EEAS Personal Data Processing Record

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

1	Title of the processing activity	**Security monitoring of ICT and cyber security incident management by EEAS Security Operations Centre (SOC)**
2	Update of the record (last modification date)	15/12/2020
3	Register reference number	2521
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: IT Division (BA.BS.3) Security Operations Centre (SOC) Functional mailbox: BA-BS-3@eeas.europa.eu Processors: External consultants working intra muros in the Security Operations Centre (SOC) team based on contract. In case of a severe cyber security incident when coordinated response is required, additional resources (CERT-EU, external incident responders from other EUIs or external companies) might be involved. Proofpoint, U.S.A. 925 West Maude Avenue Sunnyvale, CA 94085 Fireeye, U.S.A. 601 McCarthy Blvd. Milpitas, CA 95035 Data Protection Officer: Emese Savoia-Keleti, SG.AFFGEN.DPO 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

EEAS Personal Data Processing Record

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

6	Purpose of the processing activity	Purpose(s): cyber security incident management to ensure appropriate level of availability, confidentiality and integrity as well as protect data in EEAS Communication and Information Systems (CIS). Description: - Constant monitoring in EEAS CIS and collecting machine data for the purpose of detecting cyber threat and mitigating cyber incident: - Network related events (e.g.: firewall logs, meta data, URL logs, short retention packet collection, all Secure Sockets Layer (SSL) encrypted internet service is subject to decryption- Authentication events - E-mail tracking event - Security events (e.g.: antivirus, sandbox events) Step 1: utilise the non-encrypted machine data collected for automated searches and analysis to identify possible indicators of compromise, without human intervention. Step 2: In case of cyber security incident obtain evidences that could support the security analysis and mitigation efforts.
7	Legal basis and lawfulness	2018/C, 126/01, EEAS Security Rules ADMIN(2017) 10, Article 7 and Article 10 2017/46, Commission Decision on the security of communication and information systems in the EC, Article 15 due to 2010/427/EU, Article 10 2017/1584 Commission recommendation on coordinated response to large-scale cybersecurity incidents and crises 2016/1148 Directive (EU) concerning measures for a high common level of security of network and information systems across the Union
8	Categories of individuals whose data is processed - Data subjects	Any natural person using a network, services or terminal equipment operated under the control of EEAS.
9	Categories of data - Data processed	Step 1: Machine data (network, authentication, e-mail tracking and security events) is processed for automated searches and analysis without human intervention. Step 2 in case of malicious content found the following data may be processed: Name User-ID Email address IP address URL visited Time stamp Malicious links and attachments in emails

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	1. SOC team have access of the data for cyber security incident management. 2. EEAS Security investigation sector will have access of the data for incident investigation. 3. EEAS Security awareness task force will have access of the data for security education purposes in case of incident.
11	Transfer to Third Countries or International Organizations (IOs) and suitable safeguards (if applicable)	Transfer to Fireeye and Proofpoint, U.S. DPA signed between the processors and the EEAS. Processors fill in a SAAS questionnaire detailing security, data protection and storage aspects. Only a subset of the malicious traffic is designated as unknown and only this is sent to FireEye for further analysis. To reduce the risk private data is sent to FireEye: • the data is searched for personal and confidential information by automated processes. If personal information is spotted, it is immediately and permanently deleted. • false positive are permanently deleted • prior to transmitting the information, it is cleansed of specific sensitive parameters such as IP addresses, parameters in the URL and email addresses. Proofpoint stores the data in the EEA and only transfers it to the U.S. if necessary for analysis of for information sharing for threat identification development.
12	Time limit for keeping the data - Retention period	Maximum 6 months, and afterwards it will be archived. In case of investigation of security incident it might be recovered by the decision of EEAS Directorate responsible for security.
13	Data Storage	The data is stored within separated management network only accessible from pre-defined workstation
14	General description of security measures	There are administrative, physical and technical security measures implemented. SOC team members are selected based on predefined screening. SOC team members have privileged access rights based on roles and using 2 factor authentications. The data is stored within separated management network only accessible from pre-defined workstations, with enforced server and network level authentication with additional security controls and audit history.
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.

EEAS Personal Data Processing Record

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

16	Information to data subjects	A Privacy Statement contains all information provided to the Data Subject(s).