European Union
EXTERNAL ACTION

EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF THE USE OF THE SYSPER APPLICATION BY EEAS SERVICES AND THE PROCESSING OF PERSONAL DATA RELATED TO HUMAN RESOURCES MANAGEMENT BY MEANS OF THE SYSPER SYSTEM

1. INTRODUCTION

The protection of your personal data and privacy is of great importance to the European External Action Service (EEAS), including the Delegations of the European Union. You have the right under EU law to be informed when your personal data is processed [collected, used, stored] as well as about the purpose and details of that processing.When handling personal data, we respect the principles of the Charter of Fundamental Rights of the European Union, and in particular Article 8 on data protection. Your personal data are processed in accordance with Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, aligned with Regulation (EU) 2016/679, the General Data Protection Regulation. In this privacy statement you find information about how the EEAS and EU Delegations process your personal data and what rights you have as a data subject.

2. PURPOSE OF DATA PROCESSING: Why do we process your data?

The overall purpose of the present processing activity is

- To support all procedures concerning the management of human resources (recruitment, career, allocation of / to posts)
- To plan, manage and monitor staff, to contribute establishing statistics and reporting (including the annual report concerning equal opportunities, gender balance; putting in place mobility policy; establishing the AMP, the AAR report)
- To allow staff establish connection by remote access By way of exception, to allow reaching staff members in emergency situations, in particular due to security circumstances taking into account the duty of care responsibility of EU institutions and bodies, and that of the EEAS by sending emergency alert updates via private GSM numbers intended for the safety and benefit of the staff members concerned.
- To comply with the obligation in Article 15 of the Protocol 7 on Privileges and Immunities of the European Union to the TFEU (PPI) and the sincere cooperation foreseen in Article 4(3) TEU by providing information to Member States.

Description of the Sysper system

Sysper is the integrated information system developed and managed by the European Commission and used by the EEAS on the basis of a Servicel Level Agreement for the purpose of human resource management. SYSPER is considered to cover all needs concerning the treatment of information for the management of Human Resources. It facilitates the exchange of information between different user groups on central and local level.

This Privacy statement applies to the overall SYSPER system. The system consist of a set of modules, each one covering precise and specific functionalities within HR management. SYSPER is also a portal through which users have secure access to their payslips. These are prepared by the NAP application (payroll management). In addition, SYSPER allows for enhanced cooperation and exchange of information with PMO.

The specific purposes of the individual modules of the Sysper system are:

- Identification of the EEAS staff (jobholders) and establishment of the EEAS organisation chart
- Career management: recruitment, job assignments, status, grade, step, administrative position, end of service
- Time management: registration of presences and absences as well as presence planning (presence in the office and telework)
- Management of staff appraisals (CDR), promotions & job descriptions
- Management of individual rights, administrative certificates and working conditions
- Management of human capital database (e-CV)
- Reporting and statistics in order to plan, monitor and manage staff
- Serve as a basis for the NAP application managed by PMO, in particular for remunerations
- Sharing information with the PMO for the purpose of the determination, calculation and payment of financial entitlements and benefits as well as remuneration of staff members, handled by the PMO
- By way of exception, using the contact details stored in Sysper to allow reaching staff members in emergency situations, in particular due to security circumstances taking into account the duty of care responsibility of EU institutions and bodies, and that of the EEAS by sending emergency alert updates via private GSM numbers intended for the safety and benefit of the staff members concerned

The purposes of the transmission of personal data to the Member States are:

- to ensure the implementation of the privileges and immunities granted by the PPI to officials and other servants and enable national administrations to follow up on those privileges and immunities by ensuring that they are informed about the identity of EU staff members covered
- to enable Member States to compile statistics on nationals from Member States;
- to pursue and support regular institutional working relations between the Member States and the EEAS.

