

<b>01 - Title of personal data processing</b>	<b>SYSPER II</b>
02 - Reference	100
03 - Submission Date	10/06/2021
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 : <a href="https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en">https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en</a> (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	HoUResourcesandSupport@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)	European Commission Directorate HR.A
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	<p>ERA is phasing out the current e-HR database and preparing the migration to the SYSPER II EC system. ERA personal data shall be stored in the COMREF/RETO/NAP databases</p> <p>The SYSPER Interinstitutional programme supports the EU Organisations in managing and protecting personal data processed in the context of onboarding and using SYSPER.</p> <p>The Commission, as the system owner of SYSPER, collects and processes personal data in accordance with the Internal Data Protection Regulation (IDPR) – Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the European Union institutions, bodies, offices and agencies and on the free movement of such data.</p> <p>Furthermore, in terms of data protection, the DG HR SLA identifies the EU Organisation as the Data Controller and the Commission as the Data Processor pursuant to Regulation (EU) 2018/1725.</p>
----------------------------	---

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	<p>All ERA staff (Temporary and Contract agents, active and non-active)</p> <p>Trainees (active and non-active)</p> <p>Seconded National Experts (SNE) (active and non-active)</p>
-------------------	--

b - personal data	<p>All personal data related to the data subjects and their relatives (past and present)</p> <p>In order to carry out this processing operation, Directorate HR.A may collect and use the data available in SYSPER (e.g., personal, organisational, career, family composition) that concern Commission staff and other persons which are related to the Commission through their professional activity, directly or indirectly, but collaborate with the Commission outside the context of an employment contract with the Commission (including seconded national experts, trainees, and service providers working in the Commission premises), and persons related to them. This statement covers personal data used for general / horizontal processing in SYSPER. This data consist of: • personal identification number (perid); • job number; • organizational entity and activities in relation to the Commission priorities; • logs of persons to SYSPER;</p>
-------------------	--

Retention time (Article 31.1(f))	<p>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.</p>
----------------------------------	---

11 - Time limit for keeping the data	Personal identification numbers (perid) is kept during the whole active career, its breaks and also in post-activity. Information on roles, access rights, organisational entity and activities according to Commission priorities are kept for each assignment during the active career. Logs are kept for 10 years.
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	at ERA: Executive Director, Middle-managers, HR staff members, IT staff for technical support at EC: DG HR, PMO, DIGIT, IDOC all audit authorities: OLAF, IAS, ECA, external auditors
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?	No
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 on the servers of the European Commission. 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 has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised 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 authorised persons with a legitimate need to know for the purposes of this processing operation.
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

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability. You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a) and 5(1)(b) on grounds relating to your particular situation. You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading 7 below. Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 8 below) in your request.

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

Agency Regulation (EU) 2016/796Staff Regulations and CEOS and implementing Rules

17 - Lawfulness of processing	<p>Based on Article 5(1) of the Regulation 2018/1725 processing of personal data is necessary:</p> <ul style="list-style-type: none"> <li>• 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;</li> <li>• For the compliance with a legal obligation to which the controller is subject;</li> <li>• Further processing, for example for 'statistical purposes', may also be possible in line with articles 4 &amp; 6 of the Regulation 2018/1725.</li> </ul> <p>The legal bases are:</p> <ul style="list-style-type: none"> <li>• Staff Regulations of Officials of the European Communities, the Conditions of Employment of other servants of the European Communities;</li> <li>• Commission Decisions 2017/46 and 2017/8841 on the security of communication and information systems in the European Commission, especially Article 9, to fulfil our obligations as a system owner of SYSPER used to process your HR data; version 15/07/2020</li> <li>• Legal acts such as: the rules on the secondment of national experts to the Commission, as well as other legal instruments (including the Rules governing the official traineeships scheme of the European Commission);</li> <li>• the general requirements for the execution of these regulations, and the internal management rules followed by the services of the Commission while executing the tasks delegated to them;</li> <li>• administrative notices.</li> </ul>
18 - Data minimisation	All data needed to identify rights and entitlements for staff/trainees/SNE (past and present)
19 - Accuracy	All data is checked by DG HR/PMO/DIGIT
High risk identification	
20 - Threshold assessment, fill in the specific Threshold assessment-Risks entry in sharepoint.	<p>Some risky processing operations require additional safeguards and documentation.</p> <p>Special category of data is considered:</p> <ol style="list-style-type: none"> <li>1. data relating to health, (suspected) criminal offences or otherwise considered sensitive ('special data categories');</li> <li>2. evaluation, automated decision making or profiling;</li> <li>3. monitoring data subjects;</li> <li>4. new technologies that may be considered intrusive.</li> </ol> <p>Yes/No, if yes, mention which one from the above it is under field 21 below</p> <p>If any of these data concerned, you need to do a DPIA-see DPIA procedure.</p>
21 - Special category data	NA
Part C - Related documents (internal)	
22 - DPIA	NA

23 - Link to the Threshold assessment-  
Risks

24 - Other related documents

SYSPER II Privacy Notice: [https://myintracomm.ec.europa.eu/staff/Documents/technical-assistance/PS-SYSPER\\_generic.pdf](https://myintracomm.ec.europa.eu/staff/Documents/technical-assistance/PS-SYSPER_generic.pdf)