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]: Event "Fundamental Rights Dialogue", hereinafter "the Event"; taking place on 13 November 2020 in a virtual setting.

Reference number: DPR-2020-112
Creation date of this record: 20/08/2020
Last update of this record: 19/10/2020
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) Schwarzenbergplatz 11, A-1040 Vienna, Austria Telephone: +43 1 580 30 – 0 Contact: https://fra.europa.eu/en/contact Organisational unit **responsible**[4] for the processing activity: Communications and Events Unit 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	☒
The data is processed also by a third parties (Processors)	☒

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?

MCI Benelux S.A., which supports the registration and the logistics of the organization of the virtual event through a framework contract with DG SCIC and a specific contract with FRA.

MCI Group Contact: Anne Lesca - anne.lesca@mci-group.com

MCI Brussels Contact: Karolin Fink - gdpr-brussels@mci-group.com

Aventri (support@aventri.com)

Youtube

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 is responsible for the overall organisation of the event, the communication with the speakers and participants before and after the end of the event, as well as communication and promotion of the event.

The purpose of the processing of personal data is handling registration and attendance, identify and invite plenary speakers, reporting on the event, as well as event follow-up actions, such as sharing presentations among participants and feedback collection. It includes, in particular, lists and mailing lists for contacts, invitations, participants, reports, minutes, distribution of reports/minutes, feedback on reports, meeting follow-up, photographs/pictures, presentations, audio and/or video recording of speakers and participants, news and publications.
We will collect only the following general personal data necessary for the processing operation described above.

- For **participation to dialogue, a"virtual streamed session",** pre-registration will be optional. During the pre-registration, data collected will be name, surname, age range and email address (required), and organization (optional), role (optional) and country (optional).

- **For all those recording a 1 minute video via the "online video booth"**, a dedicated consent form with provide information related to the collection, use and storage of their personal information and information. (See template)

Virtual streamed session: Audio and/or video recordings are taken during the event. All those participating in the event are responsible for their interventions with their audio and video. Clear statements will be made that the session is being livestreamed and recorded before and during the session.
Those participants not intervening with audio and/or video, will also be able to use the chat function. The chat function within Zoom will be recorded and stay available for FRA. The chat and comment on the YouTube and Facebook Live streams will remain available on demand. Users can manage those comments themselves via their profile.
YouTube Chat & Comments: Those who want to engage with the Chat (Live) functionality, should be aware that using the YouTube live chat whilst being logged in with a regular Gmail

account, will means that the user's real name will be shown. This can be changed in the display settings of your account (direct link).
For speakers of virtual videos, personal data in line with this record for processing will be collected through Video Booth Systems, in order to record and edit pre-recorded one-minute videos (consent form).

Personal data will be collected through the following means:

- during the registration process to the public session. Please note that registration to the open session will be optional.
- Active participants will connect to the web conference via the Zoom Meeting. The participants connecting to the Dialogue via Zoom Meetings, can find the Zoom privacy statement here. Any EU/EEA based person connecting to the Zoom Meeting will have their data hosted in the EEA region. See the information from Zoom regarding the AWS Risk and Compliance whitepaper and AWS Security Center.
- The collection of pre-registration data and email campaigns will be managed via the software **Aventri**. The system uses essential cookies and cookies to improve your website experience and to generate anonymous, aggregate user statistics. Aventri does not do anything with the data apart from storing it for the Contractor (MCI Benelux S.A). Event reminder emails and a post-event follow up email will be sent through Aventri (cookie policy). The only cookies that will be collected during the registration process for this event are:
- PHPSESSID: Retains session state of a user activity (1st Party – Session Cookie)
- Regtoken: To track cookie consent of all essential cookies (1st Party – Session Cookie)
- selectedlanguage: Track chosen Language (1st Party – Expires in 1 day
- cookieconsent_status: Track cookie consent of essential cookies (1st Party – Expires in 12 months)

Neither of these cookies can read or access other cookies or any data from a user's hard drive. Further, neither of these cookies alone will personally identify a user; however, a cookie will recognize a user's individual web browser or device through an IP Address, browser version, operating system and other information.
For speakers, personal details (name, surname, country of origin (optional)) and contact details (email address, affiliated organisation) will be compiled based with their consent. During the livestream on YouTube Live, the participants' comments and feedback in the chat during the open session will be enabled. By using the live chat and/or comments functionalities, the users agrees with the YouTube terms and conditions. The use of the chat/comments tool remains fully optional. by visiting the event micro-website, hosted via the webservers of one.com (cookie policy). The website uses the following first-party cookies:

Domain	Name	Value	Expires on
fra.mci-events.eu	uncodeAI.css	800x600@16	session
fra.mci-events.eu	uncodeAI.images	1032	session
fra.mci-events.eu	uncodeAI.screen	800	session
fra.mci-events.eu	uncode_privacy[conse...	%5B%5D	2021-06-09 09:50:39Z

Additionally website analytics will also be collected via Fathom, which anonymizes visitors through complex hashes. Fathom does not use cookies (data policy). Anonymised information on participation to the live streamed event (e.g. number of persons, country location, duration) will be used (YouTube privacy policies). This information will be used only for FRA internal purposes to make an evaluation of the event.Walls.io will be used to display relevant content publically available on social media channels, in order to curate an easy-to access social media wall for the Event.

