01 - Title of personal data processing	Agency Extranet / Collaboration Space
02 - Reference	35
03 - Submission Date	05/04/2012
04 - Last update	1/20/2023
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	
Controller	RICOTTA Salvatore
Unit-Sector	ITFM
Controller's email	salvatore.ricotta@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)	
08a - Who is actually conducting the processing? (Article 31.1(a))	The data is processed by a third party (e.g. contractor) (Art. 29 - Processor)

08b - 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 Microsoft may use non-Microsoft organizations to help provide Online Services. As a function of their role for Microsoft, a small set of these organizations may process your customer data or personal data, only to deliver the services Microsoft has retained them to provide; they are prohibited from using your data for any other purpose. In accordance with GDPR, Microsoft discloses these subprocessors in advance of their first engagement and provide notification of any changes over time. To obtain Microsoft's disclosure of Online Services Subprocessors, you may locate it within the Microsoft Trust Center located here. The Microsoft Online Services Subprocessor List identifies subprocessors authorized to subprocess customer data or personal data in Microsoft Online Services. This list is applicable for all Microsoft Online Services governed by the Microsoft Data Protection Addendum (which is incorporated by reference in the Microsoft Product Terms) for which Microsoft is a data processor.
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	The Agency Extranet's function is to help facilitate collaboration to support the physical meetings of the parties. It is not intended to simply store documents, as most Agency information is freely available to the general public on its website. The processing operations mentioned above aim at: a) facilitating contacts, consultation, review of work progress, as well as exchange of information and ideas between the Agency and its related stakeholders, and b) managing and organising the planned events, meetings or other activities necessary, including lists for contacts, invitations, distribution of documents, information sharing, surveys, feedback on documents, follow-up actions.
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.

10a - Data Subjects	The above-mentioned access is granted to persons falling under the following categories: a) Members of national authorities, i.e. National Safety Authorities, National Railway Accident Investigation Bodies, ministries or the Representative Bodies representing the railway sector as mentioned in Article 5(3) and 38(4) of the Agency Regulation, nominated/appointed by the respective organisation or entity as “full members” or as “deputy members” of the WG, b) Coordinators of Representative Bodies and NB-Rail – persons nominated by the organisation normally from its permanent staff (not from member companies) for the overview of the Agency activities and the coordination of the activities of the organisation’s representatives in the WPs, c) Staff of the European Commission or bodies thereof, d) Members of the Administrative Board or of its Sub-Committee, e) Independent experts appointed according to Article 5(2) of the Agency Regulation, f) Other entities or individuals, as “specific cases”, on the authority of the Head of Unit responsible for the respective WG or the Executive Director. In addition, “closed” ERA Extranet sites may be created under the authority of the Heads of Units for particular purposes (e.g.: agreed confidentiality). In that case, the Head of Unit of the Chairman of this restricted area must indicate (in written and, also, in case of changes): a) the roles of the persons (internal and external) involved in that particular activity and b) a substantial justification (why).
10b - Personal data	First name, last name, E-mail Address, Company/Organisation, Sector, Job Title, Professional Address, City, Postal Code, Country, Business Phone Number, Fax Number, Office, Username.
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 and 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: ERA staff having access to the ERA Extranet, WG Members that have signed a "Non-Disclosure Agreement", 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.
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	a) All information regarding the protection, access, verification, modification or deletion/blocking of personal data is included in the Privacy Statement, contained in the Extranet's front page (https://extranet.era.europa.eu/). For all external data subjects involved, the relevant information is provided through a non-disclosure agreement (see Annex 1 attached) b) Data subjects may exercise their rights via e-mail by contacting the ERA Service Desk (servicedesk@era.europa.eu).
15a - Data subject rights	Right to have access Right to rectify Right to erase ("right to be forgotten") Right to have recourse
16 - Legal Basis	ERA Annual Work Programme, ERA Multi-Annual Work Programme (2014-2017)
17 - Lawfulness of processing	Article 5 a) of Regulation (EU) 2018/1725 The processing operations of personal data in the context of the Agency Extranet for experts' networks, workgroups and task forces are necessary for the performance of tasks carried out on the basis of the Agency Regulation.
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.

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	