EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

RECORD OF PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 REGULATION 2018/1725[1] NOTIFICATION TO THE DATA PROTECTION OFFICER

NAME OF PROCESSING OPERATION[2]: Use of SYSPER for FRA staff.

DPR-2019-063
Creation date of this record: 11/03/2019
Last update of this record: 14/06/2021
Version: 2

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: European Union Agency for Fundamental Rights (FRA) Schwarzenbergplatz 11, A-1040 Vienna, Austria Telephone: +43 1 580 30 – 0 Organisational unit **responsible**[4] for the processing activity: Corporate Services Contact: FRA-SYSPER@fra.europa.eu Data Protection Officer (DPO): dpo@fra.europa.eu)

2) Who is actually conducting the processing? (Article 31.1(a))[5]	
The data is processed by the FRA itself	☒
The data is processed also by third parties (contractor) European Commission Directorate-General for Human Resources and Security (HR-MAIL-A3@ec.europa.eu)	☒

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

2 **Personal data** is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.
Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 In case of more than one controller (e.g. joint FRA research), all controllers need to be listed here

4 This is the unit that decides that the processing takes place and why.

5 Is the FRA itself conducting the processing? Or has a provider been contracted?

European Commission Directorate-General for Informatics (DIGIT-COMREF@ec.europa.eu)

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).

The purpose of the processing operation via Sysper (HR tool managed by the European Commission) in the Agency is mainly the following:

1. To identify all staff in the Agency ("Identity Management" module);
2. To support processes of human resources management:
    a. Organisation Management modules: "Organisation Chart" and "Job Quota Management", which enable the institution to define all entities in the hierarchical structure in their organistion and then to manage the jobs within, ensuring that the quotas stipulated in the staff establishment plan are respected;
    b. Personal Data Management modules: "Employee Personal Data" (enabling personnel to view their personal data) and "Adress Declaration" (allowing staff to directly manage changes to their personal address details);
    c. Talent Management modules: core "Career Management" enabling the encoding of main career events as well as managing present and historical career data, "Basic Job Description", "Vacancy" and "Managers Vacancy";
    d. Time Management modules
    e. Document Management module: "Generation of Certificates" covering the management and production of official standard documents (e.g. certificate of employment, etc.).
    f. Report on roles and access rights: Allows checking regularly SYSPER roles (except staff role) and the associated job numbers and staff members. The report will also include technical jobs and will allow monitoring anyone who has access to our data and eventually ask for corrections or clarifications.
    g. Transfer information related to staff to the MiPS (mission management) system, owned by the PMO. This includes contact details, bank account

as well as the reporting officer who will be responsible for the approval of mission requests.

4) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are being processed?

FRA staff (including SNEs) ☒

Non-FRA staff ☐

5) Categories of personal data processed (Article 31.1(c))

Please tick all that apply and give details where appropriate. Include information if automated decision making takes place, evaluation and monitoring

(a) **General personal data:**
The personal data contains:

Personal details (*e.g. name, surname, date of birth, gender, nationality, address, photo, ID copy, social security certificate, medical certificate, military/civil Certificate, criminal record, marital status, officially recognised partnerhship, birth certificates of dependent children,*) ☒

Contact details (*e.g. postal address, email address, mobile and fax number*) ☒

Education & Training details, including language skills ☒

Employment details (*e.g. work experience , prior professional assesments, duration of contract, years of service, grade, category, job title and description, sick leave information etc.*)
☒

Financial details (*e.g. financial identification form, bank account information*) ☒

Family, lifestyle and social circumstances ☒

Goods or services provided ☐

Other (please give details): *Includes employment related data like grade, category, duration of contract, years of services, job description, job title.*

(b) **Sensitive personal data** (Article 10)
The personal data reveals:

Racial or ethnic origin ☐

Political opinions ☐

Religious or philosophical beliefs	☐
Trade union membership	☐
Genetic, biometric or data concerning health	☐
Information regarding an individual's sex life or sexual orientation	☐

6) Recipient(s) of the data (Article 31.1 (d))[6]

*Recipients are all parties who have access to the personal data. Who will have access to the data **within** FRA? Who will have access to the data **outside** FRA?*

Each FRA staff member will have access to their own personal data. ☒

Designated **FRA** staff members will also have access to the personal data (please specify which team and Unit) ☒

- Head of Corporate Services Unit;
- limited staff of Human Resources Management team;
  staff in operational services to the specific data they need to fulfil their human resources management tasks like hierarchical superiors;
- all other persons designated via delegation by one of the users.

