EEAS Personal Data Processing Record

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

1	Title of the processing activity	**EEAS Business Continuity**
2	Update of the record (last modification date)	04/01/2024
3	Register reference number	2641
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: Directorate General for Resource Management, Coordination Division (EEAS.RM.01) – Sector for Briefings, Business Continuity and Internal Communication (EEAS.RM.01.01) Functional mailbox: HQ-BUSINESS-CONTINUITY-PLAN@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 purpose of the present processing activity is to ensure business continuity (BC) in Headquarters and Union Delegations in case of unforeseen disruptions of service by establishing the appropriate plans and procedures in order to maintain critical and essential functions. This includes the collection and storage of personal data that enable the EEAS to identify and contact EEAS staff members where necessary to allow exercising duty of care for automatised sending of e-mails and/or text messages (SMS).
7	Legal basis and lawfulness	Lawfulness The processing of your personal data is necessary for the performance of a task carried out by the EEAS in the public interest, in particular for the management and functioning of the EEAS [Article 5(1)(a) of Regulation (EU) 1725/2018] as referred to in Recital 22 thereof. Legal reference Article 18 of the Decision of the High Representative of the Union for Foreign Affairs and Security Policy on the Security Rules for the EEAS, dated 19/09/2017 - ADMIN(2017) 10 EEAS Headquarters BUSINESS CONTINUITY PLAN (Ref. Ares(2019)6539106 - 23/10/2019) Decision of the High Representative of the Union for Foreign Affairs and Security Policy on general implementing provisions giving effect to the Staff Regulations and to the Conditions of Employment of Other Servants, dated 22/11/2011 - PROC HR(2011) 0013

		Decision of the High Representative of the Union for Foreign Affairs and Security Policy Amending Annex I of the Decision of the High Representative PROC HR(2011) 013, of 22 November 2011, on General Implementing Provisions for giving effect to the Staff Regulations and to the Conditions of Employment of Other Servants, dated 03/02/2014 - HR DEC(2014) 02 Decision of the High Representative of the Union for Foreign Affairs and Security Policy to extend the application of certain Commission Rules developing the provisions of the Staff Regulations and of the Conditions of Employment of Other Servants, to the EEAS, dated 29/11/2011 - PROC EEAS(2011)002 Decision of the Chief Operating Officer of the European Action Service Amending the Annex to the Decision of the Chief Operating Officer PROC HR(2011) 002 of 29 November 2011, To extend the application of certain Commission Rules developing the provisions of the Staff Regulations and the Conditions of Employment of Other Servants, to the EEAS", dated 13/02/2014 – EEAS DEC(2014) 009 Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities, in particular Article 55 concerning hours of work, overtime, shift-work, standby duty at place of work or at home Further reference EEAS Business Continuity Operations Manu al Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010/427/EU) – OJ L 201 of 3/8/2010, p. 30.
8	Categories of individuals whose data is processed - Data subjects	All EEAS staff members in EEAS Headquarters and EU delegations.

9	Categories of data - Data processed	The following categories of staff personal data automatically collected from Sysper may be processed in the context of business continuity: In Headquarters (HQ): - Name and surname - Function - Professional contact details (phone number, office number, e-mail address) - Private contact details (phone number, address, e-mail address) In Delegations: - Name and surname - Function - Professional contact details (phone number, office number, e-mail address) - Private contact details (phone number, address, e-mail address) - Nationality - Family situation If required, additional details for the specific emergency situation are collected and processed. In Headquarters (HQ): - Data in BC documents - Staff members may be asked to self-identity in case of vulnerability (medical condition 'yes' or 'no' – but no actual processing of medical details in the course of BC processing activities) in order to allow the employer to exercise duty of care In Delegations: - Location data - Data in BC documents and in EEAS Security IT application for Delegations (ESDAP / EEAS Security Portal) - Staff members may be asked to self-identity in case of vulnerability (medical condition 'yes' or 'no' – but no actual processing of medical details in the course of BC processing activities) in order to allow the employer to exercise duty of care

10	Recipients of data – Access to data	The recipients of your data may be EEAS assigned staff and line managers in your Division/Delegation to collect and store required data for the purpose of a BC locally. In order to handle an emergency situation dedicated staff of the following centralised HQ entities may also have access to your data: EEAS Business Continuity Team (BCT) is the body in charge of managing business continuity at HQ level. It is composed of the DG RM management, a representative of the SG Office and services in charge of security, IT, HR and budget. In specific situations it may need to call on other HQ services. Delegation Security Management Team (SMT): The SMT may have access in order to ensure Business Continuity and security and safety of staff. Departmental Security Coordinators are in charge of maintaining and updating BC process data (phone numbers, evacuation procedures, identification of staff in need of special assistance) and defining a Business Impact Analysis, with attention given to political events (such as major conferences) or organisational changes. RM.SECRE.1 (Field Security): The Field Security Division is in charge of providing security risk management advice and solutions, leadership of the RSO network, physical security of Delegations and staff accommodation. EEAS Medical Cell in cases where medical advice is needed. 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.
11	Transfer to Third Countries or International Organizations (IOs) and suitable safeguards (if applicable)	
12	Time limit for keeping the data - Retention period	It is essential to maintain data in business continuity documents up-to-date and only as long as needed for BC purposes. Personal data is kept for the period of employment of the individual staff member or until the next update of contact lists. BCP overview and contact lists are updated regularly, at least once a year. In the IT application - used for facilitation of day-to-day security in the Delegation as well as for providing crucial information for Delegation staff and assets in case of crisis, the EEAS Security Portal, an all-in-one online portal bringing together security relevant information for Union Delegations - a backup of the data could be kept, in general, for a maximum period of 5 years after the end date of assignment in a Delegation. The specific Privacy Statement is available on the intranet under ‘ Security in Del ’.

13	Data Storage	In the IT application - used for facilitation of day-to-day security in the Delegation as well as for providing crucial information for Delegation staff and assets in case of crisis, the EEAS Security Portal, an all-in-one online portal bringing together security relevant information for Union Delegations - a backup of the data could be kept, in general, for a maximum period of 5 years after the end date of assignment in a Delegation. The specific Privacy Statement is available on the intranet under ‘ Security in Del ’.
14	General description of security measures	
15	Rights of individuals	You have the right of access to your 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, you have the right to ask the deletion of your personal data or restrict their use as well as to object at any time to the processing of your personal data on grounds relating to your particular situation. We will consider your request, take a decision and communicate it to you 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 . For more information, please see 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 you have questions concerning the processing of your personal data, you may address them to your respective Division or Delegation administration (as the delegated controller) or to HQ BCT via the mailbox: HQ-BUSINESS-CONTINUITY-PLAN@eeas.europa.eu
16	Information to data subjects	Information for data subjects is provided in a Privacy Statement