EEAS PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF PROCESSING PERSONAL DATA RELATED TO
PERSONNEL SECURITY CLEARANCE (PSC) MANAGEMENT FOR EEAS STAFF BY THE EEAS SECURITY CLEARANCE TEAM VIA E-CLEARANCE AND ACCESS TO CLIMB E-LEARNING

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 [e.g. 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 is the management of the Personnel Security Clearance (PSC) process necessary for the follow-up of the security vetting procedure, archiving of the national opinions as provided by the National Security Authority (NSA), issuance of the Security Authorisation and Personal Security Clearance Certificate by the EEAS Designated Security Authority.

This includes also registration of the PSC status of staff and administration of the EU Learn course CLIMB (Classified Information Mandatory Briefing) in respect of access to EU Classified Information (EUCI) and secured areas defined in the EEAS Security Rules (ADMIN(2017) 10) .

In addition, a person (internal staff, external staff, visitor) can be granted unescorted access to a Secured area or Classified meeting only if he/she is security cleared (in a possession of a valid PSC). For EEAS internal staff, this person shall be authorised by the EEAS Security Authority (has a valid PSC and has to be regularly briefed on his/her responsibilities to protect EU Classified Information).

A PSC Certificate for EEAS staff is issued to certify their security clearance for the purpose of participation in classified meetings outside the EEAS.

According to the Decision of the Director General for Budget and Administration on EEAS PSC Requirements and Procedures (2019) 7, the briefing is done via the EU Learn course CLIMB (Classified Information Mandatory Briefing).

The EEAS assumes to carry out the entire management of the security clearance process for its staff members in accordance with Annex A I of the EEAS Security Rules (ADMIN 2017 (10). As of 15 June 2021, the EEAS Security Clearance Office will take over the elements of the administration of this process which used to be handled by the European Commission.

The EEAS Staff members on PSC position, requiring access to EUCI on a regular basis to perform their tasks and/or requiring access to secured areas on a regular basis to carry out their duties, have to be vetted by their National Security Authority and hold a valid Personnel Security Clearance.

In accordance with the Note on EEAS Management of PSC for its staff (Ares(2021)3290935), the "EEAS will:

- launch the PSC procedure with the concerned staff members (as previously);
- forward (endorse) the filled-in national forms to the respective National Security Authorities (NSA) in accordance with the specific Member State (MS) requirements;
- receive the final decisions by the NSAs;
- consult and inform the NSAs on specific issues; and
- communicate directly with the NSAs on all PSC related matters"

The process will consists of the following steps:

1. PSC Application

- EEAS Staff members requiring PSC receive according to the NSAs requirements, national PSC forms to apply. Those are sent by the EEAS security clearance office by e-mail to the applicants via email, along with the link to CLIMB, EEAS mandatory security briefing.

- The member of the EEAS Clearance Team register the date on which national forms and the link to CLIMB are sent to applicants in e-Clearance.
- Upon receipt, applicants fill in the national forms, provide annexes in accordance with requirements of their NSAs.
- When completed, the documents will be returned to the EEAS Clearance Office according to the requirements of the NSA (either by internal mail in a sealed envelope (diplomatic pouch for EU DELs), either via SECEM-encrypted email to EEAS Clearance Office FMB, or via an online application related to the NSA (Belgium and other MSs).
- Returned files in some cases (depending on the national requirements) will be physically or digitally stamped and signed by the Designated Security Officer – Team Leader of EEAS Security Clearance Team – or by a member of the EEAS Security Clearance Team in his/her absence, in accordance with the requirements of the NSAs.
- The filled in PSC questionnaires will be sent to the NSAs according to the requirements of the NSAs: either via registered post to the Permanent Representations in Brussels, either by registered post to the NSAs or via encrypted email to the NSAs.
- Member of EEAS Clearance Team will register in e-Clearance the date on which national forms are sent to NSAs.
- Upon receipt, NSA of applicant will carry out the vetting process and will inform EEAS Clearance Office of the outcome, in accordance with the requirements of the NSA: either by email or via registered post (delivered only with signature of the recipient) (this takes aproximatelly from 1 up to 18 months depending on the NSA procedures).

2. PSC Registration

A member of EEAS Clearance Team will open the outcome file to register the PSC details* in PSC management system e-Clearance**. According to the Art 20, Annex I, "a database on the security clearance (PSC) status of all staff placed under the responsibility of the EEAS and of EEAS contractors' personnel shall be maintained by the EEAS".
In addition, a person (internal staff, external staff, visitor) can be granted unescorted access to Secured area or Classified meeting only if he/she is security cleared (in a possession of a valid PSC or Authorisation to access EUCI).
For EEAS Internal staff, this person shall be Authorised by the EEAS Security Authority (has a valid PSC and has been regularly briefed on his/her responsibilities to protect EU Classified Information).
According to the DG RM Decision on EEAS PSC Requirements and Procedures (ADMIN (2019) 7), the briefing is done via the EU Learn course CLIMB (Classified Information Mandatory Briefing).

*PSC details consist of date the PSC is issued and period of validity.
**e-Clearance corporate system is a tool supporting the Security Division to fulfil the above requirements and purpose. It contains PSC and CLIMB information on all personnel requiring or requesting access to EUCI or Secured areas.

3. PSC Certificate Generation

- e-Clearance automatically generates a PSC Certificate for staff participating in classified meetings outside the EEAS. This Certificate is a pdf document and is sent from the functional mailbox of the EEAS Security Clearance Team to the security officer of the inviting organisation.

