

PRIVACY NOTICE FOR OLAF IDENTITY AND ACCESS CONTROL SYSTEM

1. DESCRIPTION OF THE PROCESSING OPERATION

The physical access control system is based on physical access points operated by electronic badge-readers.

It grants or denies access to the OLAF physical security perimeter within the J-30 building, as well as to special protected zones such as the IT technical rooms and other rooms where operational information is handled or stored.

It is operated under the responsibility of the Local Security Officer and used to facilitate verifications and/or investigations in case of a suspect or actual security incident.

In duly-justified cases, such as for access to the OLAF premises outside the business hours, or access to special protected areas, or access via unguarded access points (e.g. staircases, some elevators), additional biometric authentication is applied. Your fingerprints are stored on the personal badge for match-on card authentication.

The processing of your data will not be used for an automated decision-making, including profiling.

2. LEGAL BASIS FOR THE PROCESSING

The legal basis for this processing is: Article 5 paragraph 1.(a) of Regulation(EU) 2018/1725; Article 287 of the EC Treaty; Article 17 of the Staff Regulations; Regulation 883/2013; Commission Decision 1999/352; Commission Decision (EC, Euratom) 2015/443 on security in the Commission; Commission Decisions (EC, Euratom) 2017/46 and C(2006) 3602 concerning security of information and communication systems in the Commission; Commission's IT security policy (PoSec).

3. CATEGORIES OF PERSONAL DATA COLLECTED

The access control system records entry to the OLAF physical security perimeter within the J-30 building, as well as to special protected zones. It grants access based on access right categories to which each badge owner is assigned.

In order to carry out this processing operation, the system collects the following categories of personal data:

- Name,
- badge number,
- professional email address,
- department.

The personal data above are not collected from the data subject: the source from which your personal data originate is COMREF.

Gate, time and date of access are added to the collected data automatically by the system.

The fingerprints, together with personal data and picture, are collected by HR.DS from the data subject when issuing the access card.

Fingerprints are stored solely on the relevant personal access badge for match-on card authentication; they are not stored in the central system.

Staff members not able or willing to enroll to the biometric authentication may be granted access to OLAF only within the normal business hours, and only through the automated personal access gates in the guarded lobby, unless the system and other circumstances allow granting an exception.

4. WHO HAS ACCESS TO YOUR INFORMATION AND TO WHOM IS IT DISCLOSED?

The OLAF Local Security Officer, the members of the OLAF Security Team and their hierarchy have access to your personal data.

Your data may be disclosed to the Security Directorate of the DG Human Resources (HR.DS) and/or the Investigation and Disciplinary Office of the Commission (IDOC) in order to allow investigation of security incidents. In duly-justified situations, the data may be also transferred to the competent national authorities.

5. HOW DO WE PROTECT AND SAFEGUARD YOUR INFORMATION?

In order to protect your personal data, a number of technical and organisational measures have been put in place. Technical measures include appropriate actions to address 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 data being processed. Organisational measures include restricting access to the data to authorised persons with a legitimate need to know for the purposes of this processing operation.

6. HOW LONG DO WE KEEP YOUR DATA?

Your personal data may be retained by OLAF for a maximum of 1 year. Where a security incident occurs, or is suspected, the above retention period may be extended for the duration of the necessary verifications, investigations or the legal and/or administrative proceedings.

7. WHAT ARE YOUR RIGHTS AND HOW YOU CAN EXERCISE THEM?

You have the right to request access to your personal data, rectification or erasure of the data, or restriction of their processing.

You have the right to object to the processing of your data.

Any request to exercise one of those rights should be directed to the Controller (OLAF-FMB-DATA-PROTECTION@ec.europa.eu). Where you wish to exercise your rights in the

context of one or several specific processing operations or files, please provide their description and reference(s) in your request.

Exceptions or restrictions based on Regulation 2018/1725 may apply.

8. CONTACT DETAILS OF THE DATA PROTECTION OFFICER

You may contact the Data Protection Officer of OLAF (OLAF-FMB-DPO@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation(EU)2018/1725.

9. RIGHT OF RECOURSE

You have the right to have recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation(EU)2018/1725 have been infringed as a result of the processing of your personal data by OLAF.