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

Whose personal data are being processed?

FRA staff ☐

Non-FRA staff (speakers, public audience, any European Citizen) ☒

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: Name, surname, email address, age range (for all) ☒

Contact details e.g. role, affiliated organisation (mandatory only for speakers and one-minute-videos): ☒

Image, audio and/or video recordings of speakers and one-minute-videos ☒

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 (please specify which team and Unit) ☒

During the registration process, a restricted number of staff members, which are in charge of the event, can access your personal data. These include:

- selected staff in the Communication & events unit and its Head of Unit: Ingrid Haas, Afsheen Siddiqi, Dimitios Veremis, Miltos Pavlou and Nicole Romain
- selected staff in the Institutional Cooperation and Networks Unit (INST) and Head of Unit: Henri Nickels, Andreas Accardo
- and selected staff in Technical Assistance and Capacity Building Unit: Geraldine Guille, Sandra Aigner-Accardo, Thomas Tschernkowitsch

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

The data processor is MCI Benelux S.A., which supports the registration and the logistics of the organisation of the virtual event through a framework contract with DG SCIC and a specific contract with FRA.

- Isabelle Deniaud, Director PCO

- Mieke Barbé, Conference Manager
- Andrea Marengo, Registration Manager
- Marion Fabre, Conference Coordinator

The livestream provider CAS AV, will receive access to speakers' information in order to setup technical rehearsal calls and to help speakers connect to the livestream.
- Nicolas Cheruy, Project Manager

The video booth supplier, Videobooth Systems Limited, will have access to the speakers name, email address, organisation and recordings.

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) 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

[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.

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 kept after the Event to ensure implementing necessary follow up activities with regard to the purpose(s) of the processing of personal data as well as for its related management. Data necessary for logistics purposes (reimbursement of expenses, transport, etc.) are kept according to the rules set in the Regulation (EU, Euratom) 2018/1046.
Personal data related to registration and participation will be retained by FRA for a maximum of one year after the end of the event, which is 13 November 2021.

Photos, audio and video recordings are stored in FRA Communication and events Unit drive for three years (being considered as FRA flagship event). Within this time, the files to be used for communication purposes and/or be archived for historical purposes shall be selected. The remaining files shall be deleted.

Information concerning the event on the FRA corporate website will be retained for 10 years.

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	☒
Outlook Folder(s)	☒
CRM	☐
Hardcopy file	☐
Cloud (DMS)	☒
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 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

Part 2 – Compliance check and risk screening (internal)

11) Lawfulness of the processing (Article 5(a)–(e))[7]: Processing necessary for:

[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

Mention the legal basis which justifies the processing and assess that the purposes specified are purposes specified, explicit, legitimate.
(a) a task carried out in the public interest or in the exercise of official authority vested in the FRA (including management and functioning of the institution) ☒ (Examples of legal basis: FRA Founding Regulation (EC) No. 168/2007 establishing the European Union Agency for Fundamental Rights Articles 4.1 a) and 4.1 c);); FRA legal acts (Conditions of Employment, Staff Rules, Administrative Circular etc.) (b) compliance with a legal obligation to which the FRA is subject ☐ (c) necessary for the performance of a contract with the data subject or to prepare such a contract ☐ (d) Data subject has given consent ☒ (e) necessary in order to protect the vital interests of the data subjects or of another natural person ☐

12) **Principles relating to the processing of personal data (art. 4)**

12.1 Purpose limitation ☒

1. The purposes for data processing have been clearly identified and documented.
2. The details of the purposes of processing have been sufficiently referenced to in the privacy notice.
3. The processing is regularly reviewed, and where necessary the documentation and the privacy notice is updated.
4. If personal data is intended to be used for a new purpose, it is ensured that this is compatible with the original purpose or specific consent is taken for the new purpose.

12.2 Data minimisation ☒

1. Limited amount of personal data is collected for specific purposes (limited)

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.

2. The amount of personal data collected is adequate for the processing (adequate)

3. The personal data that is held is relevant to the processing, and periodically reviewed (relevant)

12.3 Accuracy ☒

1. Personal data held is kept accurate and up to date.

2. There are appropriate processes in place to check the accuracy of the data collected, record the source of that data, and to deal with data subject's requests for rectification of their data.

3. In case any personal data is incorrect or misleading, reasonable steps are taken to correct or erase it as soon as possible.

12.4 Storage limitation ☒

1. Personal data held is regularly reviewed and is not kept any longer than it is needed for the purpose it was collected. It is erased or anonymised when it is no longer needed.