4. PSC Filing

- PSCs will be filed in matching country folder and stored in EEAS Clearance Office strongbox. Access to the office is managed by an electronic lock.

For EEAS staff: officials, CA, TA, SNE and external contactors added in Sysper **:**
e-Clearance retrieves the following information directly from Sysper:

- Per ID, Name, surname, Country of birth, Nationality, Date of birth, Gender, Department, Statutory Link, Assignment End Date, Administrative Address.
- CLIMB certificate (pdf) signed by the person, and the date the course was completed

For External Staff: EU MSs Permanent Representations, NATO EU Cell staff, contractors, visitors and participants in classified meetings, military or civilian crisis management exercises:
The Security office of the person sends his/her PSC to the EEAS Security Clearance Office. The information related to: Name, Surname, Nationality, date of birth and gender is taken from the PSC itself and registered manually into e-Clearance.

For all:

The personal record contains in addition the level of the PSC, the date the PSC was granted and its period of validity.

<u>CLIMB (an EU Learn based online course)</u>

The concerned staff will receives automatic invitation (email with link to CLIMB) from the e-Clearance system and personnel will be invited to do the briefing. Once successfully completed the briefing completion data will be transferred automatically from EU Learn Database to e-Clearance.

On this basis, e-Clearance will send to the participant (only internal staff) via e-mail the course certificate (pdf) with integrated (new) features allowing to sign electronically (Name, Surname, Data, time, EEAS Logo). The signature is based on EULogin Authentication. Once signed the signature date of will be saved in e-Clearance.

3. DATA PROCESSED: What data do we process?

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

EEAS staff or staff with Sysper record
Per ID, Name, surname, Country of birth, Nationality, Date of birth, Gender, Department, Statutory Link, Assignment End Date, Administrative Address.
(All imported from SYSPER automatically).
CLIMB certificate (pdf) signed by the person, and the date the course was completed

Manually added for **external staff**
Name, Surname, Nationality, date of birth and gender.

For all: the level of the PSC, the date the PSC was granted and its period of validity

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 entrusted with managing the personal data processing under the supervision of the Head of Division is the following organisational entity:

HQ Security and EEAS Security Policy, RM.SECRE.2

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

The recipients of your data may be:

- Members of the EEAS Clearance team
- Members of the EEAS Security Policy sector (CLIMB course responsible – Read only)
- Internal Accreditation Team (Read only)
- EEAS Security managers (Read only)
- Investigators (Read only)

Personal data is not intended to be transferred to a third country or an international organisation, except where necessary for providing access to recipients as described above. In case of international transfers appropriate safeguards are ensured in accordance with Chapter V of Regulation (EU) 2018/1725. The given information will not be communicated to third parties, except where necessary for the purposes outlined above.

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

You have the right of access to your personal data and the right to correct your inaccurate, or incomplete personal data taking into account the purpose of the processing. 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 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 wish 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:

EEAS-SECURITY-CLEARANCE@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 by the EEAS in the public interest, in particular for the management and functioning of the EEAS [Article 5(1)(a) of Regulation (EU) 2018/1725] as referred to in Recital 22 thereof in order to ensure the security of EU Classified information and of secured areas as well as to comply with the legal requirement in the Security Rules (Article 5(1)(b) of Regulation (EU) 2018/1725.

Legal reference:

- EEAS Security Rules (ADMIN(2017) 10)
- DG BA Decision (ADMIN (2019) 7) on EEAS PSC Requirements and Procedures
- According to Art 20, Annex I, "a database on the security clearance (PSC) status of all staff placed under the responsibility of the EEAS and of EEAS contractors' personnel shall be maintained by the EEAS"
- Note on EEAS Management of Personnel Security Clearances for its Staff (Ares(2021)3290935)
- DG BA Note on Identification of "sensitive" posts in the EEAS Headquarters (Ares(2018)6066768)
- DG BA SI Director Note on Organisation of the Security Clearances Management Process and Delegation of Signature (Ares(2021)3290935)

Further 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 FOR DATA STORED & SECURITY MEASURES: For what period and how we process your data?

Storage period:

Personal data is kept for a maximum period of:

- **For Internal staff** or staff with Sysper record: 5 years after the person has left the EEAS or 5 years from the expiration of the last PSC record, whichever comes first.
- **For External staff:** 5 years after the expiration of the PSC

For the purpose of investigation, the files subject to investigations can be kept as long as legal claims arising from the investigations expire.

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. Physical copies of personal data are stored in a properly secured manner.

Access rights are given only to authorised and security cleared staff of the EEAS HQ Security and Security Policy. Every request is scrutinised and approved by the delegated controller/ e-Clearance Business manager.

- The data are stored in servers hosted in secure premises, protected by physical security measures, and using the EEAS IT Infrastructure.
- Administrative measures include the obligation of all EEAS & Commission personnel with access to the system to be individually security checked, and duly supervised by EEAS RM.SECRE.2 staff.
- All EEAS personnel with access to the system shall sign non-disclosure and confidentiality declarations.
- The EEAS personnel described under the point 'Recipients' are security cleared and authorised to access EUCI at minimum level SECRE UE/ EU SECRET.
- Access rights are granted to data on a strict need-to-access basis.
- Only the system administrator specifically appointed by the controller for this purpose is able to grant, alter or annul access rights of any persons. Any provision, alteration or annulment of access rights is made pursuant to strict criteria.

The EEAS keeps at all times records of all persons having access to the system and of their access rights in detail.

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.