

**RECORD OF PROCESSING ACTIVITY
ACCORDING TO ARTICLE 31 REGULATION 2018/1725¹
NOTIFICATION TO THE DATA PROTECTION OFFICER**

NAME OF PROCESSING OPERATION²: Collection of information among Jewish Communities on the situation after October 7th, 2023

Reference number: DPR-2024-206
Creation date of this record: 18.01.2024
Last update of this record:
Version:1.0

Part 1 (Publicly available).

1) Controller(s)³ of data processing operation (Article 31.1(a))
<p>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 responsible⁴ for the processing activity: Justice, Digital and Migration Unit Contact details: antisemitism-survey@fra.europa.eu Data Protection Officer (DPO): dpo@fra.europa.eu</p>

2) Who is actually conducting the processing? (Article 31.1(a))⁵
<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) <input checked="" type="checkbox"/></p> <p>The following third parties might be involved in the processing operation as processors:</p>

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?

FRA's webhosting contractor, Managing Innovation Strategies, SLL (Mainstrat) in consortium with SARENET, S.A.U

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).

FRA collected data concerning the experiences and opinions of persons self-identifying as Jews from January until June 2023 through an online survey in 13 Member States, the results of which will be presented in a report. However, the reality for many Jews in the EU changed drastically after the Hamas terrorist attack on Israel on October 7th, 2023. A reality which cannot be described with the current survey data.

In order to contextualise the findings, FRA will undertake a small data collection via LimeSurvey addressed to representatives of the largest Jewish community organisations in the Member States covered by the survey (Austria, Belgium, Czechia, Germany, Denmark, Spain, France, Hungary, Italy, the Netherlands, Poland, Romania, Sweden). The invitations to the small survey will be sent via the project manager's FRA email account to the relevant Jewish organisations. The respondents to the survey, who are not necessarily the contacts that received the invitation, will be invited to indicate the name of the organisation they are representing in order to avoid double entries.

The respondents are asked to report on the situation of the Jewish community they represent after October 7th, 2023. Descriptions of the situation for Jews in these Member States, based on the input of the respondents, will be compiled in dedicated sections of the report in an anonymised format. Anonymised quotes might be used.

The data will be processed as follows:

- The data will be collected by means of an online questionnaire which will be programmed in Lime Survey software.
- The data will be stored in the SQL database on FRA servers (located in Spain) wherefrom they will be exported into a data set.
- The data set will be securely kept (protected by password).
- The data set will be analysed by FRA staff in such a manner that the responses cannot be identified and linked to an individual person.

- The results of the analysis and anonymized quotes will become publicly available, it will not be possible to link respondents' responses to an individual person or organisation.

Apart from the personal data indicated in Section 5 below, we do not intend to collect the personal data of the respondents (not necessarily the recipients that received the invitation to the survey, since they can respond themselves, or forward the invitation to another representative or relevant person within the organisation). However, they will be asked to indicate the name of the organisation they are representing in order to avoid double entries, but they will not be asked to provide any personal information (name, email address, age, personal views and experiences etc.). Respondents are asked to report on the experiences of the community they represent by answering open-ended questions. In the unlikely event, that they share specific or general personal data, this will be deleted from the dataset before analysis.

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 in the invitation. The name of the organisation will not be made public in the report and will be deleted after the publication of the report.

In order to carry out the surveys, FRA uses the online tool LimeSurvey which, for functional purposes, collects and process some necessary personal data such as session cookies as indicated below.

The contact details of the representatives of the Jewish community organisations have been obtained by FRA from previous professional relations with FRA in the past or through desk research of publicly accessible websites.

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

Whose personal data are being processed?

FRA staff

Non-FRA staff

Representatives of the largest Jewish organisations in the Member States covered by the survey.

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

Please tick all that apply and give details where appropriate

The survey questionnaire is not asking any personal information about the respondent. In the unlikely event that respondents share any general or specific personal data with FRA, this data will be deleted.

(a) General personal data

Personal details (recipients' names and surnames obtained by FRA from previous professional relations with FRA in the past or via publicly available websites, not linked to the survey data).

Contact details (recipients' email address obtained by FRA from previous professional relations with FRA in the past or via publicly available websites, not linked to the survey data).

Education & Training details :

Employment details

Financial details

Family, lifestyle and social circumstances

Goods or services provided

Other (please give details):

Two type of session cookies are used:

1. PHPSESSID

Domain: fra.europa.eu

This cookie is native to PHP applications. The cookie is used to store and identify a users" unique session ID for the purpose of managing user session on the website. The cookie is a session cookie and is deleted when all the browser windows are closed.

2. YII_CSRF_TOKEN

Domain: fra.europa.eu

This cookie is created to prevent Cross-Site Request Forgery (CSRF). The cookie is a session cookie and is deleted when all the browser windows are closed.

(b) Special categories of personal data (Article 10)

Since the survey is focussed on the reporting of representatives on their communities, we are not asking about any personal experiences or opinions. However, since we are using open-ended questions, the respondents may reveal data on their personal racial or ethnic origin, political opinions, religious beliefs or data concerning their health or sexual orientation. In this very unlikely case, this data will be removed and not analysed.

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	<input type="checkbox"/>
N/A	<input type="checkbox"/>
(c) Personal data relating to criminal convictions and offences (Article 11)	
Criminal record (or similar, e.g. declaration of good conduct)	<input type="checkbox"/>
N/A	<input checked="" type="checkbox"/>

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 from the Justice, Digital and Migration Unit, Institutional Cooperation & Networks Unit, Equality, Roma & Social Rights Unit will have access to the survey responses.

The survey data will be processed and can be accessed by designated FRA staff working on the project. Access is restricted to authorized staff members and only these members have access rights. The contact details will only be accessible for the Project manager.

Recipients **outside** FRA:

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

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.

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

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"?

Data collected will be anonymised, and any metadata that could possibly identify an individual will be deleted.

The anonymised dataset will be stored indefinitely by FRA.

The contact details of the recipients of the survey invitations (who are not necessarily the respondents) will be stored separately until the end of the project (end of 2024). It will not be possible to link the contact detail of the recipients of the survey invitations and the survey data.

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

FRA undertakes to ensure security updates to the software and hosting environment take place in a timely manner.

The web hosting consortium has security policies in place to ensure the physical and logical security for the infrastructure it operates. The consortium has also performed a security self-assessment to demonstrate the compliance of its Data Centre with the security requirements outlined by the ISO 27001 standard.

Added to this, the following sub-sections show the specific security measures at three levels:

- 1. FRA Platform environment, by means of 2 Fortinet firewalls.*
- 2. FRA Applications, by means of Frontal Pro Web Application Firewall.*
- 3. Physical security in the Data Center.*

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 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

Please note that the data is collected anonymously. Without revealing of the respondents, the Agency will not be able to identify a particular person in the dataset. Hence, the Agency will not be in the position to modify and/or delete any data stored, without further information of the respondent because the data will be anonymised.