

Use of SYSPER at FRA

The European Union Agency for Fundamental Rights (FRA) processes the personal data of a natural person in compliance with Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

This data protection notice explains FRA's policies and practices regarding its collection and use of your personal data, and sets forth your privacy rights. We recognise that information privacy is an ongoing responsibility, and we will update this notice where necessary.

1. [Why do we process personal data?](#)
2. [What kind of personal data does the Agency process?](#)
3. [How do we process your personal data?](#)
4. [Who is responsible for the processing your personal data?](#)
5. [Which is the legal basis for this processing operation?](#)
6. [Who can see your data](#)
7. [Do we share your data with other organisations?](#)
8. [Do we intend to transfer your personal data to Third Countries/International Organizations](#)
9. [When will we start the processing operation?](#)
10. [How long do we keep your data?](#)
11. [How can you control your data?](#)
 - 11.1. [Your data protection rights](#)
12. [What security measures are taken to safeguard your personal data?](#)
13. [What can you do in the event of a problem?](#)
14. [How do we update our data protection notice?](#)

1. Why do we process personal data?

The purpose of the processing operation of personal data of FRA post-holders via SYSPER (HR tool managed by the European Commission) is to support the effective management of HR-related information in order to fulfill necessary HR processes in compliance with the Staff Regulations, CEOS and general implementing provisions.

Currently, the following modules and functions of SYSPER are available at FRA. All modules are applicable for statutory staff; only limited functions are in use for SNEs and trainees:

- a. **Organisation Management modules:** ORG (organisation chart) and DOT (job quota management), which enable FRA to define all entities in the hierarchical structure in their organisation and then to manage the jobs within those entities, ensuring that the quotas stipulated in the staff establishment plan are respected;
- b. **Personal Data Management modules:** PER/FAM enabling post-holders to view their personal data and to directly declare changes to their personal and family situation that may have an impact on their entitlements;
- c. **Talent Management modules:** enabling the encoding of career events such as step increases, reclassification, internal moves as well as managing present and historical career data (CAR), management of job descriptions (JIS), management of probationary reports (STAGE);
- d. **Time Management modules:** TIM, ATS, FLEX for encoding working hours, management of absences and leave rights, work patterns (parental, family leave, part-time), teleworking, recording of presence hours within the framework of flexible working hours, management of overtime, shifts and standby duty.
- e. **Document Management module:** DOC covering the management and production of official documents (e.g. certificate of employment, etc.).
- f. **Ethics module:** ETHICS to manage ethics-related requests such as declarations of occupation of a spouse/partner, requests for outside activities, requests to publish, declarations in case of a conflict of interest;
- g. **HR Reporting:** Data extracted from the above-mentioned modules organised in a structured format, which can be filtered, sorted, etc.;
- h. **Personal file:** Personal file data coming from NDP, available for each statutory staff member to consult their own data.
- i. **Report on roles and access rights:** Allows checking SYSPER roles (and the associated job numbers and staff members, monitoring and amendment of who has access to the data.
- j. **Transfer information related to staff to 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.

k. **Transfer information related to staff members to HAN system** (Commission's document archiving and record management system) of the following metadata to ensure the proper functioning of HAN:

1. Organizations :
 - Internal ID
 - Acronym names
 - Description names
 - Parent Internal ID
2. Users
 - Internal Person ID
 - ECAS ID
 - Email address
 - Display family name
 - Display first name
 - User assignment (unit, sectors, etc.)
 - Type job (e.g. AFF, DIS, FF, etc.)
 - Administrative position (e.g. DSN, CSR, etc.)

SYSPER does not cover recruitment processes at FRA. FRA uses an eRecruitment tool covered by a separate data protection record to manage its recruitment procedures, which has no connection to SYSPER. Data gathered in the eRecruitment tool is manually input in SYSPER once a successful applicant becomes a staff member, SNE or trainee.

Data interaction with NAP system: SYSPER data related to entitlements that lead to a change in pay will be sent directly to NAP (New Accounting Platform) after the SYSPER verification process of said entitlements is completed.

2. What kind of personal data does the Agency process?

We will collect only the following personal data necessary for the processing operation described above.

