EEAS Personal Data Processing Record

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

1	Title of the processing activity	**USE OF FINGERPRINTS FOR ACCESS CONTROL TO SECURED AREAS IN THE EEAS**
2	Update of the record (last modification date)	19/04/2024
3	Register reference number	3601
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	The EEAS processes biometric data with the aim of ensuring increased secure access control to specific zones and protection of EEAS / EU information and data. If data subjects need access to specific zones protected by biometric devices, fingerprints may be processed. Encoding and storage of the encrypted data is on the personal access pass, which remains in the possession of the pass holder. Description: The external contractor that acts as Data Processor is in charge of collecting the data: processing fingerprints and writing the encrypted data on the badge.. Authorisation of access is covered by the process of managing entry rights to EEAS premises via access badges. The access rights to secured areas are provided as per request of responsible of the area, provided that the person fulfils the access requirements to secured areas (need to know, PSC or escort). The same applies for the withdrawal of the access rights (SCS.3 should be informed of the changes on the post, leaving the entity or not needing access any more to an area). The fingerprint 'minutiae' are not stored on the data subject's badge chip. O nly the encrypted data is stored after its digital encoding via a dedicated stand-alone system. This system compiles the data through an encryption algorithm and as soon as the encoding process is completed, all previously collected data is automatically deleted from the device. When fingerprints identification is used for access control, verification is made at badge reader level, by comparison between the encrypted data on the badge chip and the scanned fingerprint. There is no local or central storage during the encryption or identification processes. There is no Artificial Intelligence tool used for real-time' remote biometric analysis of the fingerprints.

EEAS Personal Data Processing Record

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

7	Legal basis and lawfulness	Lawfulness: The processing of the personal data is necessary for the performance of a task in the public interest and for the management and functioning of the EEAS [Article 5(1)(a) of Regulation (EU) 2018/1725 as referred to in Recital 22 thereof]. Legal basis: Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19June 2023 on the security rules for the European External Action Service 2023/C 263/04 Article 4, ANNEX A, Article 6, par 3 and 4, ANNEX A II, CHAPTER II and IV Decision of the Director-General for Resource Management of the European External Action Service of 6/12/2023 on the designation of Administrative Areas and accreditation of the Secured Areas within EEAS NEO Science 27 building, in particular article 2 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	Staff with the need to access secured areas at EEAS HQ. This may include - EEAS and European Commission or Council statutory staff - Assigned external partners with the need to access secured areas at EEAS HQ - Member State Representatives External Contractor staff
9	Categories of data - Data processed	For all data subjects, fingerprints will be processed. For all badges regardless the access rights to a secured area: - First name and surname - Statutory Link - EEAS Personnel number - ID picture - Date and end of contract - Nationality - Company name (if applicable) - Management position
10	Recipients of data – Access to data	No individual or entities may have access to the fingerprints. The encrypted data is on the personal badge, which remains in the possession of the pass holder. Recipients of other data are the contractor (necessary to identify the individuals entitled to hold badges with encrypted biometric data) and EEAS staff involved in requesting, processing, providing and authorising access with badges.
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	Only encrypted data is stored on the badge. The badge is in possession of the data subject and is destroyed when the individual link to the EEAS is ended or the staff member changes the badge (e.g. because of a change of assignment, extension of contract) Data on the stand-alone device processing, encrypting and writing the fingerprints is deleted after having been written to the badge.

EEAS Personal Data Processing Record

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

13	Data Storage	There is no fingerprint storage: only the encrypted data is stored on the data subject's badge (see point 6) Data on the stand-alone device processing, encrypting and writing the fingerprints is deleted after having been written to the badge. Other data regarding access rights to a secured area are stored on secured servers of the EEAS.
14	General description of security measures	The fingerprint minutiae are not stored, only the encrypted data is stored, and only on the badge. Impossible to decrypt back to the hash of the fingerprint. Contractor staff performing the scanning is properly instructed and signs a specific confidentiality declaration. Badge holders are instructed to handle the badges securely. The badges that have been returned to the Accreditation office (e.g. because of end/change of assignment) are securely destroyed.
15	Rights of individuals	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. 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. In specific cases, restrictions under Article 25 of the Regulation may apply. If data subjects want to exercise their rights or have questions concerning the processing of their personal data, they may address them to the Data Controller via the functional mailbox: RM-SCS-3@eeas.europa.eu RM-SCS-3@eeas.europa.eu
16	Information to data subjects	A specific Privacy Statement is available for data subjects on the EEAS website. The Privacy Statement will also be displayed on the place of scanning the fingerprints.