EEAS Personal Data Processing Record

Ref. Article 31 of Regulation (EU) 2018/1725 - Legal obligation for maintaining records

1	Title of the processing activity	**Travel Clearance Application (TCA) and the related personal data processing**
2	Update of the record (last modification date)	17/04/2024
3	Register reference number	2621
4	Identity and contact details of the Data Controller Joint Controller (if applicable) Data Processor (if applicable)	EEAS Data Protection Officer: Emese Savoia-Keleti DATA-PROTECTION@eeas.europa.eu
5	Identity and contact details of the Data Protection Officer	EEAS Data Protection Officer (DPO): Emese Savoia-Keleti. SG.AFFGEN.DPO Functional Mailbox of the DPO: DATA-PROTECTION@eeas.europa.eu
6	Purpose of the processing activity	Description: The mission performer will fill out the first section of the Travel Clearance Application (TCA) form, which contains his/her personal information and the details of the mission including the itinerary. The EEAS intends to avoid exposing staff to risks they are not ready to take unless absolutely necessary for service reasons. Therefore, in advance information about inclination to travel to a risky area is also asked for at the initial phase. The form will be then sent to his/her line manager for description of the criticality of the mission. It will then be sent onwards to the Regional Security Officer/Advisor responsible of the area where the mission will take place to include a security risk assessment and the operational plans. Finally the TCA will be sent to the appropriate level of approval, most cases to the Head of Delegation. Some cases may require an approval at Managing Director level, in such cases, the TCA will be sent with the Head of Delegation' comment to the Field Security Division colleagues for opinion and then it will be submitted to the Geographical Managing Director for final decision. The information about the mission in the TCA Form gives a comprehensive overview about the risks and the foreseen mitigation measures. During the final approval of the mission, the mission performers have to declare that they are ready to perform the mission under such conditions.
7	Legal basis and lawfulness	Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 September 2017 on the security rules for the European External Action Service - ADMIN(2017) 10. - EEAS Security Rules Art. 3: duty of care obligation - EEAS Security Rules Art 19 on the advice to be provided to staff performing missions to high threat areas - EEAS Security Rules Art 11 Security Risk Management principles 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	Categories of individuals whose data is processed - Data subjects	Mission performers from EEAS HQ and all staff posted in Union Delegations.

9	Categories of data - Data processed	The data, including personal data, which may be processed for that purpose are the following: - Name/Last Name - Place of employment - Employment status - Function - Level of security trainings and experience - Willingness to travel - Detailed itinerary of mission including: mission locations, arrival and departure dates, means of transport and accommodation details - Mission justification - Security Risk Assessments and Operational Plans - Advice, comments and final decision
10	Recipients of data – Access to data	The recipients of your data may be: Mission performers concerned by the TCA request Mission performer's line manager, Head of Division/Delegation, other members of the Security Management Team (Regional Security Advisor/Officer, etc.); for higher threat areas also assigned staff of the Field Security Division Staff, Managing Director responsible for the Geographical area and delegates; assigned staff in EU Delegation: and Crisis management or investigation team (in case of emergency). 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 or in case of emergency.
11	Transfer to Third Countries or International Organizations (IOs) and suitable safeguards (if applicable)	N/A
12	Time limit for keeping the data - Retention period	The data contained in the Travel Clearance form is kept for a maximum period of 1 year, except for any case of investigation when data that is stored in the TCA form needs to be kept longer linked to an incident.
13	Data Storage	2 categories of storage: 1. Hard Copy on paper Physical copies of personal data are stored in a properly secured manner. Hard copies need to be printed by the mission performers themselves to have the operational plans (i.e. emergency numbers, addresses of hospital in the vicinity, communication procedures, transport plans) available. During the mission, the plan is kept with the mission performer. After the mission was performed, printed Travel Clearance Applications, i.e. hard copies are kept in locked cupboards. Access is restricted. After the 1 year retention files are to be shredded. 2. Electronic Data Electronic data are stored on servers that abide by pertinent security rules. Access limitation: 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. TCA forms are processed via SECEM emails.

EEAS Personal Data Processing Record

Ref. Article 31 of Regulation (EU) 2018/1725 - Legal obligation for maintaining records

14	General description of security measures	see above
15	Rights of individuals	The approved or declined TCA will be always returned to the applicant. Data subjects have the right of access to their 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, data subjects have the right to ask the deletion of personal data or restrict their use. In specific cases, restrictions under Article 25 of the Regulation may apply. To exercise their rights data subjects can contact the Data Controller via the functional mailbox: SG-CRC-3@eeas.europa.eu
16	Information to data subjects	In the TCA form itself, the mission performer has the link to the Privacy Statement, that is published in the EEAS Intranet, together with the description of the procedure and the template forms.