3. DATA PROCESSED: What data do we process?

The data, including personal data, which may be processed for that purpose are the following:

- Identification data
- Contact details
- Data, including all information, related to the job and career of EEAS staff members (such as function, grade, seniority, job description, objectives, evaluation data concerning appraisal, promotion, etc.)
- Data related to time management (presences, absences, presence in the office and telework)
- Data concerning professional experience, knowledge, skills (e-CV), etc.
- Data related to rights and obligations, including entitlements, allowances

All individuals who at present have or in the past had an employment contract with the EEAS are concerned, as well as those who are candidates to obtain such a contract. Data related to jobholders' relatives (spouse, children) are processed due to allowances.

The modules of SYSPER with specific functionalities processing personal data are the following:
Jobholder Management: this module covers all 'contractual' aspects between the EEAS and staff.
Staff appraisal (CDR): this module contains the information on the appraisal process of performance and conduct in the service, and the evaluation of the professional potential of jobholders.
Promotions: this module allows the monitoring of the promotion procedures and the related decisions taken.
Human Capital Database (e-CV): this module allows the exploitation and sharing of information on the profiles of the office bearers. It facilitates the management of your career. It collects information on your professional experience, your competences and ambitions.
Job descriptions: covers three key elements on staff member's job (job title, domains and functions&duties)
Time Management: this module will facilitate the management of the working schedules, leaves and absences for each jobholder.

Neither the medical files nor the disciplinary files are currently integrated in SYSPER.
A further service offered by SYSPER is the SYSPER Data Warehouse. By using a copy of the data stored in SYSPER this database allows the elaboration of specific reports on the situation of human resources. The applications of the data warehouse fall under the same legal provisions for data protection as SYSPER does. The access rights to the data warehouse are identical to those of SYSPER.
None of the modules of SYSPER specifically intend to process data revealing any racial or ethnic origins, any political opinion, religious or philosophical orientations, any membership in trade unions (apart from the registration of specific access rights to SYSPER which are offered to members of joint committees only) or any information on the sexual orientation of staff members.
The Privacy Statement on HR reporting contains the description of the transmission of personal data of staff to Member States.

4. DATA CONTROLLER: Who is entrusted with processing your data?

The data controller determining the purpose and the means of the processing activity is the European External Action Service (EEAS). The EEAS Directorate responsible for managing the personal data processing is the following organisational entity:

Directorate for Budget and Human Resources (EEAS.RM.BHR)

Operational Data Controllers: Coordination Division (RM.01); Post Management and Agility (RM.BHR.2)

5. RECIPIENTS OF THE PERSONAL DATA: Who has access to your data?

The designated human resource managers of the EEAS and of the operational services of the European Commission and its administrative agencies (HR, DIGIT, EPSO, PMO, OIB, OIL) have access to the specific data they need in order to fulfil their management tasks.

In accordance with the fundamental purpose of SYSPER, as a system for the management of human resources, the processing of your data and especially the decision powers for the distribution of access rights are entrusted to the human resource managers. The following potential user groups are entitled to obtain access rights to specific parts of the data:

- all jobholders within the context of the organisation of work and career development have access to their own data (modules JIS, CDR and Jobholder Management)
- the human resource managers
- the central human resource functions have access to the data that are in their specific field of competence
- the COM administrative agencies (HR, DIGIT, EPSO, PMO, OIB, OIL) have access to the data that are in their specific field of competence
- the local human resource functions have access to the data that are in their fields of competence
- Hierarchical superiors
- your direct hierarchical superior
- the superiors of your direct hierarchical superior
- The members of joint committees concerned with human resources management issues (e.g. Joint Evaluation Committee, Joint Committee for Reports, etc.)
- all other persons authorised by delegation by one of the users having certain approved Sysper access rights

Not all 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 your data.

- The information contained in Sysper is transferred to other institutions for purposes within their competence, for example in the case of an interinstitutional transfer of staff or when members of a family work for different EU institutions, in order to facilitate the management of the staff member's file, entitlements and obligations by the other institution. Data can also be transferred to the auditing or inquiring bodies, such as OLAF or the European Court of Auditors, for control purposes. Data are transmitted to Member State authorities and Permanent Representations for the purposes outlined in point 2.

The following data: name, office address, telephone and global job description are published in the internal directory of the EEAS also accessible to staff of the European Commission. The name, position and contact details solely of middle and senior management as well as specific public functions are also included in the official directory of the European Union (EUROPA – WhoisWho). The official directory can be accessed via internet to facilitate the communication between the EEAS and the external world, particularly the European citizens.

