EEAS Personal Data Processing Record

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

1	Title of the processing activity	**Analysis of Foreign Information Manipulation and Interference (FIMI) threats**
2	Update of the record (last modification date)	18/12/2023
3	Register reference number	3441
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: EEAS.SG.STRAT.2 - Strategic Communications 2: Task Forces and Information Analysis Division Functional mailbox: STRAT-DATA-ANALYSIS@eeas.europa.eu 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) Foreign Information Manipulation and Interference (FIMI), including disinformation, is a growing political and security challenge for the European Union. The purpose of analysing FIMI is to provide evidence-based insights on FIMI incidents, campaigns and activities carried out by foreign actors to inform adequate (effective and proportionate) responses across the EU. These responses are designed to protect free and open societies, democratic institutions and processes, security and universal values. The European Council's mandate underlying the STRAT.2 work stipulates that the work of the division should focus, inter alia, on the detection and analysis of information manipulation and interference activities by foreign states. Therefore, the Information Analysis, Open Source and Data Strategy Team in the EEAS.SG.Strat.2 . ("Data Team") is tasked with developing a methodology to collect and analyse data on Foreign Information Manipulation and Interference (FIMI). Description The data collection and processing is limited to publicly available online data. Tools used by the data processors collect both personal and non-personal data made expressly public by different entities on the internet. Such data is processed manually and preserved if necessary and relevant within the mandate; and constitute the basis for the development of internal analyses as well as public or internal studies on FIMI targeting the EU, its values and processes. The Data Team does NOT carry out any investigation into private or closed online communication channels. Any data-related operations from data collection to storage are either entirely manual or operate under a human-in-the-loop principle. Any data requiring storage is hosted in dedicated spaces with strict access control and retention rules. Preserved data encompasses selected online material encountered during an investigation as well as archived web links. Other data are used to store information on the data collected and the outcome of investigations.
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.

Description of the relevant provisions outlining our mandate:

Joint Communication Action Plan against Disinformation of 05 December 2018 on the EU's joint response to tackling disinformation (JOIN/2018/36)

Under the paragraph " Pillar 1:improving the capabilities of union institutions to detect, analyse and expose disinformation " the European Commission underlines that to address effectively the threat of disinformation, it isnecessary to reinforce the Strategic Communication Task Forcesof the EEAS with "additional specialised staff, such as experts in data mining and analysis to process the relevant data.It is also important to contract additional media monitoring services to cover a wider range of sources and languages and additional research and studies on the reach and impact of disinformation. In addition, there is a need to invest in analytical tools such as dedicated software to mine, organise and aggregate vast amounts of digital data". (1)

The Council Conclusions of 13-14 December 2018 stress the need for a determined response to disinformation, that addresses the internal and external dimensions of the threat and that is "comprehensive, coordinated and well-resourced on the basis of an assessment of threats". In operative terms, such assessment is given by a prior situational awareness. In line with the Action Plan against Disinformation, it calls on the EC and EEAS to step up their efforts. (2)

In the Council Conclusions of 20-21 June 2019 , the European Council calls for sustained efforts under the supervision of the HRVP to raise awareness, increase preparedness and strengthen the resilience of our democracies to disinformation. The work of the STRAT.2 is geared towards this objective too. (3)

In December 2019, the General Affairs Council Conclusions , with regard to the work of EEAS StratCom to tackle foreign disinformation, information manipulation and interference, confirmed the following three work strands: 1) pro-active communication and awareness raising; 2) support to independent media and; 3) detect, analyse and challenge such activities of the threat actors. Our mandate as Knowledge and Data team falls under the third point. (4)

In 2020, the Communication on the European Democracy Action Plan COM(2020) 790 has further expanded on the need of developing common best practices to fight disinformation. Under paragraph " 4.1 Improving EU and Member State capacity to counter disinformation " it calls on the EEAS to develop a common framework and methodology for collecting systematic evidence on foreign interference, as well as to promote a structural dialogue with civil society, private industry actors and other relevant stakeholders to regularly review the threat situation. The specific mandate of "collecting systematic evidence on foreign interference" falls under the remits of the STRAT.2. (5)

Council's Strategic Compass for Security and Defence (7371/22) aims at strengthening cooperation among Member States to enhance their resilience and ability to prevent, detect, mitigate and counter hybrid. Information manipulation, being part of the hybrid threats spectrum, is addressed in the call for further developing a Foreign Information Manipulation and Interference (FIMI) Toolbox, of which the situational awareness is an integral part. (6)

