EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

RECORD OF PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 REGULATION 2018/1725[1] NOTIFICATION TO THE DATA PROTECTION OFFICER

NAME OF PROCESSING OPERATION[2]: Analysing online hatred in selected EU Member States – Interviews & consultation of experts and stakeholders

Reference number: DPR-2021-141
Creation date of this record: 9/12/2021
Last update of this record:
Version: v0.1

Part 1 (Publicly available)

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: European Union Agency for Fundamental Rights (FRA)
Schwarzenbergplatz 11, A-1040 Vienna, Austria
Telephone: +43 1 580 30 – 0
Email: contact@fra.europa.eu
Organisational unit **responsible**[4] for the processing activity: Research and Data Unit
Contact details: just_digit_secure@fra.europa.eu
Data Protection Officer (DPO): dpo@fra.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))[5]	
The data is processed by the FRA itself	☒
The data is processed also by a third party (contractor)	☒
RAND Europe, data processor	

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

2 **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.

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

4 This is the unit that decides that the processing takes place and why.

5 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

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

Data Protection Office:
REDPO@randeurope.org

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

Sub-processor:

Centre for the Study of Democracy (CSD), 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 conducting interviews with experts and stakeholders. This is in line with the FRA Founding Regulation (EC) No 168/2007 and the project is included in FRA Programming Document 2022-2024 Fiche B.1.1, which describes the project: 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.

To obtain an understanding of the policy context and background on the way hatred is expressed in the countries covered, interviews and one workshop with experts and stakeholders involved in the subject area are needed. The software used of the interviews is Microsoft Teams (its privacy statement is available here: : Microsoft Privacy Statement – Microsoft privacy). For the purpose of approaching interviewees and experts, personal data need to be processed. Interview summaries will be anonymised. However, it may be possible that individuals are identifiable based on their job descriptions and affiliations in the summaries.

More specifically, the processor's and FRA's research team will collect and process contact details of participants in the interviews and Online Expert Workshop. The following data will be collected by searching online: name, employer's name, function title, telephone number, and email address. These personal data will be used to invite the respondents to these consultation activities and to communicate over the course of the project. For accuracy and note-taking purposes, and only with the interviewee's consent, interviews will be audio-recorded (or in case of a video-call, being video-recorded). The notes and the data related to the interviewee will be shared with FRA, but not the recordings, that will be kept by the processor's research team. Audio and video recordings will be deleted after conclusion of the study.

The interviews and online expert workshop are part of a wider research project, which includes the following activities:

Stage A: Inception. Ensure an approach to the project that is refined and agreed in consultation with FRA.

Stage B: Reading and Development

- **Activity 1: Desk research.** Mapping scale and scope of online hate speech, harassment and incitement to violence in four countries, as well as online content moderation provisions.
- **Activity 2: Interviews with stakeholders.** Supplement the desk review with additional understanding of how the institutional landscape, legal instruments and policy measures, as well as terms of service of online platforms, function in practice.
- **Activity 3: Defining the methodology for collecting online content and annotation.** Fine tune the methodology for collecting and annotating online content, including by reference to an expert workshop.

Stage C: Data Collection

- **Activity 4: Data collection from online posts.** Collect posts and comments containing some element of online hatred through a variety of methods, including public APIs, web scraping and other means.

Stage D: Analysis

- **Activity 5: Training of annotators.** Familiarise each analyst with the annotation process, including the potential psychological challenges associated with analysing hate speech, and to harmonise the process of annotating posts and comments.

- **Activity 6: Annotation of online content.** Sample posts and comments and annotate them using a pre-defined annotation scheme to contribute to the development of a categorisation and typology of online hatred.
- **Activity 7: Analysis of online content.** Analyse online content, focusing on patterns, using a mixed method approach including quantitative but also qualitative analysis.

Stage E: Reporting. Prepare and draft the project report.

This record covers the processing of personal data related to activity 2. Processing of personal data related to other activities will be covered through another record.

