

**RECORD OF PROCESSING ACTIVITY  
ACCORDING TO ARTICLE 31 REGULATION 2018/1725<sup>1</sup>  
NOTIFICATION TO THE DATA PROTECTION OFFICER**

**NAME OF PROCESSING OPERATION<sup>2</sup>:**

**Data collection, processing in annotation of online content and analysis of online content for the purpose of a research project on online content moderation**

Reference number: DPR-2021-142
Creation date of this record: 17/05/2022
Last update of this record: 24/08/2022
Version: v0.2

Part 1 (Publicly available)

<b>1) Controller(s)<sup>3</sup> of data processing operation (Article 31.1(a))</b>
<p>Controller: European Union Agency for Fundamental Rights (FRA) Schwarzenbergplatz 11, A-1040 Vienna, Austria Telephone: +43 1 580 30 – 0 Email: <a href="mailto:contact@fra.europa.eu">contact@fra.europa.eu</a> Organisational unit <b>responsible<sup>4</sup></b> for the processing activity: Justice, Digital and Migration Unit Contact details: <a href="mailto:OCM-project@fra.europa.eu">OCM-project@fra.europa.eu</a> Data Protection Officer (DPO): <a href="mailto:dpo@fra.europa.eu">dpo@fra.europa.eu</a></p>

<b>2) Who is actually conducting the processing? (Article 31.1(a))<sup>5</sup></b>
<p>The data is processed by the FRA itself <input checked="" type="checkbox"/></p> <p>The data is processed also by a third party (contractor) [mention the third party] <input checked="" type="checkbox"/> <b>RAND Europe, data processor</b></p>

<sup>1</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>

<sup>2</sup> **Personal data** is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.

**Processing** means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

<sup>3</sup> In case of more than one controller (e.g. joint FRA research), all controllers need to be listed here

<sup>4</sup> This is the unit that decides that the processing takes place and why.

<sup>5</sup> Is the FRA itself conducting the processing? Or has a provider been contracted?

**Rue de la Loi 82 / Bte 3**

**1040 Brussels**

**Belgium**

**Tel: +32 2 669 2400**

**Westbrook Centre, Milton Road**

**Cambridge CB4 1YG**

**United Kingdom**

**Tel: +44 1223 353 329**

Contact point at external third party (e.g. Privacy/Data Protection Officer – use functional mailboxes, not personal ones, as far as possible):

**Rani Viknaraja, Data Protection Office: [REDPO@randeurope.org](mailto:REDPO@randeurope.org)**

The processor/contractor was selected by FRA following a public procurement procedure.

Sub-processors:

Centre for the Study of Democracy (CSD) (Bulgaria), a subcontractor of RAND Europe for the purposes of the contract.

Spark Legal (Belgium), a subcontractor of RAND Europe for the purposes of the contract.

Thomasine Francke Rydén, a subcontractor of RAND Europe for the purposes of the contract.

**3) Purpose of the processing (Article 31.1(b))**

*Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).*

The purpose of the processing of the personal data is to collect information and data for the purpose of a FRA's research project on analysing online hatred in selected EU Member States, through the collection, processing, and annotations of 900 online posts per country in four selected EM Member States (Bulgaria, Germany, Italy, and Sweden). This is in line with the FRA mandate and the EU Regulation on the protection of personal data (see legal basis under point 11), and is grounded in FRA Programming Document 2022-2024 Fiche B.1.1, which describes the project and sets the basis for FRA to work on the topic: [PD 2022\\_2024\\_EN.pdf \(europa.eu\)](#).

