EEAS Personal Data Processing Record

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

1	Title of the processing activity	**IT Division Cyper Security (Phishing) Awareness Campaign**
2	Update of the record (last modification date)	04/01/2024
3	Register reference number	1841
4	Identity and contact details of the Data Controller Joint Controller (if applicable) Data Processor (if applicable)	European External Action Service Round Point Schuman 9A, 1046 Brussels, Belgium Data Controller contact entity: Digital Solutions - RM.SCS.5 Functional mailbox: EEAS IT HELPDESK
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 purpose of the present processing activity is to deliver a number of predefined messages (simulated phishing attacks) aiming at evaluating the awareness level of the organization and provide education. Description: EEAS user's name, department and mail addresses will be uploaded into the provided service (SaaS service) to be able to deliver the content to the users. Users will receive e-mails which they can recognise as phishing. If they click on the link provided or respond to the e-mail, they will be notified that they did not recognise a simulated phishing attack. Their attention is called to study material on the subject (reminders will be send if it is not done until the due time). Following the exercise the difficulty level of the simulated phishing exercises will be matched to the user's skill level. A simulated phishing exercise is used to check if the training was successful. If users (EEAS staff) report the e-mail as a phishing attempt, they are notified that they acted correctly. The follow-up of failing to recognise the phishing attempt are: 1. Immediate feedback on the landing page behind the phishing link (with explanations of red flags that should have been recognised) 2. Providing training material from the ICT Security team on how to recognise phishing messages (reminders will be sent if not done) - implemented on the platform 3. As a future follow-up the ICT Security team provides the colleague with simulated phishing exercises that matches to user's skill level and gradually improves the difficulty level according to the level of the user. No adverse consequences are associated with clicking on the link or responding to the e-mail and the identity of staff members is solely used for the purposes outlined above. Staff can register for security training through the normal training registration procedures as well (see e-DPO 1002).

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 your personal data is necessary 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: - EEAS Security Rules ADMIN(2017) - Staff Regulations of Officials and the Conditions of Employment of Other Servants of the EU - Article 1 (Nature and Scope), 2 (Tasks) of the Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010/427/EU) available on http://www.eeas.europa.eu/background/docs/eeas_decision_en.pdf – OJ L 201, 3/8/2010, p. 30. - EEAS IT vision for Horizon 2022 - EEAS cyber security awareness program
8	Categories of individuals whose data is processed - Data subjects	All EEAS staff and contractors with an EEAS e-mail account and personnel detached from other EU institutions or Member States with an EEAS e-mail account
9	Categories of data - Data processed	Name Department Email addresses Training course status

EEAS Personal Data Processing Record

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

10	Recipients of data – Access to data	- EEAS RM.BS.3 ICT Security team (assigned EEAS officials) - EEAS Security awareness task force for security education purposes - Service provider assigned staff, on a need-to-know basis, on documented instruction of the EEAS The selected service provider is KnowBe4 (https://www.knowbe4.com/), a US enterprise. The service is isolated and hosted in the EU. The fact that the data are processed in the European Economic Area (EEA) implies that the service provider assures to have in place a fully controlled production environment and Security Operation procedures stack to ensure compliance with data privacy regulations, namely Reg. (EU) 2016/679, the General Data Protection Regulation and Reg. (EU) 2018/1725 on the processing of personal data by the EU institutions. Knowbe4, however, is a U.S. company. The company signed a Data Processing Agreement with the EEAS including the standard contractual clauses approved by the European Commission and obliging Knowbe4 to comply with EU data protection rules. The service provider, KnowBe4, will process data on documented instructions and on behalf in accordance with the provisions of the aforementioned regulation. More information on how KnowBe4 processes personal data can be found on the website of the contractor: https://www.knowbe4.com/legal and https://www.knowbe4.com/product-privacy-notice
11	Transfer to Third Countries or International Organizations (IOs) and suitable safeguards (if applicable)	No
12	Time limit for keeping the data - Retention period	The simulated phishing exercise data will be retained for 36 months. Data of staff participating in a security training will be kept for a total of 36 months.
13	Data Storage	The data will be available in the service provider's software.
14	General description of 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. In its electronic format the data will be stored in a cloud located within the EU. The collected data are processed by assigned staff members. The database is accessible only to the recipients with the authorised administrative or viewer rights. Measures are provided to prevent unauthorised entities from access, alteration, deletion, disclosure of data. 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. Security is also ensured by the safety measures built in IT application used. With regard to the service provider, KnowBe4, as a contractor, will process personal data in accordance with Article 29 of Regulation (EU) 2018/1725. Support and operations teams have access for the sole reason of providing support and services through the KnowBe4 system which is separate from the corporate infrastructure. All accesses should be individual grated to KnowBe4 by EEAS and will be logged.
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 IT HELPDESK

EEAS Personal Data Processing Record

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

16	Information to data subjects	Data subjects are informed by a Privacy Statement communicated via e-mail and the Privacy Statement is available on the Intranet.