Ref. Ares(2023)8084350 - 27/11/2023

European Union
EXTERNAL ACTION

PRIVACY STATEMENT - DATA PROTECTION NOTICE

FOR THE PURPOSE OF

PROCESSING PERSONAL DATA IN THE ANALYSIS OF FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI) THREATS

1. INTRODUCTION

The protection of personal data and privacy is of great importance to the European External Action Service (EEAS), the General Secretariat of the Council (GSC) and the European Commission (EC). Data subjects have the right under EU law to be informed when their personal data is processed [collected, used, stored] as well as about the purpose and details of that processing.

When handling personal data, we respect the principles of the Charter of Fundamental Rights of the European Union, and in particular, Article 8 on data protection. Personal data are processed in accordance with Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, aligned with Regulation (EU) 2016/679, the General Data Protection Regulation. This privacy statement contains information about how the EEAS process personal data and what rights data subjects have in relation to the analysis of FIMI (Foreign Information Manipulation and Interference) threats performed by the Information Analysis, Open Source and Data Strategy Team in the EEAS.SG.Strat.2.

2. PURPOSE OF DATA PROCESSING

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 data collection and processing is limited to publicly available online data. Tools used by the data processors collects both personal and non-personal data made expressly public by different entities on the internet. Such data are processed manually and preserved if necessary; 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 infiltration in private 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 the investigations.

3. DATA PROCESSED

The data controller (EEAS.SG.Strat.2) and its data processors (tool providers and external contractors) monitor data in publicly available media outlets, including social media, by using commercially available media and social media monitoring tools and web capture tools. The tools collect both personal and non-personal data made expressly public by the users themselves. Since data protection is an integral part of our analysis process, we apply a privacy-by-default approach and use data minimization techniques.

IMPORTANT: We do not actively collect sensitive personal data, but we may process such data while monitoring social media where the abovementioned data is included.

The 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 include:

- account name
- website domain name
- website activity
- language

- geographic information
- screenshots and archived snapshots of publications and other visuals
- links

4. DATA CONTROLLER

Concerning the personal data, the data controller determining the purpose and the means of the processing activity is the European External Action Service (EEAS). The EEAS Division responsible for managing the personal data processing under the supervision of the Head of Division is the following organisational entity:

EEAS.SG.Strat.2 - Strategic Communications: Task Forces and Information Analysis Division

5. RECIPIENTS OF THE PERSONAL DATA

Raw data are only accessible to assigned EEAS staff and the analysts. Reports are accessible on a need-to-know basis by the following recipients:

- Assigned EEAS staff
- Rapid Alert System (RAS) members 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.

Internal or restricted reports are 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.

For important reasons of public interest, linked to the possible online and offline harms generated by targeted FIMI campaigns, there may be sharing of information with like-minded partners in International Organizations, like NATO, or third countries like the US, Canada or the UK. This sharing complies with the requirements of Chapter V. of Regulation (EU) 2018/1725.

6. ACCESS, RECTIFICATION, and ERASURE OF DATA

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 described among others in Articles 14 (4), 18, 19(1) (a-f), 20 (1) (a-d) and 22 (1) (a-b) of Regulation (EU) 2018/1725, data subjects have the right to ask the deletion of personal data or restrict their use as well as to object at any time to the processing of personal data on grounds relating to their particular situation. We will consider any request, take a decision and communicate it to the data subjects. 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. Questions concerning the processing of personal data, can be addressed to the respective Data Controllers via the functional mailbox below.

Data subjects will be requested to provide additional information to confirm their identity in case they would request access to their data or exercise their other rights. The EEAS will fulfil only requests where the identity of the requester can clearly be attributed to the personal data concerned by the request.

Rectification can be done by enabling data subjects to provide a supplementary statement and it is only justified if the information collected is not properly registered or attributed.

For enquiries please contact:

STRAT-DATA-ANALYSIS@eeas.europa.eu

7. LEGAL BASIS

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 reference:

(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 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%3AFIN&qid=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. TIME LIMIT - DATA STORING:

Data retention

The EEAS will retain identifiable information that is obtained from search tools in order to compile internal and public reports. Sensitivity and relevance of information in relation to the mandate of the EEAS Strat.2 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 are deleted if it no longer useful the original purpose of collection.

Produced public reports will not include any personal data unless belonging to public figures and in line with the mandate of the EEAS Strat.2. Data gathered by social media monitoring companies will be stored according to the company's protocols. For more information regarding the privacy notice of our tool providers please check the following webpages: Talkwalker ,Buzzsumo, SEMrush, OpenCTI , Hunchly

Security of data

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. Data is processed by assigned staff members. Access to specific files requires authorisation. 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.

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 for accessing the archives according to the user's role.

9. EEAS DATA PROTECTION OFFICER

In case of enquiries, the EEAS Data Protection Officer is reachable at data-protection@eeas.europa.eu.

10. RECOURSE

Data subjects have, at any time, the right to have recourse to the European Data Protection Supervisor at edps@edps.europa.eu.