The results of the project will contribute to understanding the extent to which certain people are prevented from participating in online communication because they

experience harassment, hate speech or (incitement to) violence online. In addition to online data collection, qualitative research will be conducted (interviews and/or focus groups) to complement the findings. The project's results will support EU and national reflexions on this topic with evidence to assess the extent and nature of online harassment, hate and (incitement to) violence with a view to informing the on-going development of regulatory and non-regulatory responses to online content moderation. The data will be collected with the purpose to answer the main research questions for this research project: 1) Understanding how online hatred manifests itself, including different types of the phenomenon; 2) Understanding how online hatred interferes with fundamental rights of victims; 3) Understanding how moderation of online hatred interferes with freedom of expression; 4) Understanding methodological challenges associated with assessing fundamental rights risks in relation to online content moderation, specifically on the freedom of expression. Ultimately, findings of the research will be issued in a FRA publication.

This record concerns the processing of personal data **for the annotation and analysis of social media posts**. This data processing consists of the following activities:

- The research team will **collect posts from online platforms** that meet the criteria for inclusion on the basis of a taxonomy for online hatred to be in Activity 4 (Data collection) and processing in Activities 6 (Annotation of online content) and 8 (Analysis of online content). The online platforms include: [Twitter](#), [Telegram](#), [Facebook](#), [YouTube](#), and [Reddit](#). It is noted that these platforms act as separate controllers for the personal data they process. With respect to the processing of personal data by these platforms, data subjects are referred to the latest versions of their attached privacy policies.
- After data collection, **a total of 900 posts per country will be annotated** by the research team, by inserting:
  - o basic, non-personal, information about each post (language, platform where it was found, geospatial data), and
  - o whether the post concerns online hatred or not on the basis of a working definition for online hatred that has been agreed during the Inception meeting.

#### 4) Description of the categories of data subjects (Article 31.1(c))

*Whose personal data are being processed?*

FRA staff

Non-FRA staff

Online platform users (Twitter, Telegram, Facebook, YouTube, and Reddit) associated with up to 900 posts per country, in Germany, Bulgaria, Italy and Sweden.

5) Categories of personal data processed (Article 31.1(c))

*Please tick all that apply and give details where appropriate*

**Activity 4 (Data collection) and processing in Activities 6 (Annotation of online content) and 8 (Analysis of online content).**

Whilst personal data is not specifically targeted, there is a risk that personal information is embedded in the posts when analysing posts and comments from online platforms (particularly when annotating collected data and providing more thorough description and analyses of selected posts). Such data might be included in the post content, and/or metadata (such as username, time stamp, or geotag), which may reveal information about personal data.

These data may contain personal data, such as:

- (Account) name, country or city of residence or gender.
- Any personal information about the originator or target which may be revealed in the post itself.

This might also include special categories of personal data as well. More specifically, the latter might include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and information regarding an individual's sex life or sexual orientation.

It should be noted that identification or linkage of such data to specific persons is very unlikely, as it would require access through a combination of the handles and the account names with the text and through potentially finding the post online by googling the text.

6) Recipient(s) of the data (Article 31.1 (d))

*Recipients are all parties who have access to the personal data. Who will have access to the data **within** FRA? Who will have access to the data **outside** FRA? No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).*

Designated **FRA** staff members   
 FRA project manager and project team members

Recipients **outside** FRA: Project team at RAND Europe [including members of the subcontractors (and sub-processors), i.e. the Center for the Study of Democracy, Spark Legal, and Thomasine Francke Rydén.

(please provide a generic/functional mailbox)   
[onlinehatred@randeurope.org](mailto:onlinehatred@randeurope.org)

7) Transfers to third countries or international organisations (Article 31.1 (e))<sup>6</sup>  
*If the personal data are transferred outside the European Economic Area or to international organisations, this needs to be specifically mentioned, since it increases the risks of the processing operation.*

**Transfer outside of the EU or EEA**

Yes   
 No

**If yes, specify to which country:**

**United Kingdom** (The respective files will be hosted and processed at RAND Europe's office in Cambridge, United Kingdom. Such a transfer is compliant with Regulation (EU) No 2018/1725 (on the basis of the relevant [European Commission's adequacy decision](#))

Only raw data will be downloaded from [Brandwatch](#) and [Crowdtangle](#). Data subjects are referred to the latest versions of the specific privacy policies (hyperlinks provided).