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

Whose personal data are being processed?

FRA staff ☐

Non-FRA staff (please specify e.g. Roma community, judges, etc.) ☒

Interviews and Online Expert Workshop:
- Experts (e.g. academics)
- Stakeholders |(e.g. representatives of civil rights organisations, government officials, platform representatives)

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

Please tick all that apply and give details where appropriate

(a) **General personal data (add or delete as appropriate – the data in the brackets are only examples)**

Personal details (name, surname) ☒

Contact details (email address, work phone number) ☒

Education & Training details ☐

Employment details (name and type of the employer/organisation, country and city of the employer/ organisation, position/function title) ☒

Financial details (e.g. financial identification form, bank account information) ☐

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other (please give details):

(b) **Special categories of personal data** (Article 10)
The personal data collected may reveal:

Racial or ethnic origin	☒
Political opinions	☒
Religious or philosophical beliefs	☒
Trade union membership	☒
Genetic, biometric or data concerning health	☐
Information regarding an individual's sex life or sexual orientation	☐
N/A	☐

(c) **Personal data relating to criminal convictions and offences** (Article 11)

Criminal record (or similar, e.g. declaration of good conduct)	☐
N/A	☐

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 FRA project team members (only details of interview and workshop participants (name, surname, name and type of employer, country and city of the employer, function title)	☒

Recipients **outside** FRA:

Stijn Hoorens (Belgium, project lead) RAND Europe
Ben Baruch (United Kingdom), RAND Europe
Sara d'Auria (Belgium), RAND Europe
Katrin Feyerabend (United Kingdom), RAND Europe
Giulia Lanfredi (United Kingdom), RAND Europe
Kristin Thue (United Kingdom), RAND Europe
Emma-Louise Blondes (Belgium), RAND Europe

(please provide a generic/functional mailbox) ☒

onlinehatred@randeurope.org

Research partners at the Centre for the Study of Democracy (Bulgaria) ☒
Milena Momchilova-Boyadzhieva (Bulgaria), Centre for the Study of Democracy
Maria Stoyanova (Bulgaria), Centre for the Study of Democracy
Atanas Rusev (Bulgaria), Centre for the Study of Democracy
Stefan Ralchev (Bulgaria) Centre for Study of Democracy

7) Transfers to third countries or international organisations (Article 31.1 (e))[6]

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 processor's headquarters are in the United Kingdom)

Moreover, in the context of the use of Microsoft Teams to conduct the interviews and the online workshop by the contractor – the data processor –RAND Europe O365 data is located in the United Kingdom. See this link regarding geo-location Commercial Licensing Terms (microsoft.com). Nevertheless, Microsoft is a US-based company and therefore data subjects shall be informed that it remains subject to the US surveillance legislation. Microsoft compliance website is available here: General Data Protection Regulation - Microsoft GDPR | Microsoft Docs

Transfer to international organisation(s)

Yes ☐

No ☒

If yes specify to which organisation:

[6] **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.

Legal base for the data transfer

☒ 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"?

All personal information collected as part of Interviews and Online Expert Workshop for this research project will be deleted one year after contract expiry (December 2023).

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)	☒
FRA network shared drive	☒
Outlook Folder(s)	☒
CRM	☐
Hardcopy file	☐
Cloud (give details, e.g. cloud provider)	☐
Servers of external provider	☒

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

Interviews and Online Expert Workshop

Prior to participation to workshop or interview, we will share the data protection notice and information with participants. The document outlines the purposes of the project, which (personal) information will be collected and processed and for which purposes, as well as the rights that participants have with regard to access, rectification, erasure, etc. Prior to the workshop or interview, we will confirm that participants are familiar with this document and take their informed consent. The document will specify that participants

may contact REDPO@randeurope.org or just_digit_secure@fra.europa.eu to exercise any of the rights listed below.

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))[7]: Processing necessary for:

Mention the legal basis which justifies the processing and assess that the purposes specified are purposes specified, explicit, legitimate.

[7] 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.