DATA PROTECTION NOTICE

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

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?
2. What kind of personal data is collected and further processed?
3. How do we collect your personal data?
4. Who is responsible for processing your personal data?
5. Which is the legal basis for this processing operation?
6. Who can see your data
7. Do we share your data with other organisations?
8. Do we intend to transfer your personal data to Third Countries/International Organizations
9. When will we start the processing operation?
10. How long do we keep your data?
11. How can you control your data?
    - 11.1. The value of your consent
    - 11.2. Your data protection rights
12. What security measure are taken to safeguard your personal data?
13. What can you do in the event of a problem?
14. How do we update our data protection notice?

1. Why do we collect personal data?

The purpose of the processing of the personal data is to collect information and data for 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).
The data controller is the EU Agency for Fundamental Rights (FRA), and the data processor is RAND Europe (Rue de la Loi 82 / Bte 3, 1040 Brussels, Belgium). The data processor was selected following a public procurement procedure (eTendering - Data (europa.eu)). RAND Europe's subcontractors Centre for the Study of Democracy (Bulgaria), Spark Legal (Belgium) and Thomasine Francke Rydén will act as sub-processors. Spark Legal is subcontracted by RAND Europe to assist with the annotation of social media posts in Italy, Sweden, Germany and Bulgaria. CSD is subcontracted by RAND Europe to assist with the annotation of social media posts in Bulgaria (see the CSD's Privacy Statement: https://csd.bg/footer-menu/privacy/, as well as Spark Legal's Privacy Statement: https://www.sparklegalnetwork.eu/privacy-policy). Thomasine Francke Rydén is subcontracted by RAND Europe to assist with the annotation of social media posts in Sweden.

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.

For the purpose to analyse existing online hatred on social media in line with the objectives above, such information needs to be collected directly from online resources. The results will provide aggregated statistical and anonymous information about online hatred published in a report that will be used to provide advice to policy makers addressing online hatred.

Personal data will be processed for the collection, and to a limited extent, annotation and analysis of social media posts.

2. What kind of personal data is collected and further processed?

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 information 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. Furthermore, any personal information about the originator or target may also be revealed in the post itself, including 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.

3. How do we collect your personal data?

Information we receive from other sources:

Data collection and processing in annotation of online content, and analysis of online content.

The research team will collect posts from online platforms that meet the criteria for inclusion on the basis of a taxonomy for online hatred. The posts will be collected from the online platforms by scraping public content:

- By using the API made available by the platforms (Telegram) or
- by using third party providers Brandwatch (Facebook, YouTube, Twitter, Reddit, and Tumblr) and/or Crowdtangle (Facebook). Please see below the links to the privacy policies of these companies:
    - Twitter: https://twitter.com/en/privacy
    - Telegram: https://telegram.org/privacy
    - Facebook: https://www.facebook.com/about/privacy/previous
    - YouTube: https://policies.google.com/privacy?hl=en-GB
    - Reddit: https://www.redditinc.com/policies/privacy-policy

It is noted that these platforms act as separate controllers for the personal data they process. To learn more on how these platforms process your data, we encourage you to read the latest versions of their privacy policies.

- After data collection, a total of 900 posts per country will be annotated by the research team, by inserting:
- basic, non-personal, information about each post (language, platform where it was found, geospatial data), and
- 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. 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 (as amended by Regulation (EU) 2022/555) to provide its stakeholders, including Union institutions and EU Member States, with assistance and expertise relating to fundamental rights. More specifically, this activity falls under Article 4(1)(a), 4(1)(c), and 4(1)(d) of the FRA amended founding Regulation, 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 the Regulation (EU) No 2018/1725.

The processing of special categories of personal data is lawful under Article 10(2)(j) of the same Regulation, as it is necessary for scientific research purposes or statistical purposes based on Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6. Who can see your data?

The personal data in social media or online meta data or posts will only be available to the project team at RAND Europe (which include members of the subcontractors (and sub-processors) Center for the Study of Democracy, Spark Legal, and Thomasine Francke Rydén) and to the FRA project manager and project team members.

7. Do we share your data with other organisations?

Personal data is processed by the Agency 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.

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

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. You can read the latest versions of their specific privacy policies (links provided under Section 3 above).

9. When will we start the processing operation?

We will start the processing operation in May 2022.

10. How long do we keep your data?

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).

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 this processing operation is in accordance with the applicable legal framework under Article 5.1.(a) and 10(2)(j) of the Regulation (EU) No 2018/1725 (please refer to Section 5 above), your consent is not required.

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.

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:

Data collection from online platforms
Only the data scientists involved in the data collection phase will have access to the third party data aggregation platforms (Brandwatch, Telegram API, and/or Crowdtangle). Data files will be downloaded on RAND Europe's network folder in the UK to which only selected team members have access. The selected 900 posts per country for annotation will be shared with sub-contractors CSD (Bulgaria) and Thomasine Francke Rydén, as well as Spark Legal (second annotation of 300 posts per country) via Egress Workspace (see below).

RAND Europe will be using pseudonymisation where possible and separating personal identifiers (which in this context, will mainly constitute usernames and handles associated with posts and comments) from other data (i.e. the posts and comments themselves along with any metadata that may be useful for analysis) at the earliest point possible.

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. Further measures have been taken to restrict access only to the designated project team.

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.

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.

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