**Transfer to international organisation(s)**

Yes   
 No

If yes specify to which organisation:

**Legal base for the data transfer**

<sup>6</sup> **Processor** in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards.

Transfer on the basis of the [European Commission's adequacy decision](#) (Article 47)

Transfer subject to appropriate safeguards (Article 48.2 and .3), specify:

a)  A legally binding and enforceable instrument between public authorities or bodies.

Standard data protection clauses, adopted by

b)  the Commission, or

c)  the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2) .

d)  Binding corporate rules,  Codes of conduct ,  Certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

Subject to the authorisation from the European Data Protection Supervisor:

Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.

Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Transfer based on an international agreement (Article 49), specify:

***Derogations for specific situations (Article 50.1 (a) –(g))***

N /A

Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply In the absence of an adequacy decision, or of appropriate safeguards, transfer of personal data to a third country or an international organisation is based on the following condition(s):

(a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards

(b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person

(d) The transfer is necessary for important reasons of public interest

(e) The transfer is necessary for the establishment, exercise or defense of legal claims

(f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

(g) The transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case

8) Retention time (Article 4(e))

*How long will the data be retained and what is the justification for the retention period? Please indicate the starting point and differentiate between categories of persons or data where needed (e.g. in selection procedures candidates who made it onto the reserve list vs. those who didn't). Are the data limited according to the adage "as long as necessary, as short as possible"?*

Posts and metadata from these activities, potentially containing personal data, will be deleted 2 years after contract expiry (meaning that they will be deleted in December 2025).

9) Technical and organisational security measures (Article 31.1(g))

***Please specify where/how the data are stored during and after the processing; please describe the security measures taken by FRA or by the contractor***

**How is the data stored?**

- |   |                                     |
|---|-------------------------------------|
| Document Management System (DMS)          | <input type="checkbox"/>            |
| FRA network shared drive                  | <input type="checkbox"/>            |
| Outlook Folder(s)                         | <input type="checkbox"/>            |
| CRM                                       | <input type="checkbox"/>            |
| Hardcopy file                             | <input type="checkbox"/>            |
| Cloud (give details, e.g. cloud provider) | <input type="checkbox"/>            |
| Servers of external provider              | <input checked="" type="checkbox"/> |

Other (please specify): Data will be held on a server located in RAND Europe's Cambridge, UK office.

10) Exercising the rights of the data subject (Article 14 (2))

*How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react?*

See further details in the Data Protection notice: [OCM-project@fra.europa.eu](mailto:OCM-project@fra.europa.eu)

**Data subject rights**

- Right of access
- Right to rectification:
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object
- Notification obligation regarding rectification or erasure of personal data or restriction of processing
- Right to have recourse
- Right to withdraw consent at any time:

Part 2 – Compliance check and risk screening (internal)

11) Lawfulness of the processing (Article 5(a)–(e))<sup>7</sup>: Processing necessary for:  
*Mention the legal basis which justifies the processing and assess that the purposes specified are purposes specified, explicit, legitimate.*

---

<sup>7</sup> Tick (at least) one and explain why the processing is necessary for it. Examples:

(a) a task attributed to your EUI by legislation, e.g. procedures under the staff regulations or tasks assigned by an Agency’s founding regulation. Please mention the specific legal basis (e.g. “Staff Regulations Article X, as implemented by EUI IR Article Y”, instead of just “Staff Regulations”)

(a2) not all processing operations required for the functioning of the EUIs are explicitly mandated by legislation; recital 17 explains that they are nonetheless covered here, e.g. internal staff directory, access control.

(b) a specific legal obligation to process personal data, e.g. obligation to publish declarations of interest in an EU agency’s founding regulation.

(c) this is rarely used by the EUIs.

(d) if persons have given free and informed consent, e.g. a photo booth on EU open day, optional publication of photos in internal directory;

(e) e.g. processing of health information by first responders after an accident when the person cannot consent.