DATA PROTECTION NOTICE

Analysing online hatred in selected EU Member States- Interviews & consultation of experts and stakeholders

The European Union Agency for Fundamental Rights (FRA or Agency) processes the personal data of a natural person in compliance with Regulation 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

This data protection notice explains FRA's policies and practices regarding its collection and use of your personal data, and sets forth your privacy rights. We recognise that information privacy is an ongoing responsibility, and we will update this notice where necessary.

1. Why do we collect personal data?

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.

The data controller is the EU Agency for Fundamental Rights (FRA), and the data processor is RAND Europe. The data processor was selected following a public procurement procedure. RAND Europe's subcontractor Centre for the Study of Democracy (Bulgaria) will act as sub-processor.

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 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.

These data are 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 for the interviews is Microsoft Teams** (its Privacy Notice 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.

Personal data will be processed to conduct interviews with experts and stakeholders.

The RAND and FRA research team will collect and process contact details of participants in the interviews (Activity 2) and Online Expert Workshop (Activity 3.1). These personal data will be used to invite the respondents to these consultation activities and to communicate over the course of the project.

2. What kind of personal data does the Agency collect?

We will collect only the following personal data necessary for the processing operation described above.

Interviews :

General personal data:

- Personal details: name, surname
- Contact details: email address, work phone number
- Employment details: name and type of employer, country and city of the employer/organisation, position/function title

Where interviews are video-recorded, special categories of personal data (like racial and ethnic origin) may be revealed.

3. How do we collect your personal data?

3a. Information you provide us

You may provide us with missing contact or employer information that is not publicly available online, through the consent form that will be provided to you before the interview, such as: name, employer's name, function title, telephone number, and email address.

For accuracy and note-taking purposes, and only with your consent, interviews will be audio-recorded, and may be video-recorded. The recordings will be kept by the research team and will not be shared with FRA. Audio- and video-recordings will be deleted after conclusion of the study.

Interview summaries, potentially containing identifiable information about experts, will be shared with the FRA project team.

3b. Information we receive from other sources

We will collect and process publicly available contact details of participants in the interviews and in the workshop by searching online: name, employer's name, function title, telephone number, and email address.

4. Who is responsible for processing your personal data?

The Agency is the legal entity responsible for the processing of your personal data and determines the objective of this processing activity. The Head of the Research and data Unit is responsible for this processing operation.

5. Which is the legal basis for this processing operation?

The processing operation is necessary to achieve the Agency's objectives, as stated in Article 2 of its founding Regulation (EC) No 168/2007 to provide its stakeholders, including Union institutions and EU Member States, with assistance and expertise relating to fundamental rights, including its tasks described in Article 4 (1)(a), (c) and (d). In particular, this activity falls under Article 2 and Articles 4(1)(a), 4(1)(c), and 4(1)(d) of the FRA founding Regulation (EC) No 168/2007 which tasks FRA with collecting, recording, analyzing and disseminating relevant, objective, reliable and comparable information and data. Therefore, the processing is lawful under Article 5(1)(a) of theRegulation (EU) No 2018/1725.

The processing of special categories of data (video revealing racial/ethnic origin) is lawful under Article 10(2)(a) of Regulation 2018/1725. Specific consent has been given and it is stored.

In addition, since participation in the survey is not mandatory and is based on the consent given by the respondents, the processing of the personal data is also in accordance with Article 5(1)(d) of Regulation (EU) No 2018/1725.

6. Who can see your data?

The details of interview and workshop participants (name, surname, name and type of employer, country and city of the employer, function title) will be available to the RAND Europe project team members (which include members of the subcontractor (and sub-processor) Center for the Study of Democracy) and to the FRA project manager and project team members.

The contact details (email address and work phone number) will only be available to project team members.

7. Do we share your data with other organisations?

Personal data is processed by the contractor (processor) only. In case that we need to share your data with third parties, you will be notified to whom your personal data has been shared with.

The details of interview and workshop participants (name, surname, name and type of employer, country and city of the employer, function title) will be shared with FRA project manager and project team members and with our research partners Centre for the Study of Democracy (Bulgaria) (see the CSD's Privacy Statement: https://csd.bg/footer-menu/privacy/), who are subcontracted by RAND Europe to assist in the research conducted in Bulgaria.

8. Do we intend to transfer your personal data to Third Countries/International Organizations

Yes. The details of interview and workshop participants will be 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).

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

9. When we will start the processing operation?

We will start the processing operation in February 2022.

10. How long do we keep your data?

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).

11. How can you control your data?

Under Regulation 2018/1725, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information. You are not required to pay any charges for exercising your rights except in cases were the requests are manifestly unfounded or excessive, in particular because of their repetitive character.

We will reply to your request 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, taking into account the complexity and number of the requests.

You can exercise your rights described below by sending an email request to OCM-project@fra.europa.eu .

11.1. The value of your consent

Since your participation is not mandatory, we need proof that you consented to the processing of your personal data. Consent will be collected by email prior to your participation in the interview or workshop. You have the right to withdraw your consent at any time, and we will delete your data or restrict its processing. All processing operations up until the withdrawal of consent will still be lawful.

11.2. Your data protection rights

a. Can you access your data?

You have the right to receive information on whether we process your personal data or not, the purposes of the processing, the categories of personal data concerned, any recipients to whom the personal data have been disclosed and their storage period. Furthermore, you can have access to such data, as well as obtain copies of your data undergoing processing.

b. Can you modify your data?

