

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

NAME OF PROCESSING OPERATION²: FRA online meeting with human rights cities, 16 September 2020.

Reference: DPR-2020-109
Creation date of this record: 24/08/2020
Last update of this record: 28/08/2020
Version: 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) Organisational unit responsible⁴ for the processing activity: Institutional Cooperation and Networks unit Contact: human_rights_systems@fra.europa.eu Data Protection Officer (DPO): Robert-Jan Uhl dpo@fra.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))⁵
The data is processed by FRA itself <input checked="" type="checkbox"/>
The data is processed also by a third party <input checked="" type="checkbox"/>
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 FRA itself conducting the processing? Or has a provider been contracted?

Lime Survey (collecting registration) - privacy policy:

<https://www.limesurvey.org/en/privacy-policy>.

Webex tool (online meeting): <https://www.cisco.com/c/en/us/about/trust-center/gdpr.html>

Joint Controller: N/A

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 personal data is for the organisation of an online meetings with human rights cities and other cities interested in becoming a human rights city. The processing allows us to:

- Send invitations to participants to the online meeting;
- Collect issues for interest to develop the agenda and address possible follow up emerging from the meeting;
- Join the online emeeting using the webex tool used by FRA.

The overall purpose of the meeting is to brief participants on the state of development of the framework of human rights cities and discuss the opportunity for more cities to join this cooperation. Discussion will follow the Chatham House Rules.

The meeting will be organised using the [Cisco Webex online](#) tool, through a license acquired by FRA. Participants will enter their name and email into the webex system. Only the names will be available to other participants. Participants will be asked to indicate in the registration process if they agree to share their email contact to others or not. The types of personal data collected by Cisco Webex are described in FRA's Webex privacy notice, available at:

https://fra.europa.eu/sites/default/files/fra_uploads/privacy_notice_cisco_webexdpr-2020-101.pdf and Cisco's webex GDPR rules are at: [Cisco Webex Meetings service](#)

Registration will be done through an online form using the LIME Survey tool (privacy policy: <https://www.limesurvey.org/en/privacy-policy>).

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

Whose personal data are being processed?

FRA staff

Non-FRA staff

Municipalities staff mostly and some specific human rights cities experts.

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

Please tick all that apply and give details where appropriate. Include information if automated decision making takes place, evaluation and monitoring

(a) General personal data:

The personal data contains:

- | | |
|--|-------------------------------------|
| Personal details:
-Name, surname, title, function. | <input checked="" type="checkbox"/> |
| Contact details
-Email, organisation, address, telephone, city. | <input checked="" type="checkbox"/> |
| Education & Training details: | <input type="checkbox"/> |
| Employment details (e.g. work experience, languages, opinions) | <input type="checkbox"/> |
| Financial details (e.g. financial identification form, bank account information) | <input type="checkbox"/> |
| Family, lifestyle and social circumstances: | <input type="checkbox"/> |
| Goods or services provided | <input type="checkbox"/> |
| Other (please give details): | <input type="checkbox"/> |

(b) Sensitive personal data (Article 10)

The personal data reveals:

- | | |
|--|--------------------------|
| Racial or ethnic origin | <input type="checkbox"/> |
| Political opinions | <input type="checkbox"/> |
| Religious or philosophical beliefs | <input type="checkbox"/> |
| Trade union membership | <input type="checkbox"/> |
| Genetic, biometric or data concerning health | <input type="checkbox"/> |
| Information regarding an individual's sex life or sexual orientation | <input type="checkbox"/> |

6) Recipient(s) of the data (Article 31.1 (d))⁶

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?

⁶ 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

Relevant staff members working in the Institutional Cooperation and Networks Unit,
and Technical Assistance and Capacity Building Unit

Other staff members from the project team responsible for the activity (D_1_2) could be involved also as back up or for follow-up activities.

Designated persons **outside** the FRA: (please specify)

7) Transfers to third countries or recipients outside the EEA (Article 31.1 (e))⁷

If the personal data are transferred outside the European Economic Area, 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

c) the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2) .

⁷ **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.

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"?

Personal data will be retained for a maximum of one year after the closing of the event, that is **16 September 2021**.

This would allow sufficient time to perform any follow up activities emerging from the event.

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?

- | | |
|--|-------------------------------------|
| FRA network shared drive | <input checked="" type="checkbox"/> |
| Outlook Folder(s) | <input checked="" type="checkbox"/> |
| CRM | <input type="checkbox"/> |
| Hardcopy file | <input type="checkbox"/> |
| Cloud (give details, e.g. cloud provider) | <input type="checkbox"/> |
| Servers of external provider
- LIME online form
- Webex tool | <input checked="" type="checkbox"/> |

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 privacy notice: e-mail to human_rights_systems@fra.europa.eu

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