01 - Title of personal data processing	**Content creation and collaboration by means of Microsoft Office 365 online**
02 - Reference	98
03 - Submission Date	22/03/2021
04 - Last update	
Part A of RECORD of processing activities according to Article 31 Regulation 2018/1725 (publically available)	Please consult the relevant EDPS guideline in your sector, if it exists, or : https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en (this url is not working with Internet Explorer, use Chrome or Firefox).
Controller(s) of data processing operation (Article 31.1(a))	In case of more than one controller, see Article 28.
05 - Name and contact details of controller	
Name of the Controller	RICOTTA Salvatore
Unit responsible for the processing the activity	Resources and Support Unit
Controler's functional mailbox	horsu-office@era.europa.eu
06 - DPO	DataProtectionOfficer@era.europa.eu 120 Rue Marc Lefrancq, 59300 Valenciennes, France Tel. +33 (0) 32 70 96 500
07 - Name, contact details of joint controller (where applicable)	
Who is actually conducting the processing? (Article 31.1(a))	The data is processed by a third party (e.g. contractor) (Art. 29 – Processor)
08 - Name and contact details of processor (where applicable)	For services related to Microsoft Office 365 cloud-based collaboration platform, Microsoft acts as data processor.Contact details: Microsoft Ireland South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland https://docs.microsoft.com/bs-cyrl-ba/compliance/regulatory/gdpr-data-protection-officer
Purpose of the processing (Article 31.1(b))	The reason why the personal data are processed and what is intended to achieve and the underlying reason for the processing. The individual steps used for the processing are described.If there is the need (later on) to further process the data for another purpose, the Data Subject must be informed in advance.

09 - Purpose of processing	as these are not supported by alternative tools or systems. The cloud-based solution Office 365 ("Office 365 platform") provided by Microsoft enables ERA to work on any corporate device and facilitates collaboration with internal and external stakeholders. The Office365 platform distinguishes between the following data categories as defined in detail in section 8: Identification data, Content data, Service generated data, Diagnostic data. 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 Agency, 1. Identification data, Content data, Service generated data, 2. Technical support to IT teams for issues with Office365, 1. Identification data, Service generated data, 3. Prevention, detection and resolution of security events (e.g. cyber-attack), 1. Identification data, Service generated data, 4. Assistance to data subjects in exercising their rights in relation to data processed within Office 365, 1. Identification data, Service generated data. The operation of this platform requires the processing of data categories by ERA, for the following specific purposes: 1. Set-up, configuration and maintenance of Office365 capabilities, 1. Identification data, Service generated data, 2. Administration of the rights allocated to a user account, 1. Identification data, 3. End-user support for issues with Office365, 1. Identification data, Service generated data, Diagnostic data, 4. Prevention, detection and resolution of security events (e.g. cyber-attack), 1. Identification data, Service generated data, 5. Assistance to data subjects in exercising their rights in relation to data processed within Office 365,
Description of data subjects and personal data categories (Article 31.1(c))	Description of the categories of persons affected and which data about them will be processed.
10 - Description of the categories of	

a - data subjects	The following categories of data subjects can be distinguished: Statutory and Non-statutory staff that are enrolled as O365 users.
b - personal data	Related to the provision of the service, ERA or Microsoft process four different categories of data, all of which may include personal data. These categories are: Identification data contains personal data necessary for the proper identification of the user and the corresponding user account, including exhaustively, 1. ERA username, email address and account status, 2. User personal data (title, last name, first name), 3. Function-related data (ERA, unit, office address and telephone number, city, and country). This information is copied to all Microsoft Office 365 data centers as per contract terms used to provide the service that allows global access and access control to the ERA's environment in Office 365. 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. Diagnostic data (also known as telemetry data) is related to the data subjects' usage of office client software. ERA has applied technical measures to disable sharing of diagnostic data with external parties, including Microsoft. 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 will allow to monitor all activity in the cloud environment of each user. To learn which events trigger the creation of service generated data, consult Annex A to the privacy notice.
Retention time (Article 31.1(f))	For how long data is retained and the related justification for this retention period? If appropriate, differentiate between the categories of personal data. If the retention period is unknown, please indicate the criteria for determining it.
11 - Time limit for keeping the data	The Agency keeps personal data for the time necessary to fulfil the purpose of collection or further processing, maintains identification data as long as the user account is activated or if users have not decided to remove or delete personal data from their account. Microsoft, as a processor for Office 365 services, may retain data for Online Services upon expiration of the subscription, i.e. during the 90-day retention period abd subsequent period, up to an additional 90 days.
Recipients of the data (Article 31.1(d))	Recipients are all people to whom the personal data are disclosed (“need to know principle”). Not necessary to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).

