

PRIVACY NOTICE FOR OLAF IDENTITY AND ACCESS CONTROL SYSTEM

1. DESCRIPTION OF THE PROCESSING OPERATION

The physical access control system grants or denies access at all entrances and exits from the OLAF physical security perimeter within the OLAF building, as well as to special protected zones such as the IT technical rooms and the OLAF Document Management Centre where operational information is handled, stored and archived.

For those staff members who may have to work outside the normal business hours, who need access to special protected areas, or who use unguarded access points (staircases) to access the OLAF secure premises, additional biometric authentication is applied. Three of your fingerprint templates are stored on the card for match-on card authentication. The recorded access control information is used to facilitate investigations in case of a security incident.

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.

The other legal basis are Article 297 of the EC Treaty; Article 17 of the Staff Regulations; Regulation 883/2013; Commission Decision 1999/352 establishing the European Anti-Fraud Office; Commission Decision 2015/443 of 13 March 2015 on Security in the Commission; Commission Decision 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission; Commission's IT security policy (PolSec); OLAF Information Security Policy.

3. CATEGORIES OF PERSONAL DATA COLLECTED

The access control system records entries and exits from the different security zones within the OLAF security perimeter. In order to carry out this processing operation OLAF collects the following categories of personal data:

- Name, staff number and card number.
- Fingerprints are stored on your personal access card alone; they are not stored in the central system. Time and date are added to the collected data.

The fingerprints are collected from the data subject. Staff members not able or willing to enroll to the biometric authentication will be obliged to access OLAF within the normal

business hours and only through the automated personal access gates in the guarded lobby.

The other personal data (name, staff number) are not collected from the data subject: the source from which your personal data originate is COMREF.

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

OLAF staff responsible for carrying out this processing operation has access to your personal data. The access control information is accessible to OLAF Security Officers only.

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 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 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?

The access control information may be retained by OLAF for a maximum of 1 year

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.

You have consented to provide your fingerprints to OLAF for the present processing operation. You can withdraw your consent at any time by notifying the controller. The withdrawal will not affect the lawfulness of the processing before the consent was withdrawn.

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 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.