EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO SECONDED NATIONAL EXPERTS (SNE) BY THE EEAS

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 purpose of the data processing activity is to process personal data of Seconded National Expert (SNE) candidates and SNEs in relation to personnel selection procedures, establishment of rights, payment of allowances, entitlements and other administrative matters.

Personal data are processed to coordinate the preparation, selection and administrative management for SNEs seconded to the EEAS [Headquarters (HQ) and EU Delegations].

3. DATA PROCESSED: What data do we process?

Personal data submitted for the purposes of selection, establishment of rights, payment of allowances and other entitlements within the following types documents:

- CVs
- Selection panel reports
- Secondment agreement including the Employer and the Expert declarations allowing the EEAS to establish the rights of the Expert and to collect personal data required for the secondment
- Bank details
- Other material related to SNE secondment (certificates, etc.)

Data processed related to SNEs and candidates for SNE posts:

- Surname, first name
- date and place of birth,
- gender,
- nationality,
- marital status,
- family composition,
- Contact details, including personal address, etc. (Information provided by the candidate to allow the practical organisation of preselection)
- Information provided by the candidate to verify whether he/she fulfils the eligibility and selection criteria laid down in the vacancy notice, i.e. proof of nationality, languages, education, employment record, other information relevant for the job skills such as knowledge of computer software and information regarding security clearance, if applicable

Data processed related to the members of the selection panel may be:

- Name
- Last Name
- Service/Function
- Score given

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 Division responsible for managing the personal data processing under the supervision of the Head of Division is the following organisational entity:

EEAS RM.HR.2 - Selection and Recruitment of Staff

selection-and-recruitment@eeas.europa.eu

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

The recipients of the data are the following, on a strict "need-to-know policy" basis:

- Designated staff of Division 'Selection and Recruitment'
- Head of Division and other dedicated staff in the division relevant for the particular recruitment
- Head of Delegation and Head of Administration in EU Delegations
- Members of selection panels including representatives of Council, European Commission and EEAS, Appointing Authority

The information in question is not intended ot be transferred to Third Countries nor to International Organisation. Data 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?

You have the right of access to your personal data and the right to correct any inaccurate or incomplete personal data. The right of rectification can only apply to factual data processed, taking into account the purpose of the processing. 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. We will consider your request, take a decision and communicate it to you without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary. For more detailed legal references, you can find information in 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 would like to exercise your rights or have questions concerning the processing of your personal data, you may address them to the Data Controller via the specific functional mailbox:

sne-delegations@eeas.europa.eu

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

Lawfulness: The processing of your personal data is necessary for the performance of a task carried out in the public interest, [Article 5(1)(a) of Regulation (EU) 2018/1725], as mandated by the Treaties, in particular by articles 5, 11, 20, 21-40, 42, 43 of the of the Treaty on European Union (TEU) and 2 (4) and (5), 205, 220-221, 326 – 334 of the Treaty on the Functioning of the European Union (TFEU). In this context, selection and administrative management related to SNEs are necessary for the management and functioning of the EEAS as referred to in Recital 22 of Regulation (EU) 2018/1725.

Legal basis:

- Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 4 February 2014 establishing the rules applicable to National Experts Seconded to the European External Action Service (HR DEC(2014) 01)

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?

- In case of selected applicants, personal data related to the selection and administrative management of Seconded National Experts are kept for 10 years after the termination of the secondment.
- Personal data of recruited candidates are stored in Sysper according to the retention policy of the Sysper IT system.
- In case of non-selected applicants, data are retained for 2 years, after the closure of the selection exercise, unless complaints are made to the European Ombudsman or the decision is challenged in court.
- In case of a complaint to the Ombudsman or a litigation, to allow for the exhaustion of all appeal channels, including appeals before the Court of Justice of the European Union and the required follow-up to judgments, the personal data shall be kept no longer than:
  - 2 years after the final decision in case of complaint before the Ombudsman
  - 5 years with an additional maximum of 2 years after the judgment on the pending case is final in case of a litigation, i.e. 5 years from the date on which the European Parliament grants discharge for the budgetary year in which the final judgment was delivered (5 + 2 years)
- Payment related financial documents linked to reimbursement of travel expenses related to the selection, recruitment, mobility and rotation exercises are kept for 5 years from the date on which the European Parliament grants discharge for the budgetary year to which the data relates, i.e. 5 + 2 years.
- When appropriate, personal data contained in supporting documents are deleted where possible as long as these data are not necessary for further purposes, e.g. control, inspection and audit, in particular in accordance with article 75 of the Financial Regulation.

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. Data is processed by assigned staff members. Access to specific files requires authorisation. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. These measures, such as firewalls, checkpoints and anti-virus filters aim at implementing a level of security appropriate to the risks presented by the processing and the nature of the personal data to be protected. General access to personal data is only possible to recipients with a UserID/Password. For connections from outside the protected network of the EU institutions, two-factor authentication is required. Physical copies of personal data are stored in a properly secured manner.

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.