Legal reference(s):

(1) European Commission, 2018, Joint Communication Action Plan against Disinformation on the EU's joint response to tackling disinformation (JOIN/2018/36) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52018JC0036

(2) General Secretariat of the Council, European Council meeting (13 and 14 December 2018) – Conclusions (EUCO 17/18) https://www.consilium.europa.eu/media/37535/14-euco-final-conclusions-en.pdf

(3) General Secretariat of the Council, European Council meeting (20 June 2019) – Conclusions (EUCO 9/19) https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf

(4) General Secretariat of the Council, Complementary efforts to enhance resilience and counter hybrid threats – Council

		(4) General Secretariat of the Council, Complementary efforts to enhance resilience and counter hybrid threats - Council Conclusions (10 December 2019) - (14972/19) https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf (5) European Commission, 2020, Communication on the European Democracy Action Plan (COM/2020/ 790) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFINqid=1607079662423 (6) General Secretariat of the Council, 2022, A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security (7371/22) https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf Further legal reference: (7) 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0427
8	Categories of individuals whose data is processed - Data subjects	Data subjects: - FIMI actors, including authors and disseminators - Individuals appearing in the materials reviewed, collected and analysed. In order to align the purpose of data collection with its storage (more in the next parts) the EEAS Strat.2 monitors accounts linked to foreign governments engaging in overt influence campaigns in the EU. Please note that often there is no specific and recognisable person behind a channel or an account, but groups or organisations, hence no personal data are collected. Individuals' accounts operating inside of the monitored channels may be captured in the monitoring. However, their data is not considered and is discarded.
9	Categories of data - Data processed	Data is collected through open source methodology following a privacy-by-default approach. The data should be relevant for investigation, minimised, and connected to delivering results in line with the mandate (no out-of-scope collection); and no consideration of private groups or chats. EEAS Strat.2 only processes data within its mandate of monitoring FIMI. We do not seek to collect personal data beyond those relevant for investigation during this process, but we may incidentally process such data (for example, if mentioned in social media posts). Types of data relevant for investigation that could be processed if available: account name website domain name website activity language geographic information screenshots and archived snapshots of publications and other visuals links

10	Recipients of data – Access to data	Data is accessible on a need to know basis by the following recipients: Assigned EEAS staff Rapid Alert System (RAS) members in the EU MS and EU Member States governments Assigned officials in other European institutions or agencies Third countries partner governments Some internet platforms, Any personal information gathered from monitoring tools onto our IT systems is visible to our data processors, such as external contractors, IT suppliers providing email, document management and storage services. Our reports may be shared with EEAS staff, EU institutions, EU governments' stakeholders and selected international or civil society partners, always on a need-to-know basis. Public reports will always be anonymised, and will not capture any personal data gathered from media monitoring.
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	Usefulness and necessity of information is reviewed every year until confirmed. Relevant data are kept for a maximum of five years unless a review after these five years indicates that data are still relevant. Data is deleted if it no longer useful to the original purpose of collection. Produced public reports will not include personal data unless belonging to public figures and in line with the mandate of the EEAS Strat.2. Data gathered by social media monitoring tools will be stored according to the company's protocols. For more information regarding the privacy notice of current tool providers please consult the following webpages: Talkwalker , Buzzsumo , SEMrush , OpenCTI , Hunchly
13	Data Storage	- Hunchly : Hunchly is a web capture tool. It runs in the browser and automatically collects, documents, and annotates every website visited by the user. - OpenCTI : Unified threat analysis platform and knowledge management database. According to the terms of service of the cloud-services agreement with the company Filigran the "Customer acknowledges that correspondence and log files generated in conjunction with a request for Cloud Services may contain sensitive, confidential, or personal information. Customer is solely responsible for taking the steps it considers necessary to protect the data, including obfuscating the logs or otherwise guarding the information (…)". Hence the EEAS is applying a strict access policy to this tool and ensures data minimisation standards for the information saved on this platform. Certain data is stored on internal servers and accessible only to the EEAS Strat.2
14	General description of security measures	Appropriate organisational measures are ensured for external contractors in their role as Data Processor. In particular, the data stored are located on a server managed by the Data Controller and secured with password/UserID. User policies are in place and will be further developed for accessing the archives according to the user's role.

15	Rights of individuals	General rule: 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: STRAT-DATA-ANALYSIS@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.