Protection Terms of the Online Services Terms, the instance of Office 365 is provisioned in the European Union and stored by Microsoft as data at rest only within that location: SharePoint Online site content and the files stored within that site, and files uploaded to OneDrive for Business. All storage encrypted at rest with Vendor key specific to EUI. All data encrypted with EUI owned and generated key and access to key only upon prior authorisation. The access to the EUI key is a technical and procedural governance policy by the vendor. ESMA will authorize access to the key. Microsoft shares data with third parties to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Customer Data or Support Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Online Services Terms. All third-party sub-processors with which Customer Data from Microsoft's Core Online Services is shared are included in the Online Services Subcontractor list. All third-party subprocessors that may access Support Data (including Customer Data that customers choose to share during their support interactions) are included in the Microsoft Commercial Support Contractors list.In principle, no. No access from third countries is expected. https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpiaoffice365?view=o365-worldwide **Data sharing with third-party sub processors** Microsoft shares data with third parties acting as their sub processors to support functions such as customer and technical support, service maintenance, and other operations. Any subcontractors to which Microsoft transfers Customer Data, Support Data, or Personal Data will have entered into written agreements with Microsoft that are no less protective than the Data Protection Terms of the Contract. All third-party sub processors with which Customer Data from Microsoft's Core Online Services is shared are included in the Online Services Subcontractor list. All third-party sub processors that may access Support Data (including Customer Data that customers choose to share during their support interactions) are included in the Microsoft Commercial Support Contractors list.https://aka.ms/Online_Serv_Subcontractor_List https://aka.ms/servicesapprovedsuppliers **Data sharing with independent third parties** Microsoft will not disclose Customer Data or Support Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data or Support Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data or Support Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

10	**General description of security measures, where possible.**	ESMA has implemented security measures to best address the Data protection as follows: 1) **Privileged access management to ensure Data Confidentiality and Integrity;** 2) **Monitoring and Auditing enabled on the tenant to ensure Compliance;** 3) **Second-Factor Authentication enabling access from outside ESMA premises (for ESMA staff);** 4) **File storage in Team (encryption at rest):** ESMA has implemented Customer Key for both SharePoint Online and OneDrive for Business. 5) **Customer Key for the Teams chats and messages;** 6) **Teams governance for O365 groups is deleting Groups/Teams older than 6 months with prior notification to owner.** Teams data is encrypted in transit and at rest in Microsoft datacentres. Microsoft uses industry standard technologies such as TLS and SRTP to encrypt all data in transit between users' devices and Microsoft datacentres, and between Microsoft datacentres. This includes messages, files, meetings, and other content. Enterprise data is also encrypted at rest in Microsoft datacentres, in a way that allows organizations to decrypt content if needed, to meet their security and compliance obligations, such as eDiscovery. Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data. Those measures shall be set forth in a Microsoft Security Policy. In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. Each Core Online Service also complies with the control standards and frameworks SSAE 18 SOC 1 Type II.
11	**For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:**	As a general principle, ESMA only processes personal data for the performance of tasks carried out in the public interest on the basis of the Treaty on the Functioning of the European Union, on the basis of the relevant legislation or in the legitimate exercise of official authority vested in ESMA or in a third party to whom the data are disclosed. ESMA processes personal data in line with Regulation (EU) 2018/1725 and Decision ESMA40-133-716. For more information, please see ESMA's Data Protection Statement on https://www.esma.europa.eu/data-protection. a) You are entitled to access your information relating to your personal data processed by ESMA, verify its accuracy and, if necessary, correct it in case the data is inaccurate or incomplete. b) You have the right to request the erasure of your personal data, if your personal data is no longer needed for the purposes of the processing, if you withdraw your consent or if the processing operation is unlawful. c) You can ask the Data Controller to restrict the personal data processing, under certain circumstances, such as if you contest the accuracy of the processed personal data or if you are not sure if your personal data is lawfully processed. d) You may also object, on compelling legitimate grounds, to the processing of your personal data. e) Additionally, you may have the right to data portability which allows you to make a request to obtain the personal data that the Data Controller holds on you and to transfer it from one Data Controller to another, where technically possible.You may exercise your rights by contacting the Data Controller (Head of the HR Unit at ESMA: 201-203 rue de Bercy 75012 - Paris) at HR.Helpdesk@esma.europa.eu. In some cases your rights might be restricted in accordance with Article 25 of the Regulation (EU) 2018/1725. In each case, ESMA will assess whether the restriction is appropriate. The restriction should be necessary and provided by law and will continue only for as long as the reason for the restriction continues to exist. If you have additional questions or concerns you can also contact ESMA's DPO at DPO@esma.europa.eu You have the right to lodge a complaint with the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under the Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by ESMA.In case of queries please consult ESMA's Data Protection Officer (DPO@esma.europa.eu). For more information please refer to: https://www.esma.europa.eu/about-esma/data-protection