01 - Title of personal data processing	Organisation Codes Register (OCR)
02 - Reference	101
03 - Submission Date	15/11/2021
04 - Last update	30/10/2021
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	GIGANTINO Anna
Unit responsible for the processing the activity	Analysis and Monitoring Unit
Controler's functional mailbox	AOD.aam@era.europa.eu
06 - DPO	Zografia Pyloridou 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 cloud-based services related to Microsoft Azure Active Directory, 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 In compliance with the terms of the Art. 27 of the GDPR, Microsoft Ireland Operations Limited is Microsoft's representative in the European Union that offers customer support through Microsoft's Privacy web form, located at http://go.microsoft.com/?linkid=9846224. The Microsoft Data Protection Officer is Mr Steve May.

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	Through the OCR, the Agency is creating, allocating and providing public access to the Organisations' code to access its registers and databases. Free access to OCR is granted to public to read data, while a username and a password are needed for data submission. Therefore, a registration of personal data is requested through the Stakeholder Relations Management (SRM) tool, in order to get an authorised access and to be contacted in case of any need (for further details see the relevant privacy notice, available on the Agency website).
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	Railway Undertakings (RUs) and ERA staff respectevely requested of: submitting OC request; validating submitted request.
b - personal data	The collected personal data for the Stakeholders (defined as "Guest") account type are the following: Identity • Name ("Last name" + "First name") • User Principal Name (The UPN is the login ID for the user and equivalent to the email of the contact info) • User type ("Member") • Object ID (system string) • Issuer (based on Microsoft notation) • Account creation time • Account last sign-in date Contact info • Email • Alternate email • Proxy address
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	Personal data for the ”Guest” account type is retained as follows: As long as users are recorded as active. If the user is registered through a third party, the period of activity will usually correspond to a contractual link with that party, but the Agency will consider the user active if it continues to receive user’s information (in the case of an automatic link) or until user’s account expires. After the expiration date, data is kept › in the Azure Active Directory for a period of 30 days, before its deletion, › 6 months after the deletion in logs and back-up media. Azure AD general service provisions At the expiration of the subscribed services, two consecutive and different 90 days periods apply: - A first 90 days period start at expiration. During this period data are still available for the ERA to download the data. This period is intended to give some extra time to the customer should it had not already downloaded all data it wants to keep at the expiration. - A second 90 days period starts right at the end of the first 90 days during which Microsoft will be deleting all the copies of the data. At the end of this second period (so 180 days after the expiration of the subscription) all the data shall have been deleted. It applies regardless of the location of the data, so if data are duplicated in several locations, all copies in all these locations shall be deleted. These data deletion processes are audited yearly as part of our compliance with ISO27018. In case of incident the data will be kept for analysis for a longer period to establish evidence or to defend a right in a legal claim pending before a court.
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	1. Agency staff involved in the related service and administration, operation and troubleshooting of the application. 2. 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. Microsoft Corporation, as processor, is committed under the terms of the Interinstitutional License Agreement and related documents to respect the obligations of the GDPR. The nature and the purpose of the processing is related to the provision of the Online Service pursuant to Customer's volume licensing agreement.
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?	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?	Free access to OCR is granted to public to read data, while a username and a password are needed for data submission. Therefore, a registration of personal data is requested to obtain credentials in order to get an authorised access. All personal data are processed only by designated staff and stored on Microsoft cloud servers located in Europe, which abide by the ERA’s IT security rules and standards, 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. For more information about the ERA Authentication Service (EAS) allowing the authenticated users to have access to the ICT resources in a manner that ensures the confidentiality, integrity and availability of the information assets please refer to the Azure Active Directory relevant record in this register (74).
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	
Data subject rights (tick if "Anytime")	Right to have access Right to rectify
Part B - Compliance check and risk screening (internal) - Compliance check (Articles 4 and 5)	
16 - Legal Basis	Commission Implementing Decision (EU) 2018/1614 laying down specifications for the vehicle registers
17 - Lawfulness of processing	The processing is lawful under Art. 5(a) of Regulation EU 2018/1725 repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC: Processing is necessary for the performance of a task carried out in the public interest.
18 - Data minimisation	Free access to OCR is granted to public to read data. The mandatory personal data are those collected just to allow registered users to request a code for their organisation to access ERA registers and databases (including OSS).

19 - Accuracy	For data submission users provide the needed data.
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	NA
Part C - Related documents (internal)	
22 - DPIA	NA
23 - Link to the Threshold assessment-Risks	
24 - Other related documents	Privacy notice on Agency website (https://www.era.europa.eu/content/data-protection)