EEAS Personal Data Processing Record

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

1	Title of the processing activity	**The EEAS Visitors' Management System: e-Visitor**
2	Update of the record (last modification date)	07/10/2021
3	Register reference number	2421
4	Identity and contact details of the Data Controller Joint Controller (if applicable) Data Processor (if applicable)	Data Controller: European External Action Service Rond Point Schuman 9A, 1046 Brussels, Belgium Data Controller organisational entity in charge of managing the processing activity: HQ Security and EEAS Security Policy (RM.SECRE.2) Functional mailbox: EEAS-Security-Accreditation@eeas.europa.eu Processor: Proxyclick, Rue Saint-Hubert 17, 1150 Brussels, Belgium 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	Purpose(s) - The EEAS visitors' management system aims at managing all processes related to the organisation of a visit to the EEAS premises. It facilitates a smooth check-in process, provides a high level of security and reliable information on the number of visitors inside the building as well as increases the safety of visitors. - It also ensures the protection of EEAS security and safety interests, including staff under the responsibility of the EEAS, EEAS premises, physical assets, information and visitors. - The purpose of processing data required in the context of the COVID-19 pandemic prevention measures is to ensure fulfilling the necessary public health measures and to protect EEAS/EU Delegations' staff and third parties, including external visitors by containing and preventing the spread of the Coronavirus (COVID-19) in the current emergency context. Description Registration of the visit will be implemented through the application e-Visitor on the EEAS Intranet where all statutory staff (HOST) will be able to 'pre-register' their visitors. During the pre-registration phase the HOST will need to type in first name, last name, ID/ Passport number and nationality of the visitors as mandatory fields. Email and phone numbers remain optional fields. The HOST can modify the data at all times. The access to the dashboard (the IT application) is granted through EU Login credentials. Once this is completed, and when the visitor presents him/herself at the main entrance reception desk (Capital building- HQ, Kortenberg 150 or Belmont) he/she will be able to proceed with the check-in. The first name, last name, nationality and passport/ ID number will be deleted automatically after 2 years (kept for this period for the purpose of security reasoned investigation) at the Cloud Customer's server. In the framework of the protection against the spread of the COVID-19 pandemics, visitors are requested to answer two questions concerning whether they have been in contact with anyone who tested positive with Covid-19 in the last 14 days and whether they have any of symptoms of fever, tiredness, dry cough, loss of smell/taste. These answers can be sent via e-mail before the meeting or registered in e-visitor the latest when checking in. Answer options are 'yes' or 'no'. If the answer to any of the questions is 'yes', the visitor will be requested to reconsider the form of the visit and make arrangements for an alternative solution, including a video-conference with the host.
7	Legal basis and lawfulness	Lawfulness The processing of personal data is necessary for the performance of a task carried out in the public interest and in the exercise of official authority vested in the EEAS, namely to preserve the security of its buildings. The processing is lawful under Article 5(1) (a) of Regulation (EU) 2018/1725. Data, including health-related information is processed based on Article 10.2 (i): public interest in the area of public health, in addition to Art. 5.1 (a): necessary for the public interest in the exercise of duty of care and Art. 5.1 (e) vital interest of individuals. Legal Basis - 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. - Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community(OJ 45, 14.6.1962, p. 1385) - Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19/09/2017 on the security rules for the European External Action Service (ADMIN(2017)10).
8	Categories of individuals whose data is processed - Data subjects	- EEAS Staff (HOST) who pre-register the visit - EEAS Visitors who take part in the visit, including representatives of Member State organisations, public authorities, private enterprises or civil society, educational institutions etc. * EU institutions, in particular based in Brussels, are exempt

