EEAS Personal Data Processing Record

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

1	Title of the processing activity	**Schoolmaster IT application as part of the Goalkeeper software environment**
2	Update of the record (last modification date)	04/01/2024
3	Register reference number	1861
4	Identity and contact details of the Data Controller Joint Controller (if applicable) Data Processor (if applicable)	European External Action Service (EEAS) Rond Point Schuman 9A, 1046 Brussels, Belgium EEAS.PCM.1 - Integrated Approach for Peace and Security Email: secretariat-esdc@eeas.europa.eu Processor The Schoolmaster IT application and data processing operation is under the management responsibility of the European Security and Defence College (ESDC)
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	Schoolmaster aims to capture the largest possible amount of information on training opportunities relevant to the EU Common Security and Defence Policy (CSDP), and to crisis management in general, and to make this body of information easily accessible at a central location online . It is also used to manage training requirements for CSDP, including the focal points for training areas. Personal data stored within the system is twofold, I. public interface and II. back-office. I. The purpose of the public interface is to enable for the public audience to subscribe by providing an email address to receive notifications of courses ; option for unsubsrcibing is provided. The purpose for interested individuals to subscribe is to get alerts about training offers provided through Schoolmaster. The purpose of the back-office is to manage the different users rights within the system and to enable users to grant access to their Compartments (Institutional Coordinators) or Networks (Network Coordinators) in order to publish courses. The purpose of login information is to follow the level of activity and to report Member States about the state of play within the overall use of the system. The purpose of data regarding CCTs and MDLs is to share this body of information for back-office users in order to foster pooling and sharing. The purpose of providing contact points is that the users can turn to them for more information or other questions or requests regarding specific trainings.

7	Legal basis and lawfulness	Lawfulness: The processing of the personal data is necessary for the performance of a task carried out by the European External Action Service in the public interest and 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. Legal references: n May 2015 Council Conclusions on CSDP: 8971/15 n EU Policy on Training for CSDP, doc. ST 7838 2017 INIT, dated 3 April 2017. n Implementing Guidelines for the EU Policy on Training for CSDP, doc. 11437/22, dated 15 July 2022. n Council Decision (CFSP) 2020/1515 of 19 October 2020 establishing a European Security and Defence College 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	Subscribed user to the public interface User role in Schoolmaster (Schoolmaster Admin, Compartment Admin, Institutional Coordinator, Network Coordinator) Civilian Coordinator for Training and Military Discipline Leader Training organiser’s contact persons

9	Categories of data - Data processed	I. Data processed through the public website of the Schoolmaster IT application: For contact persons for courses: Name Contact Details (e-mail, type of contact, professional phone number (optional), professional postal address/ city/ country/ postal code (optional), fax number (optional) For subscribers to the Schoolmaster alert service Name e-mail address II. Data processed through the back-office website of the Schoolmaster IT application : Given Name, Family name (for Admin, Network Coordinator, Compartment Admin, Institution Coordinator) Professional e-mail address Professional telephone/fax number and postal address (optional) Role w ithin the system Last access to the system (for Admin, Network Coordinator, Compartment Admin, Institution Coordinator) Member since (for Admin, Network Coordinator, Compartment Admin, Institution Coordinator)
10	Recipients of data – Access to data	Designated EEAS staff responsible for the Schoolmaster IT application in the EEAS, IT Division and in the European Security and Defence College (ESDC): RM.SCS.5 – IT project development/maintenance team PCM, CPCC, EUMS assigned staff ESDC (European Security and Defence Collage) assigned staff.

11	Transfer to Third Countries or International Organizations (IOs) and suitable safeguards (if applicable)	The access to the back-office may be granted in the future to course organisers in Third States and IOs, who wish to publish courses in the Schoolmaster, to be part of CSDP Training Programme. They will have access to relevant Network and other Third States information therein (name and email of the focal points), and they will see only the information regarding CCTs and MDLs (functional/professional email). Course organisers in third countries will have access only to their own data. Transfer of personal data to these course organisers will be in compliance with Chapter V of Regulation (EU) 2018/1725. EEAS will regularly review the access rights of third states and IOs in close consultation with the Data Protection Office and ESDC.
12	Time limit for keeping the data - Retention period	Personal data are stored as long as the user is active in the system unless a request for deletion of data is filed by data subjects. Data of users inactive for more than two years are removed unless they need access due to their job function. Data of users whose job function ceases, are removed on notification. Data are only kept longer, until the expiry of legal claims, in case of incidents or if necessary for investigations or if legal proceedings are in progress. After the Schoolmaster application has ceased to be operational, the data will be destroyed at the central server level by the EEAS after the period of 1 year.
13	Data Storage	Online platform/IT tool – managed by EEAS Digital Solutions Division (RM.SCS.5), system is hosted at DIGIT data center and all the data are stored there. The data are accessible through the internet using authentication procedures and secure protocols.
14	General description of security measures	Specific EEAS IT security measures are as follows: the access to the Schoolmaster back office environment is made through the use of the EU Login service to prevent any unauthorized disclosure or access to the application; accidental loss of data is prevented by the DIGIT infrastructure and backup procedures. The hosting site has geographical redundancy; the unauthorised access to the storage media as well the rights to read, copy or modify data on the storage media is prevented through the DIGIT and EEAS IT security specific rules and by the architecture of the system; the personal data stored in the system can be modified by authorised users having access to the back office section in which the data have been uploaded (Schoolmaster Institutional Coordinators); for contact details uploaded by data users through the e-mail alert subscription service, data can be modified by authorised users in the EEAS (EEAS IT Division) upon request of the data subject; preventing unauthorised persons from using data-processing systems by means of data transmission facilities is implemented by using https protocol, which is a standard protocol for secure systems; at the application level the following issues are addressed by using appropriate authentication and authorization procedures: Ø ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers; Ø ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body; The application has auditing and logging procedures implemented, allowing tracking of users' actions

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: goalkeeper.schoolmaster@eeas.europa.eu . Technical queries about the functioning of the Goalkeeper-Schoolmaster application can be addressed to the following functional mailbox managed by the EEAS : goalkeeper.schoolmaster@eeas.europa.eu
16	Information to data subjects	A specific Privacy Statement is available for data subjects on the intranet/internet. The Privacy Statement is also attached to related communication and available on the main page of Schoolmaster.