

# EEAS Personal Data Processing Record

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

1	Title of the processing activity	<b>Use of blacklisted airlines and other non-certified airlines authorisation form by the EEAS (EU Delegations)</b>
2	Update of the record (last modification date)	03/01/2024
3	Register reference number	3181
4	Identity and contact details of the Data Controller Joint Controller (if applicable) Data Processor (if applicable)	European External Action Service Rond Point Schuman 9A, 1046 Brussels, Belgium Data Controller contact entity: SG.CRC.3 - Field Security Functional mailbox: sg-crc-3@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	<p>The purpose of the processing is to record and transfer information of EU staff in need of using EU banned airlines and other non-certified airlines for missions or authorised travel. In order to ensure that the EEAS/EU Delegations exercised due diligence in assessing that no alternative means of transport are viable and that the importance of the mission justifies the risks to which the mission performer is exposed by using such airlines, the form needs to be filled. The Line Manager has to authorise the use of these airlines based on the opinion of the RSO covering the country of departure and/or the RSO covering the country of arrival or in transit depending on the existing alternatives to avoid the use of the blacklisted airline. It has to be ensured that staff use these less secure means of transport only in case of necessity. In addition, the form ensures that the mission performer gives his/her explicit consent to using such airlines.</p> <p>It is necessary to record and transfer information to the insurance company regarding the use of EU banned airlines and other non-certified airlines</p> <p>.</p>
7	Legal basis and lawfulness	<p>Lawfulness: The processing of personal data is necessary for the performance of a task carried out by the European External Action Service in the public interest, in particular for management and functioning of the EEAS [Article 5(1)(a) of Regulation (EU) 2018/1725] as referred to in Recital 22 thereof.</p> <p>It is also necessary for compliance with a legal obligation (Article 5 (1) b).</p> <p>Legal basis : 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: Article 3 on the duty of care obligation. 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.</p>
8	Categories of individuals whose data is processed - Data subjects	EU staff in Delegation or in EEAS HQ using in EU banned airlines and other non-certified airlines when on mission or authorised travel.

# EEAS Personal Data Processing Record

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

9	Categories of data - Data processed	<ul style="list-style-type: none"> <li>- First Name/Last Name</li> <li>- Airline</li> <li>- Flight details: <ul style="list-style-type: none"> <li>From (city) / to (city)</li> </ul> </li> <li>Outbound flight: departure date and time; arrival date and time</li> <li>Return flight, departure date and time; arrival date and time</li> </ul>
10	Recipients of data – Access to data	<p>The recipients of your data may be:</p> <p>Within the EEAS/EU Delegations:</p> <ul style="list-style-type: none"> <li>- superior of mission performer, RSO, Administration section of the EU Delegation, Head of Delegation and other members of the Security Management Team (Regional Security Advisor/Officer, etc.);</li> <li>- assigned staff dealing with security matters in EEAS Field Security Division;</li> <li>- assigned staff dealing with the administration of travel insurance in the EEAS Headquarters;</li> </ul> <p>Outside the EEAS: insurance company</p>
11	Transfer to Third Countries or International Organizations (IOs) and suitable safeguards (if applicable)	N/A

# EEAS Personal Data Processing Record

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

12	Time limit for keeping the data - Retention period	<p>1 year after the end of the trip.</p> <p>Personal data may be kept for information and historical, statistical or scientific purposes for a longer period of time including the publication on the EEAS Intranet with appropriate safeguards in place. Archiving shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of individuals. Reports and other material containing personal data are archived according to e-Domec policy.</p> <p>In case of an incident, event or enquiry by authorities, data subjects or other concerned individuals' personal data will be preserved as long as the legal claims arising from the investigations expire or any follow-up action is due. This includes pending cases, appeals and court judgments to allow for the exhaustion of all appeal and other channels of legal remedies. In any case, personal data will not be kept longer than 5 years after the judgment on the pending case is final.</p> <p>When appropriate, personal data contained in supporting documents should be deleted where possible, if that data is not necessary for audit, inspection or other control purposes.</p>
13	Data Storage	<p>Each EU Delegation/EEAS Division will store the Use of Blacklisted Airlines and other non-certified Authorisation Forms electronically on the Shared drive and/or in paper form in locked cupboards. EU Delegations/EEAS Divisions will destroy the forms once the period of one year is over.</p>
14	General description of security measures	<p>Blacklisted Airlines and other non-certified airlines Authorisation Forms are sent via corporate e-mail to the insurance company. The e-mail system is protected by a userID and password.</p> <p>Electronic versions are stored on drives with access protected by a userID and password.</p> <p>Physical copies of personal data are stored in a properly secured manner, hard copies are collected and kept in locked cupboards.</p>
15	Rights of individuals	<p>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 their personal data or restrict their use as well as to object at any time to the processing of their personal data on grounds relating to their particular situation.</p> <p>The EEAS will consider the request, take a decision and communicate it to the data subject 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. Data subjects are informed in the Privacy Statement that they can find more information in Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725.</p> <p>In specific cases, restrictions under Article 25 of the Regulation may apply. If data subjects wish to exercise their rights or have questions concerning the processing of their personal data, they may address them to the functional mailbox that each EU Delegation will provide.</p>
16	Information to data subjects	<p>Individuals are informed during the collection of data, as they will have to complete and sign the form in which they are informed about data protection provisions applied in the processing of personal data. A Privacy statement will be made available or will be reachable via a link.</p>

# EEAS Personal Data Processing Record

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