2. Policies with standard retention periods are in place in case of data storage for periods exceeding their purpose.

3. There are appropriate processes in place to deal with data subjects' requests for erasure of their data (right to be forgotten).

4. Personal data is not kept for longer than for the intended purpose, except for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In such cases these personal data are clearly identified.

12.5 Integrity and confidentiality ☒

1. An analysis of the risks presented by the data processing is performed, therefore assessing the appropriate level of security to be put in place.

2. When deciding which security measures to implement, the state of the art and costs of implementation are considered.

3. Appropriate technical and organizational measures are in place for security of the personal data.

4. When appropriate, measures such as pseudonymisation and encryption are used.

5. There are appropriate measures in place to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

6. A well-defined information security policy is in place and is regularly reviewed for improvements.

12.6 Accountability ☒

1. Data protection policies are implemented and adopted where proportionate.

2. A 'privacy by design and default' approach is taken throughout the entire lifecycle of processing operations.

3. There are written contracts in place with organisations that process personal data on our behalf.

4. Documentation of the processing activities is maintained and kept up to date.

5. Personal data breaches are reported and recorded where necessary.

6. Data protection impact assessments are carried out and documented for personal data processing which result in high risk to data subjects' interests.

7. Adherence to relevant codes of conduct.

12.7 Transparency and Rights of data subjects ☒

1. Compliance with the conditions pertaining to the information to be provided, and the rights of data subjects mentioned in Articles 15 to 24.

2. Compliance of the data processing with the articles listed above have been stated in the privacy notice.

13) High risk identification

Does this process involve any of the following?

☐ (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

☐ (b) processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or

☐ (c) a systematic monitoring of a publicly accessible area on a large scale.

☒ N/A

☐ One or more boxes ticked = DPIA is required

Indicate if the processing operation corresponds to one or more of the types of 'risky' processing operations on the EDPS 'positive' list for which a DPIA is required, pursuant to article 39.4:

☒ N/A

☐ Yes = DPIA is required

14) Security measures checklist (art. 33)

14.1 Detailed description of information security measures in place

The Agency has several security controls in place to protect personal data from unauthorised access, use or disclosure.
The software/tools being used are GDPR compliant, and have good security measures;

Personal data will be stored on Aventri, where also the pre- and post-events emails will be sent from; the personal data will not be downloaded and stored, or sent via email.

Personal data will be accessible for FRA via an online approval report directly on Aventri, which will be password protected, so that no files with personal data need to be transferred via shared drives or via encrypted excel files & email.

The emails with participants will go via a dedicated inbox eu-fra-events@mci-group.com; emails will be sent via Outlook for Business. Only the MCI staff with access to the inbox will be able to access these emails, and MCI internal procedures include double verification to log into the server/mailboxes.

As there are no payments to be processed from participants, personal data of the participants can be purged once the contract is closed.

14.2 Supporting documentation
If applicable, indicate the relevant supporting documentation for the security measures applied:
☐ Attached
☐ Link:

14.3 Measures adopted
Indicate the type of measures in place by selecting what's applicable from the following list, or by adding measures as appropriate to the relevant processing operation:
☐ **Organisational measures**

☐ Risk Assessment and Risk management underlie the relevant security measures.
– An analysis of the risks presented by the processing has been undertaken, and it has been used to assess the appropriate level of security required to be put in place.

– When deciding what measures to implement, the state of the art and costs of implementation has been taken into account.

– An information security policy (or equivalent) or an associated set of policies are in place in specific areas and steps to make sure the policy is implemented are taken (e.g. controls to enforce them).

– The information security policies and measures are reviewed regularly and, where necessary, improved.

☐ **Technical measures**
☐ Physical security
Description
Click here to enter text.
☐ Cybersecurity
Description

Click here to enter text.

☐ Encryption and/or pseudonymisation of personal data

Description

Click here to enter text.

☐ Any other, specify

Description

Click here to enter text.

☒ The data will be hosted on infrastructure that is either owned by FRA or on 3rd party infrastructure that has been approved by FRA and meets its security requirements. Thereby, measures are in place to

- aim for using privacy-enhancing technologies (PETs);
- ensure confidentiality, integrity availability and resilience of processing systems and services;
- to restore availability and access to personal data in a timely manner in the event of physical or technical incident.

Description

Click here to enter text.

☒ Any data processor used also have appropriate technical and organisational measures in place.

Description

15) Other linked documentation

Please provide links to other documentation of this process (consent form, privacy notice, project documentation, security related policies /measures, threshold assessment or DPIA etc.)

Privacy Notice for Data Subjects FRD.docx

Consent Form speakers and one-minute-video.docx

Responsible Head of Unit	Signature	Date
Nicole Romain Communications & Events Unit	Nicole Romain Digitally signed by Nicole Romain Date: 2020.10.20 15:33:09 +02'00'	20/10/2020