(a) General personal data:

- Personal details (name, surname, date and place of birth, gender, nationalities, marital status, officially recognised partnership ((including divorced or legally separated partners) with the names and dates of birth of the spouse/partner, names and dates of birth of dependent children)
- Contact details (postal address, current and former, also of dependents, email address, mobile number, emergency contact. In case of leave spent away from the place of employment, contact details (address and phone number) at the place of leave may be provided)
- Education & Training details, registered EU language only
- Employment details (type of contract, duration of contracts, grade and step, work schedules and absences, outcome of probation assessment, resignation file. In case of requests for outside

activities, or to publish works, or declarations of occupation of a spouse/partner then relevant information linked to that professional activity will be processed)

- Financial details (bank account information, salary information/payslips, declarations linked to previous employment in case of transferring pension rights)
- Family, lifestyle and social circumstances (as it relates to family composition, absences linked to family events and declarations concerning financial or family benefits that impact entitlements)
- Other:
 - Internal person ID
 - ECAS ID

(b) Special categories of personal data:

- Data concerning health (dates of sick leave, special leave due to illnesses of family members and periods of invalidity are recorded but no medical certificates of medical diagnoses/information should be stored in SYSPER)
- Information regarding an individual's sex life or sexual orientation might be revealed if a spousal/partnership relationship is declared

Neither the medical files nor the disciplinary files are integrated in Sysper.

3. How do we process your personal data?

You provide us the personal data, following the employment contract between the Agency and the staff member. Some personal data are encoded by the designated FRA staff members in the HR function and other is encoded directly by the staff member.

4. Who is responsible for the processing of your personal data?

The Agency (controller) is the legal entity responsible for the processing of your personal data and determines the objective of this processing activity. The Head of Administration is responsible for this processing operation.

5. Which is the legal basis for this processing operation?

Processing personal data in SYSPER is necessary for the management and functioning of the Agency. Article 24 of FRA's Founding Regulation (EC) No. 168/2007 establishing the European Union Agency for Fundamental Rights, as amended by Regulation (EU) 2022/555 (the amended founding Regulation), provides that the staff of FRA are subject to the Staff Regulations of Officials and the Conditions of Employment of Other Servants (CEOS). The processing of the personal data that is handled in SYSPER is required in order to fulfil the rights and obligations set out in the Staff Regulations and CEOS. Therefore, the processing is lawful under Article 5(1)(a) of the Regulation (EU) 2018/1725.

Moreover, the processing of personal data is necessary to effect the employment contract entered into between FRA and the data subject, including establishment in post, grading, career evolution and

processing of financial entitlements. Therefore, the processing is necessary under Article 5(1)(a) of the Regulation (EU) 2018/1725.

The processing of special categories of data is further based on Article 10(2)(b) of Regulation (EU) 2018/1725. Specifically, the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

6. Who can see your data?

Each FRA post-holder will have access to their own personal data

Designated FRA staff members will also have access to the personal data, as follows:

- Designated staff members (TA/CA) in the HR function and the Head of Unit Administration, in accordance with their area of work will have access to relevant modules of SYSPER required for the performance of their duties
- Line managers performing line management and leave approval duties and the Director as Appointing Authority have access to the specific data they need to fulfil those tasks e.g. to review and approve leave and telework requests, to validate timesheets, to complete probation reports
- Any other staff member designated via delegation own rights by one of the users will have access according to the delegation. At FRA, the policy is that if a leave manager is absent for a prolonged period the role can only be delegated to a(nother) Head of Unit.
- The staff member assigned the role of SYSPER Admin has certain access to the system for the extent required to manage access rights.

Designated persons outside FRA as follows:

- HR staff responsible for administrating SYSPER in DG HR as well as developers and helpdesk in DG DIGIT, HR and PMO who need those data to solve bugs, to test new developments or for user research and usability tests.
- Data recipients in charge of managing HAN system (Commission's document record and archiving system).

7. Do we share your data with other organisations?

The information is transferred to other institutions for example in the case of transfer of staff to another EU entity following recruitment 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.

In case that we need to share your data with other third parties, you will be notified to whom your personal data has been shared with.

8. Do we intend to transfer your personal data to Third Countries/International Organizations?

No.

9. When will we start the processing operation?

The processing operation started as of April 2019, when import exercise to Sysper has commenced.

10. How long do we keep your data?

The retention periods for data in SYSPER are set at the level of DG HR as owner and administrator of the SYSPER system. The retention periods are the same for all agencies and the Commission and FRA does not have the possibility to adjust them.

The data will be stored for different periods depending on the related HR process.

General retention principle: In general, personal data in SYSPER is stored until the end of the staff member's activity working for the EU (though after the end of their employment at FRA, only a limited portion of this data remains visible to FRA; the rest is available to the next EU employer in case of further employment or to PMO in case of retirement, invalidity or receiving EU unemployment allowance). Data related to subsisting rights and obligations need to be conserved for a longer period. The Commission Common Level Retention List specifies the duration for each type of data (at present, data linked to subsisting rights has a retention period of 8 years after the expiry of all rights of the staff concerned and of any dependents, and for at least 120 years after the date of birth of the person concerned).