The recipients of your data may specifically include:

- Management of the EEAS, in particular assigned staff members in the Directorate of Budget and Human Resources (RM.BHR) and designated EEAS.SG office staff with purpose limitation
- Assigned EEAS staff members dealing with human resources management and specific procedures with purpose limitation
- Assigned staff in emergency circumstances dealing with security measures including the facilitation of the SMS alert system with purpose limitation

Personal data is not intended to be transferred to a third country or an international organisation. The given information will not be communicated to third parties, except where necessary for the purposes outlined above.

6. ACCESS, RECTIFICATION, ERASURE OF DATA: What rights do you have?

All staff members have access to their own data in the SYSPER system. As a staff member (both in active and non-active status), you are entitled of the right to read your identification file. This access right is limited to reading (a possible exception can be your personal title and certain other data which do not have any direct impact on the rights of the individual).

In the context of the modules on Professional Evaluation and on Jobholder Management, you have the right to introduce part of the data yourself. This is namely your auto-evaluation and information concerning your profile, etc. This allows you to verify the accuracy of your data and, if necessary, to directly correct it. Certain data need to be validated by an EEAS official, a line manager or superior, in particular if these data influence the financial rights and obligations of the person concerned. In this case, the right to introduce or validate the data is given to the hierarchical superior or to staff that is at the same time entitled to verify the facts. You have the right of access to your own personal data and the right to correct any inaccurate or incomplete personal data. The right of rectification can only apply to factual data processed. Under certain conditions, you have the right to ask the deletion of your personal data or restrict their use as well as to object at any time to the processing of your personal data on grounds relating to your particular situation. Your attention is also drawn to the fact that erasure may not be possible for specific data categories. We will consider your request, take a decision and communicate it to you. For more information, please see Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. In specific cases, restrictions under Article 25 of the Regulation may apply. If you have questions concerning the processing of your personal data, you may address them to the operational Data Controller:

EEAS SYSPER HELPDESK <sysper-heldesk@eeas.europa.eu>

7. LEGAL BASIS: On what grounds we collect your data?

- The processing of the personal data is necessary for the performance of a task carried out by the European External Action Service in the public interest by the EEAS, in particular the management and functioning of the EEAS [Article 5(1)(a) of Regulation (EU) 2018/1725 as referred to in Recital 22 thereof].
- The processing of the personal data is also necessary for compliance with the obligation of duty of care according to Article 3 of the Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 April 2013 on the security rules for the European External Action Service 2013/c 190/01 [Article 5(1)(b) of Regulation (EU) 2018/1725].
- The processing of the personal data is necessary for the performance of the employment contract between the staff member and the EEAS and its preparation at the request of the data subject. [Article 5(1)(c) of Regulation (EU) 2018/1725].

Legal reference(s):

- Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities
- Protocol No. 7 on the privileges and immunities of the European Union to the Treaty on the Functioning of the European Union
- PROC EEAS(2011)001 of 29/11/2011 Decision on Adopting the Common Inter-institutional rules for implementing certain provisions of the Staff Regulations and of the Conditions of Employment of Other Servants
- PROC EEAS(2011)002 of 29/11/2011 To extend the application of certain Commission Rules developing the provisions of the Staff Regulations and of the Conditions of Employment of Other Servants, to the EEAS
- EEAS DEC (2014)009 of 13/02/2014 Amending the Annex to the Decision PROC HR(2011)002 of 29/11/2011 "To extend the application of certain Commission Rules developing the provisions of the Staff Regulations and of the Conditions of Employment of Other Servants, to the EEAS"
- EEAS DEC (2014)032 of 26/06/2014 Amending the Annex to the Decision PROC HR(2011)002 of 29/11/2011 "To extend the application of certain Commission Rules developing the provisions of the Staff Regulations and of the Conditions of Employment of Other Servants, to the EEAS" as amended by the Decision of the Chief Operating Officer EEAS DEC(2014) 009 of 13 February 2014
- EEAS DEC (2014) 048 of 13/11/2014 Decision of the Chief Operating Officer ad interim of the EEAS to apply by analogy the Commission Decision SEC (2014) 543 extending till 31 December 2015 the Commission Decision C(2013) 4459 of 25 July 2013 suspending the requirement laid down in Article 3(1) of the Commission Decision C(2011) 1264 of 2 March 2011 on

the general provisions for implementing Article 79(2) of the Conditions of Employment of Other Servants of the European Union, governing the conditions of employment of contract staff employed by the European External Action Service under the terms of Article 3a and 3b of the said Conditions

