Ref. Ares(2026)10226702 - 30/10/2026

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

DATA PROTECTION NOTICE

Management of personal files

The European Union Agency for Fundamental Rights (FRA or Agency) 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 collect and process your personal data?
4. Who is responsible for 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. Do we need your consent?
    - 11.2. Your data protection rights
12. What security measure 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 is to enable the management and consultation of the FRA staff members' personal files in accordance with Article 26 of the Staff Regulations, applicable by analogy to temporary staff and contract staff on the basis of Articles 11 and 81 of the Conditions of Employment of Other Servants of the European Union (CEOS).

The personal file includes all documents concerning the administrative status and all reports relating to the staff members' ability, efficiency and conduct, as well as any comments by the staff member on such documents. The documents contained in the personal file are used to determine the rights of the data subjects, manage their contracts of employment and represent an overall view of the working relationship with FRA.

FRA will process personal files via the application Digital Numérisation des Dossiers Personnels (NDP). Data from the NDP application will be transmitted to SYSPER, where staff members can freely consult their own personal file electronically. Some information available in the staff member's digital personal file comes directly from the relevant SYSPER module, e.g. the probation report is drawn up in the SYSPER STAGE module and accessible to staff, ethics declarations are processed directly in SYSPER etc. – this forms part of the documentation related to their "ability, efficiency and conduct". Payslips are processed and published by the PMO and also made available for the staff member via SYSPER.

Other documents which have not been generated directly in SYSPER are scanned by HR personnel and uploaded to the NDP application. The staff member receives a notification from the NDP system when a file is published with information on how they can consult their file.

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, personnel number, date and place of birth, gender, nationalities, copy of passport/ID, birth certificate, change of name procedure, residence certificate, military/civilian service)
- Contact details (address, 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)
- Education & Training details (study certificates incl. copy of diploma(s), documents attesting ability to work in a third language, training completed)
- Employment details (employment certificates attesting professional experience (e.g., employment contracts, employers' references, payslips), determination of professional experience, grading, employment contract, contract decisions, appointment decision, interinstitutional transfer decisions, probationary period report/extension and objectives, establishment decision, appraisal reports, reclassification decisions, reassignment decisions, transfer decisions (Art. 7 and 29 of the Staff

Regulations), secondment, leave on personal grounds (request, agreement, renewal, reinstatement, JSIS and pension coverage), invalidity, special leaves, work schedules and absences)

- Financial details (bank account information of the staff member and any third party receiving payment, salary information/payslips, data on allowances, entitlements, benefits, reimbursements, pension rights, declarations linked to previous employment in case of transferring pension rights)
- Family, lifestyle and social circumstances (marriage certificate, registered partnership, birth certificate of children, adoption/recognition of a child/child under guardianship, members of the household, copy of divorce decree/separation/custody)
- Other (recruitment file (job offer, acceptance, vacancy notice, job description), resignation, decision on (non-)renewal of contract, medical fitness certificate, criminal record (confirmation of receipt only), decisions related to invalidity and occupational disease, administrative requests, complaints and related decisions, disciplinary files, ethics declarations and requests, training applications, certificate of employment)

(b) Special categories of personal data:

- data revealing racial or ethnic origin (may be revealed by the passports/ID and birth certificate)
- political opinions (may be revealed in case of a request upon Article 15 of the Staff Regulations)
- religious or philosophical beliefs (if disclosed on any of the staff member's documents)
- genetic data, biometric data, data concerning health
- information regarding an individual's sex life or sexual orientation (if evident from marriage or partnership declarations)

3. How do we collect and process your personal data?

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

4. Who is responsible for processing 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 the Administration Unit is responsible for this processing operation.

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

The management of personal files is necessary for the functioning of the Agency and for compliance with a legal obligation which the Agency is subject to. The processing of personal data is necessary in order to fulfil the rights and obligations set out in the Staff Regulations and CEOS, which apply to the staff of the Agency by virtue of Article 24 of Council Regulation (EC) 168/2007, as amended by Council Regulation (EU) 2022/555 (FRA's Founding Regulation). Personal files are established in accordance with Article 26 of the Staff Regulations, applicable by analogy to temporary and contract staff pursuant to Articles 11 and 81 of the CEOS. Therefore, the processing is lawful under Article 5(1)(a) and (b) 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)(c) 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 in the HR function will have access to the aspects of the personal file which are required for the performance of their duties;
- The staff members' Head of Unit as line manager, and the Director as Appointing Authority may be given access to specific data from the personal file that they need to fulfil their functions but do not have access to the personal file as such or to NDP.

Designated persons outside FRA as follows:

- European Commission DG HR and DG DIGIT may temporarily access data to provide functional and technical support, fulfilling their role of second line support to all the Agencies using NDP;
- European Commission Pay Master Office (PMO) for the purpose of management of entitlements such as pensions and allowances, on the basis of a Service Level Agreement concluded between FRA and PMO.

7. Do we share your data with other organisations?

The personal file may be transferred to another EU institution or agency in the case of the transfer of the staff member, in order to facilitate the human resources management in the other institution. This will take place only upon the official request of the new institution/agency following recruitment.

In addition, certain administrative details may be disclosed to legislative or supervisory bodies such as the European Court of Auditors, OLAF or in case of a request from the European Ombudsman or the Court of Justice in view of a complaint.

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 starts when you enter the service.

10. How long do we keep your data?

Personal data in NDP is stored until the end of the employment relationship with FRA. Data related to subsisting rights and obligations need to be conserved for a longer period. Those data have a retention period of 8 years after the expiry of all rights of the staff member concerned and of any dependents, and for at least 100 years after the recruitment of the staff member.

In accordance with Article 27 of Annex IX of the Staff Regulations, disciplinary decisions may be withdrawn from the personal file earlier (after 3 years in case of a written warning or reprimand and after 6 years in case of other sanctions), at the request of the data subject and provided that the Appointing Authority has granted the request.

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 were 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 staffadmin@fra.europa.eu.

11.1. Do we need your consent?

Since the use of personal files are mandatory in accordance with the Staff Regulations and CEOS, 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 restrict 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 1725/2018 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: I) 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?

Your personal data will not be used for an automated decision-making including profiling.

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.

Electronic files are processed via the NDP application, which is managed by the European Commission DIGIT. 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 14001, ISO 22301, ISO 27001, ISO 50001, ISO 9001, PCI DSS, PFS, Tier Rating Compliant: Tier IV, Uptime Institute rating: Tier IV.

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 staffadmin@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

Electronically signed on 30/10/2026 14:21 (UTC+01) in accordance with Article 11 of Commission Decision (EU) 2021/2121