Privacy Statement/ Data Protection Notice

For the processing activity: use of SYSPER for EDA staff, including management of digital personal file (NDP)

This Privacy Statement provides information on the processing and the protection of your personal data and on the rights you have as a data subject.

1. TITLE OF THE PROCESSING ACTIVITY

Use of SYSPER for EDA staff, including management of digital personal file (NDP)

2. CONTROLLER OF THE PROCESSING ACTIVITY

EUROPEAN DEFENCE AGENCY EDA Human Resources Unit hradmin@eda.europa.eu	Data Processor: European Commission Directorate General for Human Resources and Security (DG HR)

3. PURPOSE OF THE PROCESSING ACTIVITY

EDA is using SYSPER, HRM IT tool owned and managed by the European Commission, to support the management of main HR administration processes and to ensure that personal data is kept accurate, is traceable and rapidly retrievable.

SYSPER has different basic and optional modules, of which EDA uses the following:

- Identity Management module: "Identity Management" (COMREF/RETO)
- Organisation Management modules: "Organisation Chart" and "Job Quota Management"
- Personal Data Management modules: "Employee Personal Data" and "Address Declaration",
- Talent Management modules: "Career Management"
- Time Management modules: basic "Time Management", including basic work patterns, leave rights, absences
- Document management module: "Generation of Certificates"
- NDP (Numérisation des Dossiers Personnels) module: Staff digital personal files.

4. DATA PROCESSED

a. Data subject categories:

EDA postholders (staff) and their family members.

This includes temporary agents, contract agents, seconded national experts, trainees, interims, and former staff members (since certain data need to be retained for a longer period if they relate to subsisting rights and obligations, e.g.orphan's allowance).

b. Data categories processed:

Within the different SYSPER basic modules, the following types of personal data are processed for the above-mentioned purpose:

• surname, first name, personnel number, gender, nationality, address, telephone number, place of origin;

• Date of birth, marital status, officially recognised registered partnership, identity and date of birth of spouse or partner, identity and date of birth of dependent children and date of adoption if relevant, and associated certificates for the applicable cases;

• EDA Unit to which the jobholder is assigned, category, grade, status, contract information (duration, renewal, termination), years of service, unique payroll number (NUP), administrative status and career (advancement to step, reclassification, reassignment);

• Bank account number;

• Information on medical fitness (only administrative data, fit/not-fit for work);

• Information on absences and work pattern: sick leave (with or without a medical certificate), special leave, annual leave, parental and family leave, and the results of calculations, particularly regarding the balance of entitlements (balance of absences, leave, parental and family leave entitlement, time credits purchased). In case of absences for health reasons (absences with or without medical certificate) and in case of special leave, SYSPER does not process medical data of the EDA staff member or his/her family members, just administrative data related to the nature of the absence.

• Information on telework away from the place of employment;

• The staff's personal file;

• Administrative acts necessary for the application of the Staff Regulations, i.e. Decisions on disciplinary procedures and measures; Decisions on invalidity (only administrative data); Decisions relating to outside and to post-employment activities.

5. RECIPIENTS OF THE DATA

Access to the data is provided on a strict need-to-know basis depending the function and responsibility of each user. In addition, access rights may be adjusted to cover specific parts of the data. The following user groups have been identified as having access rights:

Internal recipients:

• All jobholders in relation to their own data; for certain data (e.g. email address, phone number) the jobholders/data subjects are able to perform a change themselves.

• The EDA HR team;

• The AACC and managers with roles in respective workflows, as well as staff to whom such roles have been delegated. Not all of the users have the same access rights to personal data. The profile of each user (function and responsibility) determines their need and entitlement to access specific sets of data in SYSPER;

External recipients:

• Commission services in relation to their specific field of competence. In particular, Commission's Directorate General of Human Resources (DG HR) and PMO, for offering and managing the SYSPER IT application under a Service-Level Agreement;

• In case of employment by a new EU institution/agency/body after the end of service at EDA, personal data are transmitted on a need-to-know basis and as required for the performance of tasks carried out in public interest, in line with recitals 21, 22 and Article 5(1)(a)(b) of Regulation (EU) 2018/1725, and Article 26 of Regulation No 31 (EEC), 11 (EAEC) ('EU staff Regulations') and Article 11 of CEOS as applicable to the new employer.

• External contractors that may be working on the maintenance of the IT infrastructure linked to SYSPER;

• Upon request if relevant for the handling of files under their tasks, personal data may be transmitted to: European Court of Justice, European Ombudsman, European Data Protection Supervisor, European Anti-Fraud Office (OLAF), Internal Auditor, EDA College of Auditors.

6. MEANS OF PROCESSING AND MEASURES OF SECURITY OF THE DATA

SYSPER is an IT application that employs a series of horizontal, generic components to support all business functions in a uniform and consistent manner. This is particularly important in key areas such as: Security, Actors (SYSPER uses information in the organisational hierarchy and jobs defined therein, in order to automatically determine who needs to do what at each step of the administrative procedures), Workflows and notifications. A Security Convention has been agreed with the Commission and delivers key aspects on security features such as the security of the facilities and of EDA network.

For information, the present notification provides requirements of the Convention - but cannot disclose technical measures. Some of the aspects are: Access control measures, Monitoring activity with logging and reporting on physical access, Physical security measures for outside working hours, Specific organisational measures regarding physical protection Information security management, audit/assessments or penetration tests, Alerts and/or regular reports. Policy/security operating procedures defined and network access control infrastructure and mechanisms. Such measures have been taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and to prevent all others unlawful forms of processing.

7. RIGHT OF ACCESS TO YOUR PERSONAL DATA AND OTHER RIGHTS OF THE DATA SUBJECT

Data subjects have the right to access their personal data, the right to request rectification of any inaccurate or incomplete personal data, the right to erasure, the right to restriction of processing, the right to object to the processing, as applicable and at any time, under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725. Personal data processed for the purpose of this processing activity is not subject to automated decision making.

For any queries regarding the processing of personal data, or to exercise these rights, data subjects can contact the data Controller at **hradmin@eda.europa.eu** or the Data Protection Officer at dataprotection@eda.europa.eu .

8. RETENTION OF THE DATA

The retention takes place within the SYSPER system. Personal files are kept for 8 years after the extinction of all rights of the person concerned and of any dependants, and no less than 20 years after the recruitment of the staff member.

9. LEGAL BASIS FOR THE PROCESSING OPERATION

Processing of personal data is necessary for the performance of tasks carried out in the public interest by EDA, including operations needed for the management and functioning of EDA, and for compliance with legal obligations to which EDA is subject in accordance with Articles 5(1)(a),(b) of Regulation (EU) 2018/1725, and: Articles 33 and Article 104 of Council Decision (EU) 2016/1351 of 4 August 2016 concerning the Staff Regulations of the European Defence Agency ("The EDA Staff Regulations") that establish the obligation to have personal files and govern their creation, maintenance and access; Provisions of Title II Chapters 3, 4, 5, 6, 8 and Title III Chapters 2,3,4,5,6,7,8 and of Title V of the EDA Staff Regulations, on specific rights, entitlements, obligations of the staff members and decisions of the AACC; Respective Provisions of Council Decision (EU) 2016/1352 concerning the rules applicable to SNEs.

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.