01 - Title of personal data processing	**SINGLE RULES DATABASE (SRD)**
02 - Reference	95
03 - Submission Date	19/10/2020
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	GIGANTINO Anna
Unit responsible for the processing the activity	Analysis and Monitoring Unit
Controler's functional mailbox	AOD.aam@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 ERA (responsible unit) itself
08 - Name and contact details of processor (where applicable)	
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 processing of personal data in the SRD is needed to enable certain functionalities regarding notifying countries', ERA's, EC's or EFTA's tasks fulfillment. Particularly, credentials (username and password) are required to upload, edit, draft and notify national rules, reply to assessment results submitted by ERA, communicate with the Agency and EC/EFTA, manage SRD users, reference data, examination and assessment results of national rules, validation of national rules of notifying countries and communicate with them concerning a specific national rule.

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	Authorised staff from notifying countries (namely EU Member States, Norway, Switzerland) Authorised staff from ERA, EC and the European Free Trade Association (EFTA).
b - personal data	Family name Name E-mail Address In addition, in order to protect the content against inappropriate behaviors (e.g. Hacking attempts) an Audit Trail has been implemented, recording logged-in users' actions: * Timestamp * Username * Source IP address * Action details. Finally, regarding "first-party cookies", every time users visit SRD, they will be prompted to accept cookies or to modify settings, in order to: not be tracked by your browser (for analytics services, advertising networks, etc.) and/or opt-out from analytics data collection (for further details read Web analytics privacy in Matomo).
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 information is retained until the user account is deleted or for the lifetime of SRD, designed as a permanent tool - until the relevant legislation is changed.
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. Designated Member State staff for the purposes of registering and submitting national rules originating from their Member State and Switzerland, as well as accepting or rejecting the examination results or official opinions submitted by ERA; 2. Designated ERA staff for the purposes of assigning, assessing and submitting their examination results or their official opinions on the national rules; 3. Designated European Commission staff for the purposes of validating and submitting their validation results for the national rules originating from a EU Member State; 4. Designated EFTA staff for the purposes of validating and submitting their validation results for the national rules originating from Norway; 5. Designated ERA staff for the purposes of administration, operation and troubleshooting of the application.
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?	Personal data is not intended to be transferred to any third country outside the EU.
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 are processed only by designated staff and stored on servers in ERA premises which abide by the ERA’s IT security rules and standards. 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) and privacy notice (https://intranet.era.europa.eu/Data-Protection/Lists/Records/Attachments/77/Privacy%20Statement%20-%20Azure%20Active%20Directory.pdf)
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 Right to erase (“right to be forgotten) Right to restrict of processing Right to data portability Right to object
Part B - Compliance check and risk screening (internal) - Compliance check (Articles 4 and 5)	
16 - Legal Basis	Article 27 of Regulation (EU) 2016/796 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Railways and repealing Regulation (EC) No 881/2004
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: ((a) 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).
18 - Data minimisation	Free access to SRD is granted to public to read data. The mandatory personal data (namely Family name, first name and e-mail) are collected to allow registered users to submit, draft, national rules and communicate with ERA, EC etc.
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	None
Part C - Related documents (internal)	
22 - DPIA	None
23 - Link to the Threshold assessment-Risks	
24 - Other related documents	