Microsoft O365 services

Record of ESMA activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, 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.

Nr.	Item	Record Information
	Microsoft O365 services	
1	**Last update of the record**	17/04/2023
2	**Reference number**	ESMA40-1831253891-1477
3	**Name and contact details of controller**	Controller: Head of ICT Unit for service's enablement at ESMA: itdpo@esma.europa.eu Joint controllers: ESMA's Head of Departments for the personal data within their respective data processing remits. Address of the controllers: **European Securities and Markets Authority (ESMA)**

		201-203 Rue de Bercy **75012 Paris** **France**
4	**ESMA area entrusted with processing**	ESMA/ICT/CMS (Corporate Management Systems)
5	**Processors (if any)**	Microsoft NV/SA
6	**Name and contact details of DPO**	Data Protection Officer (ESMA) dpo@esma.europa.eu
7	**Name and contact details of processor (where applicable)**	Microsoft NV/SA, Da Vincilaan 3 Corporate Village, 1935 Zaventem (Belgium)
8	**Purpose of the processing**	1) To efficiently accomplish ESMA's attributed tasks carried out in the public interest under Regulation (EU) No 1095/2010 of the European Parliament and of the Council, ESMA needs a modern, secure, and reliable set of digitized productivity tools, highly coupled and compatible with technological industry accepted standards. These tools transversally support all business processes (support processes from all departments) and provide different but integrated functions to ESMA staff, stakeholders, and other external parties. The main functionalities under the scope of these tools are: • Information and data authoring (industry-wide compatible document editors and processors);

		• Information and data exchange (e.g., electronic email system, online instant messaging, voice and video calls); • electronic documents handling (document and records lifecycle management, including but not limited to document's sharing and storage); • efficient collaboration and productivity: applications that leverages efficient collaboration withing and among working groups (e.g., Team's channels). 2) To leverage resiliency, availability, security, and efficiencies in relation to electronic productivity services: managed cloud services bring efficiencies when supporting collaborative technologies (including but not limited to ensuring continuous product support, maintenance and protection against evolving security vulnerabilities which prevent from security incidents and personal data breaches). The set of collaborative and productivity tools at ESMA are leveraged by the Public Cloud service delivered by Microsoft in Europe, namely Office365 which includes: • Microsoft Teams (for video and voice communications and virtual meetings and the one-stop interface for other applications such as SharePoint, OneDrive and Outlook features) • Office solutions and editors (i.e., Word, Excel, PowerPoint) • Outlook (electronic email integrated suite including calendar items, contact lists, tasks, notes, etc.); • OneDrive for business (file sharing service); • SharePoint online (as the main document management solution); • Microsoft active Directory in the Cloud, namely Azure AD (for the storage of user accounts and identity information and for carrying-out identification and authentications processes)

		Importantly, these collaborative tools are not meant specifically to process personal data by ESMA, but rather, in supporting ESMA in the exercise of its missions and tasks, may entail the processing of personal data.
9	**Description of categories of persons whose data ESMA processes and list of data categories**	Categories of persons: • ESMA Statutory staff (TAs, CAs); • ESMA non-statutory staff (SNEs, Interims, Trainees, External consultants); • External stakeholders (e.g., NCAs; TRs, CRAs users); • EU citizens (e.g., electronic emails when communicating with ESMA); • Vendors, Services' Providers (e.g., Markets data services providers, ICT services or products providers, etc.). Categories of Data: • Content Data: Bulk data which mainly represents core ESMA's business information and non-business information necessary to support ESMA's business processes. This information can be processed in different ways (e.g., office documents and files, meetings and conversations chats, voicemail recordings, transcriptions, email content, etc.). ESMA's statutory users shall only use ESMA's designated end-user systems for purposes compatible with the ESMA Acceptable Use policy. In this context, as a general rule, ESMA discourages users to process personal data on ESMA's systems, when this is not necessary. ESMA aims at avoiding any incidental processing of private user information and has set up the following "by design" principles or safeguards:

		• Services' Enablement Data: minimized data functionally required to access and use the service or technically needed for the service to work: • Identity contact data: e-mail address, profile picture (on voluntary basis only), user's full name, phone number (professional and personal to leverage multifactor authentication), and the current professional role and function. • Diagnostic and service data: call quality data and call history data, diagnostic data related to the user's service usage and technical information required for problem troubleshooting purposes. This information shall only be used to perform root cause analysis and problem determination/solution and do not for other purposes. Diagnostic data might contain personal data. Examples of personal data: IP addresses, user accounts, personal data in memory dumps, filenames, etc.). • Security information: ○ Identification credentials (e.g., encrypted passwords, authentication tokens, multi factor authentication one-time codes and access rights); ○ User's activity logs will not focus on personal data but just on the activity required to perform cybersecurity threats assessments and investigations (e.g., to assess if personal data breach really happened). This information will be preserved for a period of 1 year in Unified Audit logs in Office365. Examples of personal data are: IP addresses, user accounts, timestamps, geolocations, and resources accessed. • System-generated Log Data: These are data that Microsoft generates to guarantee the service and quality level agreements. Information in this category includes services use or performance data (e.g., service quality data, call connectivity failures, system downtimes, etc.). This data may contain personal data (e.g., usernames) and might be used to infer information belonging to specific data subjects (identifiable natural persons).

10	**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 to keep the necessary ESMA's business information during a useful timeframe). 3) For Content Data related to Teams (files, recordings), in addition to the default retention periods set by OneDrive for Business and SharePoint, other specific retention periods are applied by ESMA's Controllers to ensure personal data in business information is kept only as long as necessary. 4) Content Data stored in OneDrive for business will be kept for as long as the user account is active. Once the user account disabled, all content shall be deleted upon 30 days. 5) For Content Data stored in SharePoint Online (Sherpa): ESMA´s Controllers shall ensure the right security access controls to preserve the need-to-know principle according to the confidentiality, integrity and availability levels of the information processed. They will also supervise and monitor compliance with the different potential retention periods that might apply according to the data stored and the business processes supported. Retention periods for different processing operations shall be strictly applied accordingly under the responsibility of Controllers. 6) The email system is considered a multipurpose collaboration tool supporting both: business processes and internal organisational processes. Consequently, the different data category types processed in the email system will abide to different retention policies, being the default retention set to 10 years. ESMA´s Controllers shall tailor the right retention periods to comply with the applicable retention and archiving requirements.

11	**Recipients of the data**	Personal data processed is disclosed to ESMA statutory and non-statutory staff holding an approved and valid business access need: - The Cloud Service Provider (Microsoft) as a general rule, will not have access to personal data in the content data without a prior and explicit consent from the Controller. Microsoft may eventually have access to personal data for the delivery of the cloud services (e.g., services' enablement or system's log data) by following the principle of minimization and purpose limitation (e.g., user accounts, file names, IP addresses, resources accessed, etc.) only upon prior agreement of the Controller and to fulfil agreed-to technical tasks (e.g., technical problem determination, troubleshooting, etc.). • 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. • 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.
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**	1. Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments) 2. SharePoint Online site content and the files stored within that site, and files uploaded to OneDrive for Business 3. Azure Active Directory (Azure AD)

		ESMA's Office 365 services are provisioned in the European Union and stored by Microsoft as data at rest only within the European Union therefore, the contract with Microsoft Ireland does not include any SCC. Nevertheless, such SCCs exist between Microsoft Ireland and Microsoft Corporation. Additionally, the ILA obliges the contractor "to enter into valid SCCs before engaging in any transfer". Microsoft stores some ESMA's Content Data exclusively in the EU. This concerns a subset of content data of the core online services, which Microsoft defines as customer data. Since these servers are located in the EU, the system-generated server logs about the individual use of these Core Services are also processed in the EU. Additionally, Microsoft processes user accounts data in Azure Active Directory (Azure AD) in the EU too. Content data are stored in the data centre where the Azure AD service is running, i.e., in the case of ESMA this means in data centres in the Netherlands and Ireland. System-generated logs related to the Azure AD do not contain personal data such as usernames, phone numbers, or IP addresses. However, the attribute "UserObjectId" which identifies authentication attempts to users can be considered personal data. These logs, and activity reports, are stored in the EU, as well as push notifications from Microsoft Authenticator Application. The customer data can be routed via other locations during the transfer and can also be processed in other regions. In this regard, processing can take place at any location where Microsoft operates (except in China, as this is a separate cloud). This also applies to data replication.