Designated persons **outside** FRA: (please specify) ☒

- HR staff responsible for administrating SYSPER in DG HR as well as developers and helpdesk in DG DIGIT who need those data to solve bugs, to test new developments or for user research and usability tests.
- IT professionals in DIGIT, HR and PMO.
- Data receipients in charge of managing MIPS (Commission's mission management system).
- The information could be transferred to other institutions for example in the case of an inter-institutional transfer of staff in order to facilitate the human resources management in the other institution.
- Data can also be transferred for specific purposes of control to the auditing or inquiring bodies like the Internal Audit of the European Commission, OLAF or the Court of Auditors, EDPS, etc. in respect of the provisions of the Regulation (EU) 2018/1725.

7) Transfers to third countries or recipients outside the EEA (Article 31.1 (e))[7]

[6] No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).

[7] **Processo**r in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards.

If the personal data are transferred outside the European Economic Area, this needs to be specifically mentioned, since it increases the risks of the processing operation.

Transfer outside of the EU or EEA
Data are transferred to third country recipients:

Yes ☐

No ☒

Transfer to international organisation(s)

Yes ☐

No ☒

If yes specify to which organisation:

Legal base for the data transfer

☐ Transfer on the basis of the European Commission's adequacy decision (Article 47)

☐ Transfer subject to appropriate safeguards (Article 48.2 and .3), specify:

a) ☐ A legally binding and enforceable instrument between public authorities or bodies.
Standard data protection clauses, adopted by
b) ☐ the Commission, or
c) ☐ the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2) .
d) ☐Binding corporate rules, ☐ Codes of conduct , ☐ Certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

Subject to the authorisation from the European Data Protection Supervisor:
☐ Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.

☐ Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

☐ Transfer based on an international agreement (Article 49), specify:

Derogations for specific situations (Article 50.1 (a) –(g))

☐ N /A
☐ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply
In the absence of an adequacy decision, or of appropriate safeguards, transfer of personal data to a third country or an international organisation is based on the following condition(s):

☐ (a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
☐ (b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
☐ (c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
☐ (d) The transfer is necessary for important reasons of public interest
☐ (e) The transfer is necessary for the establishment, exercise or defense of legal claims
☐ (f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
☐ (g) The transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case

8) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Please indicate the starting point and differentiate between categories of persons or data where needed (e.g. in selection procedures candidates who made it onto the reserve list vs. those who didn`t). Are the data limited according to the adage "as long as necessary, as short as possible"?

The retention duration is administered by the owner of the system, namely: DG HR. The data will be stored for different periods depending on the related HR process. Most of the personal data will be retained so long as the owner is working for the EU. In some cases, some data might be retained longer, when a staff member is in pension for instance, etc. The Agency has no power to modify this. The only actions that can be undertaken by the HR administrators of the Agency are to create, modify, or correct data. The Agency cannot delete an individual profile entirely. Retention periods are in accordance with the document management filing plan retention periods.
For more detailed information on the retention for every category of personal data, please see the European Commission's Sysper Record of Processing Activity.

9) Technical and organisational security measures (Article 31.1(g))

Please specify where/how the data are stored during and after the processing; please describe the security measures taken by FRA or by the contractor

How is the data stored?

Document Management System (DMS)	☐
FRA network shared drive	☐
Outlook Folder(s)	☐

CRM	☐
Hardcopy file	☒
Cloud (give details, *e.g. cloud provider*)	☐
Servers of external provider	☒

Other (please specify):
The data is stored by DIGIT in accordance with the SLA provisions which are aligned with the DP regulations.

10) Exercising the rights of the data subject (Article 14 (2))

How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react?

See further details in the privacy notice: e-mail to FRA-SYSPER@fra.europa.eu

Data subject rights

☒ Right of access

☒ Right to rectification

☒ Right to erasure (right to be forgotten) – the data subject can request to delete the data when the personal data are no longer necessary for the purposes for which they were collected.

☒ Right to restriction of processing

☒ Right to data portability

☒ Right to object

☒ Notification obligation regarding rectification or erasure of personal data or restriction of processing

☒ Right to have recourse

☐ Right to withdraw consent at any time