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]:
Video questions submitted by participants to the Human Rights Communicators Network Meeting 28-29 June 2021

Reference number: DPR-2021-134
Creation date of this record: 14-06-2021
Last update of this record: 14-06-2021
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) Schwarzenbergplatz 11, A-1040 Vienna, Austria Telephone: +43 1 580 30 – 0 Email: contact@fra.europa.eu Organisational unit **responsible[4]** for the processing activity: *Communications and Events Unit* Contact details: *event@fra.europa.eu* 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	☒

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?

The data is processed also by a third party (contractor)

FRA contractor (processor): **Tipik**

Avenue de Terveuren 270, B-1150 Brussels, Belgium

info@tipik.eu ☒

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 the personal data (a video question recorded and submitted by a member of the Human Rights Communicator Network) is to be able to ask a specific question or raise a specific challenge faced on the topic of communicating on human rights in times of disinformation during the virtual Human Rights Communicators Network Meeting that will take place on 28-29 June 2021 and related follow up communication activities. FRA will receive the video and display an edited version during the virtual meeting.The video will be further used for communication activities related to this topic.

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

Whose personal data are being processed?

FRA staff ☐

Non-FRA staff: ☒

Participants to the virtual Human Rights Communicators Network Meeting that will take place on 28-29 June 2021, having submitted a video question.

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 (e.g. name, surname, photo) ☒

Contact details (email address) ☒

Employment details (name of position and name of organization) ☒

Other (please give details):
Personal video of the communicator: self-image and voice ☒

(b) **Special categories of personal data** (Article 10)
The personal data collected reveal:

Racial or ethnic origin (self-image - video) ☒

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 ☒

During the review process, a restricted number of staff members, who are in Communications and Events Unit, can access your personal data. These include FRA staff members working in the Unit for the event "Human Rights Communicators Network Meeting" and the Head of Unit.

Recipients outside FRA:
Staff of FRA's contractor Tipik info@tipik.eu

Selected staff of Tipik have access to the data through the development of the event website and registration platform.

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 ☒

*The meeting where the videos will be displayed will be hosted via Webex-Cisco. We are aware that this is a U.S.-based company and thus after the Schrems II ruling we need to have additional safeguards in place even when data is stored only in EU-based servers. These measures are needed to address the risk of a transfer of data from Webex-Cisco to U.S. authorities under a federal law order (as foreseen by U.S. federal law). To address this very rare possibility, we made sure that Webex-Cisco enables end-to-end encryption: this kind of encryption ensures that personal data in clear cannot be accessed neither by Webex-Cisco itself.

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

[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.

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 video will be retained for a maximum of 6 months after having been received. Since the video question will be used for a "live panel debate" or for a workshop, as per given consent of the data subject, a few seconds might appear as part of a 3 min video summary clip of 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?

Document Management System (DMS)	☐
FRA network shared drive	☒
Outlook Folder(s)	☐
CRM	☐
Hardcopy file	☐
Cloud (cloud provider M365)	☒
Servers of external provider FRA contractor (processor): Tipik Avenue de Terveuren 270, B-1150 Brussels, Belgium info@tipik.eu	☒

For the video question to be played during the online event, the server of the external contractor providing the technical infrastructure of the event will have the video stored. The video data is stored in the EU and not transferred outside EU.

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 event@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