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]: Research Project on "The impact of the Terrorism Directive on fundamental rights"

Reference: DPR-2020-097
Creation date of this record: 08-04-2020
Last update of this record: 16-06-2020
Version:2

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: information@fra.europa.eu Organisational unit **responsible**[4] for the processing activity: Research & Data Contact: just_digit_secure@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 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 ☒ Skype for Business Online (Joint Controller with FRA for the data processed throughout interviews conducted via Skype) Contact form: https://privacy.microsoft.com/en-GB/privacy-questions Cisco Webex (Joint Controller with FRA for the data processed throughout interviews conducted via Webex) email: privacy@cisco.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).

The purpose of the processing of the personal data is to collect information and data for the purpose of a research project. The European Commission requested an evidence based advice in the context of their report on the added value of Directive 2017/541 with regard to combating terrorism (Article 29 of Directive (EU) 2017/541). The project will collect data and map the implications of the application of individual provisions of the Directive 2017/541 at the Member State level on fundamental rights and freedoms. The project consists of a desk research in the 25 EU Member States covered by the Directive and interviews with individual experts carried out in selected Member States. The information from the interviews will feed into the preparation of a report to be published in 2021.

In order to carry out interviews with experts, their contact details and background information about their work and professional status needs to be collected. The Agency might perform face to face or video call interviews. If the latter applies, some extra categories of personal data of the interviewee may be processed by the Agency and the online video platform. You can find more details on this below.

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

Whose personal data are being processed?

FRA staff	☐
Non-FRA staff (interviewed experts in the field of counter-terrorism)	☒

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 collected include:

Personal details (*name, surname)* ☒

Contact details (*email address, mobile number*) ☒

Education & Training details ☐

Employment details (*work experience, name and type of the employer/organisation, address of the employer/ organisation*) ☒

Financial details (*e.g. financial identification form, bank account information*) ☐

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other (please give details): ☒
In the event of Skype interviews the following personal data will be collected

- User information: first name, last name, caller ID, telephone (optional), email address, profile picture (optional).
- Meeting metadata: topic, appointment data, participant IP addresses, device/ hardware information.
- Text, audio and video data: Users have the option of using the chat, question or survey functions in an online meeting. In this respect, the text entries they have made are processed in order to display them in the online meeting and, if necessary, to log them. In order to enable the display of video and the playback of audio, the data from the microphone of the users' end device and any video camera of the end device are processed accordingly during the duration of the meeting.
- Desktop & Application Sharing allows users to collaborate over video chat while also sharing their desktop or selected application with everyone in the meeting. If sharing is initiated, depending on what is being shared, all conversation participants will be able to see the monitor(s), entire desktop, or selected application on their computer's screen.
- Users can manually set their location by entering a custom location into the location control in the Skype for Business user interface. The time zone is collected directly from the user's computer operating system. Depending on how the user or administrator has configured the privacy settings location and time zone information is shared by Skype for Business and made available to other users through the Contact Card

In the event of Cisco Webex interviews please see the respective privacy notice and record

(b) **Sensitive personal data** (Article 10)
The personal data reveals:

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	☐

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?*

Designated **FRA** staff members (please specify which team and Unit) ☒

During the research, a restricted number of staff members, which are part of the project team, can access your personal data. These include the project team members and the Head of Unit of Research & Data.

Designated persons **outside** FRA: ☒

Skype for Business Online or Cisco Webex with regards to the personal data processed during the online interviews

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	☐

[6] No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).

[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.

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) EU-US Privacy Shield

☐ 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"?

Personal data described above will be kept for 24 months after their collection. All physical and electronic copies held by FRA will then be deleted.

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	☒
Document Management System	☒
Outlook Folder(s)	☒
CRM	☐
Hardcopy file	☒
Cloud (give details, *e.g. cloud provider*)	☐
Servers of external provider	☒

Other (please specify):

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 just_digital_secure@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