For more detailed information on the retention for every category of personal data, please see the European Commission's [Sysper Record of Processing Activity](#) and records cited.

11. How can you control your data?

Under Regulation 2018/1725, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information. You are not required to pay any charges for exercising your rights except in cases where the requests are manifestly unfounded or excessive, in particular because of their repetitive character.

We will reply to your request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

You can exercise your rights described below by sending an email request to FRA-SYSPER@fra.europa.eu

11.1. The value of your consent

Since the use of SYSPER is mandatory in accordance with the FRA's adherence to the DG HR information management system, you are not required to provide your consent.

11.2. Your data protection rights

a) Can you access your data?

You have the right to receive information on whether we process your personal data or not, the purposes of the processing, the categories of personal data concerned, any recipients to whom the personal data have been disclosed and their storage period. Furthermore, you can have access to such data, as well as obtain copies of your data undergoing processing.

b) Can you modify your data?

You have the right to ask us to rectify your data you think is inaccurate or incomplete at any time.

c) Can you restrict us from processing your data?

You have the right to block the processing of your personal data. If you do, we can no longer process them, but we can still store them. In some exceptional cases, we will still be able to use them (e.g. with your consent or for legal claims). You have this right in a few different situations: when you contest the accuracy of your personal data, when the Agency no longer needs the data for completing its tasks, when the processing activity is unlawful, and finally, when you have exercised your right to object.

d) Can you delete your data?

You have the right to ask us to delete your data when the personal data are no longer necessary for the purposes for which they were collected, when you have withdrawn your consent or when the processing activity is unlawful. In certain occasions we will have to erase your data in order to comply with a legal obligation to which we are subject.

We will notify to each recipient to whom your personal data have been disclosed of any rectification or erasure of personal data or restriction of processing carried out in accordance with the above rights unless this proves impossible or involves disproportionate effort from our side.

e) Are you entitled to data portability?

Data portability is a right guaranteed under Regulation 2018/1725 and consists in the right to have your personal data transmitted to you or directly to another controller of your choice.

In this case, this does not apply for two reasons: 1) in order for this right to be guaranteed, the processing should be based on automated means, however we do not base our processing on any automated means;

II) this processing operation is carried out in the public interest, which is an exception to the right to data portability in the Regulation.

f) Do you have the right to object?

When the legal base of the 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” which is the case in most of our processing operations, you have the right to object to the processing. In case you object, we have to stop the processing of your personal data, unless we demonstrate a compelling reason that can override your objection.

g) Do we do automated decision making, including profiling?

No.

12. What security measures are taken to safeguard your personal data?

The Agency has several security controls in place to protect your personal data from unauthorised access, use or disclosure.

The data is stored by DIGIT in accordance with the SLA provisions which are aligned with the DP regulations. The data are stored at the Commission's Computing Centre in Luxembourg and are therefore protected by the numerous security measures implemented by the Directorate-General for Informatics to protect the integrity and confidentiality of the Institution's electronic assets. The European Commission's datacentre compliance includes the following certifications: ISO 27001, 14001, ISO 22301, ISO 50001, ISO 9001, PCI DSS, PFS, Tier Rating Compliant : Tier IV, Uptime Institute rating: Tier IV.

Access to personal data is protected by the management of access rights which are strictly limited to the principle of "need to know", according to the tasks assigned to access holders. The login and password are managed by the European Commission's Common Authentication Services (EU Login). Accesses, as well as any modifications performed on the data, are logged to ensure traceability of these actions. These logs include who modified the data, when, and what modifications were done, including previous values and new values.

For more information on the security measures adopted by the Commission see the Commission decision on the security of communication and information systems in the European Commission: [EUR-Lex - 32017D0046 - EN - EUR-Lex \(europa.eu\)](#).

13. What can you do in the event of a problem?

a) The first step is to notify the Agency by sending an email to HR@fra.europa.eu and ask us to take action.

b) The second step, if you obtain no reply from us or if you are not satisfied with it, contact our data protection officer (DPO) at dpo@fra.europa.eu.

c) At any time you can lodge a complaint with the EDPS at https://www.edps.europa.eu/data-protection/our-role-supervisor/complaints_en, who will examine your request and adopt the necessary measures.

14. How do we update our data protection notice?

We keep our data protection notice under regular review to make sure it is up to date and accurate.

END OF DOCUMENT