PRIVACY STATEMENT

regarding the use of SYSPER for EDA staff

1. INTRODUCTION

This Privacy Statement describes the measures taken to protect your personal data with regard to the use of Sysper for EDA staff 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. PROCESSOR

European Commission, due to its ownership of the system where the data are stored and secured.

4. PURPOSE OF THE PROCESSING

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: EDA Staff's personal files.

5. DATA PROCESSED

The data subjects are EDA postholders 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).

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

- 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;
- EDA Unit to which the jobholder is assigned, category, grade, status, duration of contract, years of service, unique payroll number (NUP), administrative status and career;
- Information on medical fitness (only administrative data);
- Information on absences: 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.
- Decisions on invalidity (only administrative data).
- Decisions relating to outside and to post-employment activities.

6. 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:

- All jobholders in relation to their own data;
- 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;
- Commission services in relation to their specific field of competence. This relates in particular to PMO that falls under the Directorate General of Human Resources (DG HR) and with whom EDA has a Service-Level Agreement;
- External contractors that may be working on the maintenance of the IT infrastructure linked to SYSPER;
- Belgian authorities in the context of processing access to the "digital key" for staff and family members holding a special ID card.
- Upon request if relevant for the handling of files: European Court of Justice, European Ombudsman, European Data Protection Supervisor, European Anti-Fraud Office (OLAF), Internal Auditor, EDA College of Auditors.

7. PROTECTION AND SAFEGUARDING 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 (SYSPER allows for the definition – and the enforcement – of a coherent, transparent and easy security policy via configuration)
- 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 (SYSPER uses common workflow and notification engines to define and execute the various workflow steps and to deliver required notifications, depending on configurable conditions).

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. Annex 1 of the Convention provides EDA physical security measures, while Annex 2 and 3 of the Convention provide EDA network and IT security measures.

For information, the present notification provides requirements of the Convention - but cannot disclose technical measures.

Some of the aspects of Annex 1 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[…]

Some of the aspects of Annex 2 and 3 are:

- Information security management
- Information security audit/assessments or penetration tests
- Alerts and/or regular reports
- The hardening is applied on the devices
- Policy/security operating procedures defined and network access control infrastructure and mechanisms (e.g. external/internal firewall, gateway, router, IDS/IPS, etc.) implemented onthe perimeter of the corporate network

Having regards to the state of the art and the cost of their implementation the controller has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected (restricted access, logs, etc.). 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.

8. RIGHT OF ACCESS AND RECTIFICATION OF THE DATA

Data subjects have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access their personal data, and, to rectify them, in case they are inaccurate or incomplete. Where applicable, they have the right to erase their personal data, to restrict the processing of their personal data, to object to the processing, and the right to data portability.

Data subjects have the right to access their personal data and for certain data (e.g. email address, phone number) the data subjects are able to perform a change themselves. For other changes (e.g. changes in the family situation, which might affect benefits or health insurance, change of nationality) the data subjects need to address a request to the controller along with the relevant supporting documentation.

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: hradmin@eda.europa.eu.

Justified requests for blocking and erasure are treated within 15 working days after the request has been deemed legitimate.

9. TIME LIMIT FOR STORING 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.

10. LEGAL BASIS FOR THE PROCESSING OPERATION

Article 5(1)(b) of Regulation 2018/1725;

Article 5(1)(d) of Regulation 2018/1725 (for staff and family members with a special ID card for the purpose of obtaining the 'digital key' (a user name and password) in order to access Covid-19 vaccination certificate, EU digital Covid-19 certificate and/or Covid-19 test results via Belgian authorities;

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

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.

11. 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.

12. 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.

13. 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.