9	Categories of data - Data processed	For EEAS HOST / FPI HOST/ EUSR HOST (Staff of the EU Special Representatives) - [“meeting organiser”]: First name, Last name, EEAS, EUSR (professional) email address or Commission (professional) email address, Office address, office telephone number, user mobile number (optional) For EEAS VISITOR / FPI VISITOR/ EUSR VISITOR [“invited participant, guest”]: First name, Last name, Nationality, Passport or ID number, E-mail (optional), Phone number (optional), company (optional), validity of the Security Clearance if EU Classified meeting is organised in KO building, time and date of check in and check out. In the context of the COVID-19 pandemic prevention measures additional information is processed: Data on whether the visitor has been in contact with anyone who tested positive with Covid-19 in the last 14 days Data on whether the visitor has any of symptoms of fever, tiredness, dry cough, loss of smell/taste
10	Recipients of data – Access to data	EEAS staff of the organisational entity acting as meeting organiser (HOST); In respect of data required in the context of the COVID-19 pandemic prevention measures the meeting organiser will be notified in an e-mail only about the fact that at least one of the answers was “Yes” Staff of the Service for Foreign Policy Instruments (FPI) of the European Commission, when FPI acts as the meeting organiser, has access to the same data as the meeting organiser in the EEAS. EEAS staff who act as administrators/host of the system Assigned staff of HQ Security and EEAS Security Policy (RM.SECRE.2) with access to Yes/No replies on screen Contractors of external security companies in charge of EEAS accreditation 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 Contractor of external company Proxyclick which is the service provider of the system and acts as Cloud Customer has only access if absolutely required for troubleshooting purposes, under the binding clauses of the Data Processing Agreement (DPA). Even though not considered as recipients under Regulation (EU) 2018/1725, investigating entities of the EEAS, the EU and Police forces in the exercise of their official authorities may be granted access to personal data processed by the e-Visitor system. This is subject to the authorisation by the relevant EEAS Authority.

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	For EEAS HOST: Data is kept until the host staff member is employed by the EEAS as it is part of the user provisioning and access rights to the system and for subsequent 5 years until the exhaustion of all claims related to a possible disciplinary action. For EEAS VISITOR: Automatic deletion of data after 2 years. Data concerning risk factors in the context of the COVID-19 pandemic prevention measures are to be kept for 30 days taking into account the general incubation and quarantine period of fourteen days plus one day prior to the visit (for testing and feedback of results) equalling fifteen days doubled for the purposes of staff safety, contact tracing and duty of care (timeframe to be adjusted according to updated information issued by ECDC or WHO for the incubation period, as needed). Data will be automatically deleted after 30 days. For the Covid questionnaire data will not be retained further for an audit trail than the 30 days defined in the system, except for the scenario described below. In case it is required to keep data longer exclusively for reasons of protection of public health , including when a positive case being detected or traced back to a particular meeting makes it necessary to ensure the possibility to warn individuals who are at risk of contamination, data may be furthermore needed and therefore specific information on particular days/visits will be retained for the time period required to be informed about eventual positive test of any participant of the meeting as well as for the time-period technically needed for subsequent manual deletion of the selected data.
13	Data Storage	Data are stored in the e-visitor system.
14	General description of security measures	Security measures 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. 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. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. Security is also ensured by EU Login account authentication through unique password, associated with only one email address with double authentication. The e-Visitor system is cloud-based to which the EEAS has administrator rights. The cloud provider selected for the tool provides sufficient assurance to act on behalf of EU Institutions and to implement the necessary technical, organisational and data protection measures as well as to verify the effectiveness of those measures (effective security strength in data traffic encryption, copies of audit certificates) based on legally binding contract clauses including the protection of personal data. Responses to the questions asked in the context of the COVID-19 pandemic prevention measures are only visible to persons on a need-to-know basis.

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 have questions concerning the processing of their personal data, they may address them to the Data Controller via the functional mailbox: EEAS-Security-Accreditation@eeas.europa.eu
16	Information to data subjects	A specific Privacy Statement is accessible for data subjects on the IT tool, e-Visitor. The Privacy Statement is also available on the website of the EEAS.