- All relevant implementing provisions for giving effect to the Staff Regulations and to the Conditions of Employment of Other Servants adopted by the EEAS including among others:
- PROC HR(2011)013 of 22/11/2011 on general implementing decisions giving effect to the Staff Regulations and to the Conditions of Employment of Other Servants
- HR DEC (2014) 02 of 03/02/2014 Amending Annex I of the Decision of the High Representative PROC HR(2011)013 of 22/11/2011 on General Implementing Provisions for giving effect to the Staff Regulations and to the CEOS
- Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 April 2013 on the security rules for the European External Action Service 2013/c 190/01; Article 3 thereof on Duty of Care

Further legal reference:

- Council Decision of 26 July 2010 establishing the organisation and functioning of the EEAS (2010/427/EU) – OJ L 201, 3/8/2010, p. 30.

8. TIME LIMIT - DATA STORING: For what period and how we process your data?

Personal data is stored, as a rule, for the duration of the activity within the EEAS. Certain data is retained beyond the period of activity, to the extent until these data are in relation to remaining rights or obligations (e.g. pension rights). Personal data of a non-recruited external candidate is deleted after the expiration of the eligibility period for any complaints, i.e. all channels of recourse have been exhausted.
Personal files are retained according to the Common Retention List.

Security of data
Appropriate organisational and technical measures are ensured according to Article 33 of Reg. (EU) 2018/1725. The collected personal data are stored on servers that abide by pertinent security rules. The datasets are safeguarded in the Data Center of the Commission in Luxembourg, and therefore covered by the numerous defensive measures implemented by DG DIGIT to protect the integrity and confidentiality of the electronic assets of the EEAS. Measures are provided to prevent unauthorised entities from access, alteration, deletion and disclosure of data.

Data is processed by assigned staff members. General access to personal data is only possible to recipients with a UserID/Password. The access to the personal data is protected by the management of the access rights which are strictly limited to specific user groups. The access entitlement is given in accordance with the principle of 'the need to know', while taking into consideration the function, the job and the responsibilities of the applicant for an access right. Consequently, the access rights are continuously updated in accordance with the changes in the assignments of the jobholders.

The login and the passwords are managed by the common certification service of the European Commission. EC Sysper Record including security measures: https://ec.europa.eu/dpo-register/detail/DPR-EC-01230.

Each owner of an access right has the possibility to delegate his rights to a person of confidence, who has a justified "need to know" to have access to the data concerned. This delegation is transparent and reversible. The responsibility relies on the actor who delegates the access right. As the delegation is related to a function of a job and not to a person, the delegation consequently expires when the person leaves the job. Thanks to the technique of 'audit trail' each access and manipulation of data in SYSPER can be identified and traced. Only the data for which a user has obtained the corresponding access right can be visualised, printed and saved by that user.

Where internal transmission of personal data is necessary between EEAS organisational entities or other EU institutions, it should be sent using SECEM encrypted emails in line with the *"EEAS best practices on handling and protecting sensitive and EU classified information"* (Ref. Ares(2020)2358268). Printouts and paper-based processing should be minimised. Where printing paper files is inevitable for a specific purpose, hard copies are to be stored in other secured storage containers and destroyed immediately after no longer in use.

9. EEAS DATA PROTECTION OFFICER: Any questions to the DPO?

If you have enquiries you can also contact the EEAS Data Protection Officer at data-protection@eeas.europa.eu.

10. RECOURSE

You have, at any time, the right to have recourse to the European Data Protection Supervisor at edps@edps.europa.eu.