12 - Recipients of the data	The recipients of the personal data are: Authorised Agency staff dealing with the provisioning of O365 user accounts, Microsoft's personnel managing the databases on Microsoft cloud servers and their sub-processors' personnel on a need-to-know basis. All recipients of the data are reminded of their obligation not to use the data for any further purpose other than the ones for which they were collected. The personal information collected will not be communicated to third parties. In case there is the need to share your data with third parties, you will be notified with whom your personal data has been shared.
Transfers to third countries or International Organisations (Article 31.1(e))	If the personal data are transferred outside the EU, this needs to be specifically mentioned, since it increases the risks of the processing operation (Article 47).
13 - Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	Yes Transfers of personal data outside the European Union are not foreseen. However, diagnostic data covered by contractual rules may be sent to Microsoft outside EU territory. Transfer subject to appropriate safeguards (Article 48.2 and .3) – Standard data protection clauses as per Inter-Institutional License Agreement signed by the EU Commission and Microsoft. 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 EC. The activities of all sub-processors are in scope of third-party audits.
General description of security measures, where possible (Article 31.1(g))	Please specify where the data are stored (paperwise and/or electronically) during and after the processing. Specify how they are protected ensuring “confidentiality, integrity and availability”. State in particular the “level of security ensured, appropriate to the risk”.

14 - How is data stored? What are the security measures implemented?	All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the Agency's in its premises or alternate site or in Microsoft datacentres in the EU (linked to the Agency's and Commission's Office 365 environment). All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. In order to protect your personal data, the Commission (who represented the Agency in the negotiations with Microsoft) has put in place several strong contractual safeguards, complemented by technical and organizational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorized access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorized persons with a legitimate need to know for the purposes of this processing operation. The Agency is actively configuring customer data location (at rest) of its Office 365 services. Staff mailboxes are encrypted at rest with the Agency's customized keys. Files which are uploaded in Teams, One Drive and SharePoint Online are also encrypted at rest with the Agency's customized keys . The online services the Agency will use are offered from data centres in EU Member States, respectively Ireland, the Netherlands, Austria or Finland. No content data will be stored outside the EU territory. Any log files generated by using Microsoft Office 365 online services can be analysed in the US, and while the Commission (and hence the Agency) cannot technically avoid this, strong contractual safeguards apply to this data. Any data in transit is protected by strong encryption. The Commission (who represented the Agency in the negotiations with Microsoft), has taken legal and technical measures to protect personal data that are transferred outside the EU/EES according to Chapter V of Regulation 2018/1725.
Information/Transparency (Article 14-15)	Information shall be given in a concise, transparent and easily accessible form, using clear and plain language.
15 - For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable) see the data protection notice	The Agency makes available: the privacy notice and information on how data subjects can exercise their rights will be permanently available to data subjects in the M365 environment. In "My account" data subjects can review the privacy policy under the tab "Organization Privacy Statement" together with information on the dedicated functional mailbox for data subject requests. available at the ERA website:
Data subject rights (tick if "Anytime")	Right to have access Right to rectify Right to erase (“right to be forgotten) Right to have recourse
Part B - Compliance check and risk screening (internal) - Compliance check (Articles 4 and 5)	
16 - Legal Basis	FINANCIAL REGULATION OF THE EUROPEAN RAILWAY

17 - Lawfulness of processing	Processing is 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. ERA Financial Regulation adopted by ERA Management Board (Decision n° 206) Article 28 "Performance and principles of economy, efficiency and effectiveness The data processing is considered lawful under art. 5(a), of the Regulation (EC) 2018/1725, because it is 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.
18 - Data minimisation	The user information are kept at the minimum required detail in order to execute the missions.
19 - Accuracy	All the information related to the data subjects are checked and validated against the user accounts notation.
High risk identification	
20 - Threshold assessment, fill in the specific Threshold assessment-Risks entry in sharepoint.	Some risky processing operations require additional safeguards and documentation. Special category of data is considered: 1. data relating to health, (suspected) criminal offences or otherwise considered sensitive ('special data categories'); 2. evaluation, automated decision making or profiling; 3. monitoring data subjects; 4. new technologies that may be considered intrusive. Yes/No, if yes, mention which one from the above it is under field 21 below If any of these data concerned, you need to do a DPIA-see DPIA procedure.
21 - Special category data	No
Part C - Related documents (internal)	
22 - DPIA	DPIA-O365: https://intranet.era.europa.eu/ITFM/ICT%20Management/DPIA%20-%20O365.docx?Web=1
23 - Link to the Threshold assessment-Risks	
24 - Other related documents	