EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA RELATED TO SECURITY VERIFICATIONS, BACKGROUND CHECKS FOR EMPLOYEES OF EXTERNAL CONTRACTORS REQUIRING ACCESS TO EEAS PREMISES

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?

Purpose

The purpose of the present processing activity is to collect and use your personal data to make an informed decision on whether to grant access to you, as employee of an external contractor of the EEAS, to the EEAS premises.

Description

Belgian authorities and eight EU Institutions and Bodies (European Commission, European Parliament, European Council, Council of the European Union, European External Action Service, European Economic and Social Committee, Committee of the Regions, European Defence Agency) have signed in May 2019 a Memorandum of Understanding (MoU) for the implementation of Security Verifications of external contractors.

In order to safeguard the security interests of EU institutions and bodies pursuant to Article 4(3) of the Treaty on European Union and Article 18 of the Protocol on the Privileges and Immunities of the European Union of 8 April 1965, the Belgian Authorities will facilitate the implementation of security verifications consisting of the consultation and evaluation of data transmitted by the intelligence and security services as well as of judicial data transmitted by the police services, if appropriate. The security verification requests will be managed by the competent Administrative Authority of the Belgian State (SPF Affaires étrangères, Commerce extérieur et Coopération au développement - Direction Protocol, Rue des Petits Carmes 15, 1000 Bruxelles). Inappropriate access to EU premises could cause damage to the protection of the external security of the State and the international relations of Belgium, in particular if the physical security or the reputation of the European Institutions and Bodies were harmed.

The verification will take place on the request of the European Institutions and Bodies and will result in either a positive or negative security advice for each individual assessed. This security certification will be issued by the Belgian National Security Authority. As an employee of an external contractor who needs access the EEAS premises, you are required to be subject to a security verification and for this reason you will need to give your data necessary to conduct the security verification in order to obtain a security advice. If you refuse to be subject to a security verification, you may express your refusal by indicating it via registered mail to your employer or to the Data Controller (see point 4). In this case you will not be given access to the EEAS premises. Your employer will electronically transmit your data listed under point 3 in an Excel sheet which will be forwarded in a secure way to the Administrative Authority.

Rationale

On request of the European Institutions and Bodies, the Administrative Authority agreed that the access to EU premises for employees of external contractors would benefit from security verification as determined by section 22quinquies of the Act of 11 December 1998. This verification shall be carried out by the authority referred to in section 15, subsection 1 of the same Act. The permission by the Administrative Authority is legally justified as per the grounds mentioned in section 22 quinquies of the aforementioned Act.

3. DATA PROCESSED: What data do we process?

The data, including personal data, which may be processed by the EEAS and its HQ Security and Security Policy Division are as follows:

- Last name and first name
- Address
- Function or profession
- Nationality
- Date and place of birth
- Belgian national number (for Belgian citizens)
- ID or passport number (for non-Belgian citizens)
- Country of Issue
- Employer, company ID number and email address
- Photo
- Outcome (positive/negative) of the security verifications without justification details

Data is managed by electronic means (e.g. excel sheet) as agreed by the parties of the MoU referred to in point 2. Providing personal data is mandatory to meet the contractual requirement on services delivered on the premises of the EEAS. If you do not provide your personal data, possible consequences are refusal of access rights to EEAS premises.

Additional information on the processing:

Outgoing data

The assigned staff member (Point of Contact - POC) of the EEAS will transmit the personal data to the Administrative Authority electronically in a secure way.

Incoming data

The POCs of the EU Institutions & Bodies will store the outcome of the security verification by the National Security Authority (NSA) of Belgium. They will share the negative outcomes of the security verifications with the other EU institutions and bodies, parties to the MoU of May 2019, taking into account Recital 21 of Regulation (EU) 2018/1725 for the transmission

Outcome of the security verifications

The EEAS will only receive a positive or negative outcome. The employee will be informed by the Administrative Authority in a well-reasoned letter in case the security advice is negative.

The EU institutions will not have access to any justification of the outcome.

