

PRIVACY STATEMENT

for the processing operations in the framework of administrative inquiries

1. INTRODUCTION

This Privacy Statement describes the measures taken to protect your personal data with regard to the action involving the present data processing operation and what rights you have as a data subject.

EDA protects the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data (Article 1.1 of Regulation No 2018/1725).

2. CONTROLLER OF THE PROCESSING OPERATION

European Defence Agency
Rue des Drapiers 17-23
B-1050 Brussels
www.eda.europa.eu

3. PURPOSE OF THE PROCESSING

The processing of personal data is necessary in order to establish whether a staff member failed to comply with his or her obligations under the EDA Staff Regulations and, where appropriate, impose a disciplinary penalty in accordance with them.

4. DATA PROCESSED

Data processed are the following:

Title, first name, surname, date of birth and function;

The behaviour, action or inaction of the person subject to an administrative inquiry and/or a disciplinary procedure;

The personal data related to the outcome of the procedure for the person concerned, e.g. penalties, financial liability;

As the case may be, the penalty imposed on the person concerned;

Information regarding third parties (witnesses, informants);

Sensitive data in the meaning of Article 10;

In some cases, the processing of personal data, such as health data or data regarding the civil status of the persons involved in the inquiry, might also be necessary.

5. RECIPIENTS OF THE DATA

EDA Chief Executive, Senior Management, Director Corporate Services, Head of Human resources, appointed Investigators, Legal Advisor/DPO; Disciplinary board, in the event where a disciplinary procedure is opened; Authorised staff of the Human Resources Department, for filing and including the final disciplinary decision in the personal file.

OLAF in accordance with Decision 16/04 of 22 February 2016. EDA will ensure, through a case-by-case review, that the transfer of personal data is not automatic but will only take place when and as necessary for the legitimate performance of the tasks under the recipient's competence.

Involvement of staff must be strictly limited on a need to know-basis and only when necessary for the legitimate performance of tasks covered by the competence of the recipient.

Any recipient of the data shall be reminded of their obligation not to use the data received for other purposes than the one for which they were transmitted.

6. PROTECTION AND SAFEGUARDING OF THE DATA

Personal and disciplinary files are stored in secure cupboards within the Human Resources Unit accessible only to authorised persons. Access to personal and disciplinary files of the staff member concerned is limited to the data subject and to EDA personnel specifically authorised to have access to personal files, i.e. the authorised HR staff, the internal auditor, the members of the College of Auditors and the AACC. The data subject does not have direct access. The personal file and/or disciplinary file is taken out of the secure cupboard by the authorised staff member and handed to the data subject for consultation on the spot. Electronic files will be stored in the shared drive with access restricted to authorised HR persons and the legal adviser.

Exchange of emails shall be strictly limited to authorised recipients on a need to know basis and treated through confidential emails that contain only strictly relevant data.

If sensitive information has to be exchanged with the external partners mentioned among the list of recipients, IT shall provide, upon request, certificates (Public/private keys) externally recognised to encrypt and/or sign that information.

7. RIGHT OF ACCESS AND RECTIFICATION OF THE DATA

Data subjects have the right to access their personal data and the right to correct any inaccurate or incomplete personal data, as well as to request the removal of their personal data, which will be implemented within 10 working days after the request has been deemed legitimate. If the data subject has any queries concerning the processing of his/her personal data, s/he may address them to the data controller at the following mailbox: hadmin@eda.europa.eu

However, the exercise of these rights might be restricted within the limits of the possible exemptions of Article 25 of Regulation 2018/1725. These exemptions shall be applied in a restrictive manner.

Justified requests are treated within 10 working days after the request will have been deemed legitimate.

If the staff member submits a request, under Article 164 to the Staff Regulations, for the deletion of a written warning or reprimand (3 years after the Decision) or in the case of another penalty (6 years after the Decision, except for removal from post) and the AACC grants the request, the disciplinary file which led to the penalty will also be deleted. In the case of a warning ("mise en garde") which is not a disciplinary sanction but a formal reminder about the need to observe the highest ethical standards, the warning is placed in the staff member's personal file for 18 months.

8. TIME LIMIT FOR STORING DATA

Pre-inquiry file: maximum retention period of two years after the adoption of the decision that no inquiry will be launched. This maximum retention period could be necessary for audit purposes, access requests from affected individuals and complaints to the Ombudsman.

Inquiry file: When the Agency launches an inquiry including the collection of evidence and interviews of individuals, there could be three possibilities: i) the inquiry is closed without follow-up, ii) a caution is issued or iii) the AACC adopts a formal decision that a disciplinary proceeding should be launched. For cases i) and ii), a maximum of five-year-period from closure of the investigation is a necessary retention period, taking into account audit purposes and legal recourses from the affected individuals. For case iii), the Agency transfers the inquiry file to the disciplinary file, as the disciplinary proceeding is launched on the basis of the evidence collected during the administrative inquiry.

Disciplinary file: taking into consideration the nature of the sanction, possible legal recourses as well as audit purposes, the maximum retention period after the adoption of the final Decision is 10 years.

No personal data is kept for historical, statistical or scientific purposes. Only aggregated data (e.g. list of open and completed cases) will be used for statistic purpose.

9. LEGAL BASIS FOR THE PROCESSING OPERATION

Article 5(b) of Regulation 2018/1725;
Article 31 of Council Decision (CFSP) 2015/1835 of 12 October 2015 defining the statute, seat and operational rules of the European Defence Agency.

10. CONTACT DPO

In case you have any questions or queries concerning data protection at the European Defence Agency, you can also contact the Data Protection Officer at dataprotection@eda.europa.eu.

11. RECOURSE TO EDPS

As a data subject you have the right to have recourse at any time to the European Data Protection Supervisor (<http://www.edps.europa.eu>) at edps@edps.europa.eu.

12. ADDITIONAL INFORMATION

More information on Data Protection at the European Defence Agency can be obtained on our public website <https://www.eda.europa.eu/Aboutus/how-we-work/data-protection>.