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]: Third FRA survey on discrimination and hate crime against Jews in the EU – online data collection and website**

| Reference number: DPR-2020-171 (to be completed by the DPO) |
|---|
| Creation date of this record: 12.10.2022 |
| Last update of this record: 20.10.2022 |
| Version:1.0 |

## Part 1 (Publicly available)

| 1) Controller(s)[3] of data processing operation (Article 31.1(a)) |
|---|
| Controller: European Union Agency for Fundamental Rights (FRA)<br>Schwarzenbergplatz 11, A-1040 Vienna, Austria<br>Telephone: +43 1 580 30 – 0<br>Email: contact@fra.europa.eu<br>Organisational unit **responsible**[4] for the processing activity: Justice, Digital and Migration Unit<br>Contact details: *antisemitism-survey@fra.europa.eu*<br>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), Kantar Public, Belgium | ☒ |
| Kantar Public is acting as 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?

Contact point at external third party GDPR@kantar.com

## 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).*

For FRA to provide its stakeholders evidence-based advice on the experiences of Jewish population with antisemitism, hate-crime and discrimination as well as their perceptions on Jewish life in the EU, the agency needs to collect data concerning the experiences and opinions of persons self-identifying as Jews. Data collected through an online survey allows the agency to analyse the current situation and trends of experiences and life of Jews living in the following 13 member states: Austria, Belgium, Czechia, Denmark, France, Germany, Italy, Hungary, The Netherlands, Poland, Romania, Spain, Sweden.

The data gathered through the online survey consist of survey respondents' answers to the survey "Third survey on discrimination and hate crime against Jews in the EU", which is voluntary. The survey will collect respondents` answers regarding personal experiences and opinions concerning antisemitism, hate-crime, discrimination, living an open Jewish life, rights awareness, religious beliefs, health limitations and socio-demographic characteristics.

The invitation to the survey is coordinated via decentralised awareness raising activities. Community leaders, organisations, stakeholders and other multipliers are asked to share the link to the open online survey website with their members and contacts. There is no possibility of linking personal information identifying respondents (such as name, address, contact information, etc.) with the answers provided in the survey.

The website of the survey will be informing potential respondents and potential multipliers about the survey content and the start date prior to the launch of the survey. Interested potential respondents and organisations can request via email (eujews@kantar.com) a reminder invitation once the survey goes live. To this end, they send an email to the contractor specifying their request. Kantar Public processes their personal data (name (if given) and email address – voluntarily provided by the potential respondent) and uses

the provided email addresses to send out mass email invitation to an undisclosed list of recipients to invite signed up respondents to participate via open link once the survey is live. There is no possibility of linking personal information (name or email address) with the answers provided in the survey due to the open link provided. After the end of the field phase, the contractor will delete the personal data (name, email address etc.) provided. The email addresses will not be used for any other purpose.

## 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.) ☒
Respondents to the survey who self-identify as Jews (aged 16+)

## 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

Via email pre-registration - *only if provided by potential respondents via sending an email to the contractor before the survey indicating that they would like to receive an invitation once the survey starts*- : email address and *(if provided*) name, surname
Via the survey:
gender, age (no name/surname/contact details), country of birth ☒

Contact details

Via the website - *only if provided by potential respondents via sending an email to the contractor before the survey indicating that they would like to receive an invitation once the survey starts*- : email address
Via the survey: None ☒

Education & Training details :

Via the survey: highest educational attainment level ☒

Employment details ☐

Financial details ☐

Family, lifestyle and social circumstances ☒

Goods or services provided ☐

Other (please give details): perception of societal problems including antisemitism, experience of antisemitism, bias-motivated harassment, violence and vandalism,

discrimination, importance of religious practices, rights awareness, trust in and attachment to institutions, as well as the encrypted IP addresses, and cookies:
Respondents can only complete the survey online, and for the quality control and validation of the data, the survey will collect cookies and the encrypted IP address (in order to allow respondents to take a break from completing the survey and to continue another time where they left off). These cookies can be turned off by the respondents and are transmitted voluntarily. For the management and assessment of the data collection, the survey will also collect anonymous metadata and paradata such as information concerning the type of device (PC, smartphone, tablet, etc.) used to complete the online survey.

(b) **Special categories of personal data** (Article 10)
The personal data collected reveal:
Through their responses, respondents might reveal special categories of personal data:

| | |
|---|---|
| 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
Justice, Digital and Migration Unit, Institutional Cooperation & Networks Unit,
Equality, Roma & Social Rights Unit ☒
*A restricted number of staff members (limited to the project members and specific persons assigned to the topic) will have access to the anonymised survey dataset*

Recipients **outside** FRA:
eujews@kantar.com ☒
*Kantar Public's research staff will have access to the contact details provided by potential respondents via email until the end of the field work (approx. March 2023) and will use the email addresses to inform about the launch of the survey.*
*Survey data on experiences and opinions (content of the survey) provided by respondents will be accessible by Kantar Public's research staff until the end of the contract + 12 months.*

## 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**:

***Transfer to international organisation(s)***

Yes ☐

No ☒

If yes specify to which organisation:

***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

[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.

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"?*

The personal data provided via email for the invitation to the survey will be stored by Kantar Public in internal serves in a secure environment according to data protection guidelines and kept until the end of the field phase (approx. March 2023).

The personal data based on the respondents' answers to the survey questions will be stored on Kantar Public internal servers until the end of the contract (approx. August 2023). After this point, the collected data will be anonymised i.e. any metadata that could possibly identify an individual will be deleted. Kantar Public will retain the anonymised data for a maximum of 12 months from the date of delivery of the final contractual obligation (the final project report) after which they will be deleted by Kantar Public.

After receiving the final data set, the agency will double-check that the data set does not contain any personal data. Any personal data detected as a part of this process will be deleted by 31 August 2023. The anonymised dataset will be stored indefinitely for research purposes in data centers located within the EU.

## 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 (Microsoft Office 365. For further information, please refer to the relevant Data Protection Notice) | ☒ |
| Servers of external provider | ☒ |

Other (please specify):
*The data is collected via an online survey tool owned by Kantar Public and is located within the EU. The data is stored by the contractor Kantar in the EU and no transferred outside EU; the data transmission between the contractor and the FRA takes places via a secure network ("kiteworks")*

## 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: e-mail to PublicCompliance@kantar.com or *antisemitism-survey@fra.europa.eu*

***Data subject rights***

☒ Right of access

☒ Right to rectification

☒ Right to erasure (right to be forgotten)

☒ Right to restriction of processing

N/A 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 5.1 (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.