You have the right to ask us to rectify your data you think is inaccurate or incomplete at any time.

c. Can you restrict us from processing your data?

You have the right to restrict the processing of your personal data. If you do, we can no longer process them, but we can still store them. In some exceptional cases, we will still be able to use them (e.g. with your consent or for legal claims). You have this right in a few different situations: when you contest the accuracy of your personal data, when the Agency no longer needs the data for completing its tasks, when the processing activity is unlawful, and finally, when you have exercised your right to object.

d. Can you delete your data?

You have the right to ask us to delete your data when the personal data are no longer necessary for the purposes for which they were collected, when you have withdrawn your consent or when the processing activity is unlawful. In certain occasions we will have to erase your data in order to comply with a legal obligation to which we are subject.

We will notify to each recipient to whom your personal data have been disclosed of any rectification or erasure of personal data or restriction of processing carried out in accordance with the above rights unless this proves impossible or involves disproportionate effort from our side.

e. Are you entitled to data portability?

Data portability is a right guaranteed under Regulation 1725/2018 and consists in the right to have your personal data transmitted to you or directly to another controller of your choice.
In this case, this does not apply for two reasons: I) in order for this right to be guaranteed, the processing should be based on automated means, however we do not base our processing on any automated means; II) this processing operation is carried out in the public interest, which is an exception to the right to data portability in the Regulation.

f. Do you have the right to object?

When the legal base of the processing is "*necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body*" which is the case in most of our processing operations, you have the right to object to the processing. In case you object, we have to stop the processing of your personal data, unless we demonstrate a compelling reason that can override your objection.

g. Do we do automated decision making, including profiling?

Your personal data will not be used for an automated decision-making including profiling.

12. What security measures are taken to safeguard your personal data?

The Agency has several security controls in place to protect your personal data from unauthorised access, use or disclosure. We keep your data stored on our internal servers with limited access to a specified audience only.

More concretely, organisational measures include:
- ICT and Data Management Policy
- Internal rules on data protection and retention
- Annual mandatory training and certification for all staff on information security
- Risk assessment of the processing operations

Technical measures include:
- Cybersecurity
- Physical security
- Report mechanism for security issues
- Control of access to electronically held information
- Password policy
- Encryption or pseudonymisation
- Data breach policy

The data processor also implements appropriate technical and organisational measures.

In particular, the data processor's security measures embrace some of the following organisational and technical measures.
- Data Protection Policy
- Overarching Privacy Notice and various bespoke project related Privacy Notices
- Guidance on Withdrawal of Consent and Withdrawal Log

Some further measures implemented at the particular stages of the project by the data processor are the following:

Qualitative data collection (Interviews and workshops)

Interview and workshop participants would be provided with Information Sheets and Data Protection Notices explaining the purpose of the research, the data being collected, how this will be used, the extent to which their data will be shared with other parties, along with information on their rights and how to exercise these. Both the Information Sheets and Data Protection Notices too would be reviewed and confirmed by the Data Controller prior to the commencement of these activities.

To prevent the collection of any special category of personal data: we will not include any questions to that effect in the questionnaire; we will develop protocols that discourage the naming of individuals in the

provision of examples; we will provide guidance to the interviewers to help ensure that these data are not recorded, should such information be revealed inadvertently. Video-recordings may reveal special categories of personal data.

Secure data storage and processing

The processor has in place a range of measures to ensure appropriate data storage. Its information security management system is certified to ISO 27001:2015, and it also holds a Cyber Essentials Plus certification.

Data will be stored on a RAND Europe's network folder. Access will be restricted to the designated project team, and further subfolders restricted to specific team members where tighter controls are appropriate and material does not need to be made available to the entire team.

All RAND Europe laptops have full disk encryption, and require two-factor authentication at login. So whilst controlled material should not be stored on these devices, the processor nonetheless has in place mitigating measures should data be inadvertently placed upon them.

Secure transfer of data within the team and with FRA

Finally, with regard to the project requirement for appropriate measures for effective communication and exchange of information within the project team and with respect to individual team members and FRA, RAND Europe uses Egress Workspace for secure file transfer and collaboration. Egress Workspace is UK hosted, employs AES 256-bit encryption for data at rest and TLS encryption. Data is stored in ISO 27001 and SOC 2 audited data centres in accordance with GDPR and the EUDPR.

Data protection at study conclusion

Where it is necessary to transfer electronic records back to the Data Controller at study conclusion, RAND Europe will use its secure file transfer platform that utilises AES-256 encryption and a TLS tunnel for transfers. For additional protection the processor will compress and encrypt the files prior to the return of data at the end of the study or the transfer of any data to the Data Controller.

Data that should be destroyed on premise, or otherwise, will follow the procedures specified and agreed with FRA.

Additionally, the processor would consider any other mechanisms that the controller may feel as appropriate to the data in question and would of course act under its instruction on such matters.

13. What can you do in the event of a problem?

a) The first step is to notify the Agency by sending an email to OCM-project@fra.europa.eu and ask us to take action.

b) The second step, if you obtain no reply from us or if you are not satisfied with it, contact our Data Protection Officer (DPO) at dpo@fra.europa.eu.

c) At any time you can lodge a complaint with the EDPS at http://www.edps.europa.eu, who will examine your request and adopt the necessary measures.

14. How do we update our data protection notice?

We keep our data protection notice under regular review to make sure it is up to date and accurate.

END OF DOCUMENT