		Additionally, Microsoft will continue to incidentally transfer some personal diagnostic data to the USA for security purposes. Microsoft indicates that the information is pseudonymised and aggregated and that malicious activities on customer' servers and end user devices prior to the transfer, Microsoft can still transfer pseudonymised personal data such as device identifiers and IP addresses to its centralised security monitoring and logs. The information in transit and at rest is protected by Encryption controls. ESMA protects the information at rest from third parties by using its own, dedicated, encryption and decryption keys. The information in transit mainly protected by the trusted Cloud Provider (Microsoft). Moreover, 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. Under exceptional circumstances (such as: e.g., email service incidents, problems, changes or security incidents) access to external ESMA's service providers located within EU boundaries or from third countries can be granted upon prior ESMA's management authorisation, ESMA's approved Data Processors and third parties.
13	**General description of security measures, where possible.**	ESMA has implemented security measures to best address the Data protection as follows: • Strong identification and authentication of user identities (including Second-Factor Authentication);

		• Privileged access management to control administrative accesses and to preserve data confidentiality and integrity; • Security monitoring and auditing enabled on the tenant to ensure early detection of personal data breaches; • File storage in Teams (encryption at rest): ESMA has implemented Customer Key for both SharePoint Online and OneDrive for Business data encryption at rest • Customer Key for the Teams chats and messages; • Access to customer data is given upon prior approval and on discretionary basis (case by case basis) using the feature named "Customer Lockbox" which will be used when technical troubleshooting is needed by third parties with a valid need-to-access, • Teams' governance for O365 groups is deleting Groups/Teams older than 6 months with prior notification to owner. In addition to those measures, the Cloud Provider abides to comply with the EUDPR provisions (Regulation (EU) 1724/2018) as set forth in the EC DIGIT framework contract. Also, the Cloud provider adheres to industry information security and privacy certifications, including but not limited to the 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.
14	**Information on how to exercise your rights to access, rectification, object and data portability (where applicable), including recourse right.**	As a general principle, ESMA only processes personal data for the performance of tasks carried out in the public interest on the basis of its founding regulation and other EU acts under its remit, in the legitimate exercise of official authority vested in ESMA. To fulfil its mission, ESMA uses Microsoft Office 365 Public Cloud as part of its electronic administration services. ESMA leverages collaborative Microsoft Office 365 applications in Europe (hosted and delivered from Europe) to transversally support most of its business processes and business operations, which may include the processing of personal data.

		The main processing operations under the scope of Office 365 which entail personal data processing are the following: video and voice communications, virtual meetings, document processor and editors, electronic email (including calendar items, contact lists, tasks, electronic notes, etc.), electronic file sharing services, electronic document management and user and identity management in the Cloud. Personal Data from ESMA statutory and non-statutory staff, markets stakeholders, third parties and data subjects (e.g., citizens) are strictly processed for the exercise of ESMA's legitimate powers and missions. The information is protected with proportionate, and industry accepted security controls and it is accessed according to a valid and approved business need (including but not limited to enforcing ESMA's own encryption controls to isolate the information from third parties). To achieve these goals, ESMA entrust the processing of the data to Microsoft cloud service provider in Europe, who acts as a data processor for ESMA and under the instructions of ESMA's Controllers. Default Personal data retention periods will vary from application and will be supervised by ESMA's Controllers accordingly. 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 . To exercise your Data Privacy Rights you can address your requests to the Controller at (itdpo@esma.europa.eu). 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. 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. Further information regarding your Data Privacy Rights can be found at: https://www.esma.europa.eu/about-esma/data-protection If you have additional questions or concerns, you can also contact: 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