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 Directorate General for Resource Management
HQ Security and EEAS Security Policy Division – RM.SCS.3

E-mail contact address: SECURITY-VERIFICATIONS@eeas.europa.eu
Postal address: 9A Rond Point Schuman, 1046 Brussels, Belgium

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

The recipients of your data may be:

- Assigned EEAS staff members (Points of Contact), including the Division of HQ Security and EEAS Security Policy (EEAS.RM.SCS.3)
- Designated members and management, including the Directorate General for Resource Management and the Directorate for Security and Real Estate
- Other concerned EU institutions and bodies' assigned staff members involved in the verification procedure, including the POC (Point of Contact) of the concerned EU institutions and bodies
- Belgian Authorities, including the Belgian Ministry of Foreign Affairs, the National Security Authority (NSA)
- National Security Authorities of countries whose nationals are subject to the security verification. (This data processing and exchange of information is handled solely by the Belgian Authorities
- Contractors of external security companies in charge of EEAS access control services, who for the performance of their duties need access to the IT system (subject to their "need to know") and to follow the instructions of the EEAS Internal Security in application of the EEAS access policy

Personal data processed for the purpose of the present security verification implemented by the Administrative Authority of the Belgian State is handled and accessed through the *SPF Affaires Etrangères / FOD Buitenlandse Zaken (Address:* Rue des Petits Carmes 15, 1000 Bruxelles, Belgium, Phone: +32 2 501 81 11, Contact through the following webform link: http://diplomatie.belgium.be/en/Contact

Access to your personal data is provided by the form you completed to the EEAS staff responsible for carrying out this processing activity and to authorised staff according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

The above-mentioned form is sent to the Belgian Ministry of Foreign Affairs, which will have access to your personal data.

Agreed in the MoU (Section IV. 4.1), when a negative security advice is received, the EEAS will inform other institutions and bodies participating in the MoU about the security advice.

Personal data is not intended to be transferred by the EEAS to a third country nor to an international organisation. Your personal data will *not* be used for an automated decision-making including profiling. The given information will not be communicated to third parties, except where necessary for the purposes outlined above and when the EEAS may be required to do so by law.

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. 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. 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 functional mailbox:

SECURITY-VERIFICATIONS@eeas.europa.eu

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

Lawfulness of the processing is in accordance with Article 5 (1) (a) and (b) of Regulation (EU) 2018/1725.

The EEAS processes your personal data, because:
(a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;
(b) processing is necessary for compliance with a legal obligation to which the controller is subject.

Processing pursuant to Article 5 (1)(a) refers to the EEAS' task of ensuring security in the EEAS as provided for by EEAS Security Rules (Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the EEAS - ADMIN(2017) 10).

Processing by the Belgian national authorities is carried out according to the following Belgian legal and regulatory framework on security verifications:

- Act of 11 December 1998 on classification and security clearances, security certificates and security advice, its accompanying Royal Decree of 24 March 2000 and the Royal Decree of 8 May 2018 modifying the Decree;
- Royal Decree of 8 May 2018 establishing the activity sectors and the competent administrative authorities as referred to in Article 22 quinquies, § 7,
- Royal Decree of 8 May 2018 establishing the list of data and information that can be consulted in the context of the execution of a security verification.

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?

The EEAS and its Division for HQ Security and EEAS Security Policy only keeps your personal data for the time necessary to fulfil the purpose of collection and further processing. Personal data is, therefore kept for a period of 5 years from obtaining the security advice, plus 6 months for an administrative retention. The 5 year period corresponds to the validity of the security advice.
II. Files related to the contracting arrangement and supporting document regarding the security verification are to be kept for up to 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) for control, inspection and audit purposes for control by Internal Audit, Ex-post Control Services and the European Court of Auditors

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. General access to personal data is only possible to recipients with a UserID/Password. All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the EEAS or of the European Commission. Physical copies of personal data are stored in a properly secured manner.

The processing activity is carried out pursuant to the EEAS Security rules (Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the EEAS - ADMIN(2017) 10).

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.