RECORD OF PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 REGULATION 2018/1725[1] NOTIFICATION TO THE DATA PROTECTION OFFICER

NAME OF PROCESSING OPERATION[2]:

Operationalising National Independent Monitoring Mechanisms under the Pact on Migration and Asylum – Effective monitoring and investigations", expert meeting organised by the EU Agency for Fundamental Rights (FRA), on 9-10 November 2026, in Vienna, Austria.

Reference number: DPR-2026-263 (to be completed by the DPO)
Creation date of this record: 11.09.2026
Last update of this record:
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) Rennweg 12, 1030 Vienna, Austria Telephone: +43 1 580 30 – 0 Email: contact@fra.europa.eu Organisational unit **responsible**[4] for the processing activity: Institutional Cooperation and EU Charter Unit Contact details: DFPE@fra.europa.eu Data Protection Officer (DPO): dpo@fra.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))[5]

Reco[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 by the FRA itself ☒

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

- The European Commission, as provider of EUSurvey. FRA uses EUSurvey for the registration form and for the anonymous feedback survey, which runs with IP tracking switched off. The Commission may have access only to host and usage information (see the EUSurvey privacy statement for more information).
- Microsoft, as provider of Microsoft Teams, only if a speaker or participant joins online

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Please provide a 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 the organisation of the expert meeting "Operationalising National Independent Monitoring Mechanisms under the Pact on Migration and Asylum – Effective monitoring and investigations", taking place on 9-10 November 2026, in Vienna at FRA premises.

The meeting brings together the national Independent Monitoring Mechanisms (IMMs) that Member States are required to establish or appoint under Article 10 of the Screening Regulation and Article 43(4) of the Asylum Procedure Regulation, together with other relevant national and European actors. It follows up on the online meeting of 11 June 2026, which mapped the current status, needs and challenges of the IMMs.

FRA organises the meeting with substantive inputs from the Frontex Fundamental Rights Officer, the European Network of National Human Rights Institutions (ENNHRI) and the Council of Europe. FRA and these three organisations moderate the sessions and share their expertise during the discussions. FRA alone carries out the organisation of the meeting, including the invitations, the registration, the access to the venue and the catering.

The processing activities include sending out invitations, handling registration and attendance, granting access to the venue, taking photographs for communication purposes, organising the catering at FRA premises and a dinner at an external venue on 9 November 2026, reimbursing travel and accommodation expenses of the representatives of the national IMMs, reporting on the meeting, and follow-up actions such as sharing presentations among participants and collecting feedback. They include, in particular, the creation and management of participant lists and mailing lists, the distribution of documents and the meeting follow-up.

To invite participants, FRA uses the contact details of the participants in the online meeting of 11 June 2026, publicly available contact details found online, contacts from FRA's professional and research networks, and contacts suggested by the Frontex Fundamental Rights Officer, ENNHRI and the Council of Europe. If an invited expert cannot attend, FRA may ask them to suggest other experts from their organisation.

FRA sends the invitations by e-mail, with a link to the registration form in EUSurvey, administered by FRA. FRA collects the data that participants provide in the registration form, in the subsequent e-mail correspondence and during the meeting. Participants also provide the information FRA needs to reimburse their travel and accommodation expenses. FRA organises the reimbursement in accordance with the applicable

European Commission rules and processes the payments in SUMMA, the EU accounting system.

In the registration form, participants may indicate dietary and accessibility requirements. Dietary requirements may reveal health information or religious beliefs. FRA processes this data only with the participants' explicit consent and only to organise the catering, the dinner and access to the venue.

For access to FRA premises, FRA provides a list of participants' names for the security check at the entrance (personal data of participants to access FRA premises is processed as described in the record Record of processing - Access control and video surveillance systems in the context of FRA premises).

FRA prepares minutes and a meeting report for reporting and follow-up. The minutes do not attribute statements to named individuals, and the report does not name the participants.

With the participants' consent, FRA compiles a participant list with name, surname, contact details, function/job title, and the name and type of the employer/organisation. FRA shares this list with the Frontex Fundamental Rights Officer, ENNHRI, the Council of Europe, other participants and other relevant bodies included in the functioning of the IMM, to facilitate communication between participants. FRA also shares the agenda, including the names, photographs and short biographies of speakers and moderators, with the participants and the three organisations.

The meeting is an in-person meeting. If a speaker or participant cannot travel, they may connect via Microsoft Teams, and the meeting becomes hybrid.
With the participants' consent, FRA staff take photographs during the meeting, which FRA may publish on its website and social media channels. At the end of the meeting, FRA collects anonymous feedback through a satisfaction survey in EUSurvey, with IP tracking switched off.

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 meeting, which include policy makers, public authorities, national human rights institutions, equality bodies, data protection officers, non-governmental organisations, service provides, social partners, experts, officials from EU or UN organisations)

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: title, first name, surname, country of residence ☒

Contact details: email address, mobile telephone number ☒

Education & Training details ☐

Employment details: function/job title, name and type of employer/organisation) ☒

Financial details: ☒

For participants whose travel and accommodation expenses are reimbursed, FRA collects the following data for the processing of payments in SUMMA (see the related data protection notice):

- Business partners: date, place and country of birth, address, e-mail, identity document number, personal identification number, banking details (including bank account information and possibly a bank statement), possibly business data, and a legible copy (recto/verso) of an identity card, passport or other identification document
- Supporting documents (e.g. invoices, tickets, boarding passes)

If participants or their employer are already registered in SUMMA, FRA asks participants to verify the accuracy of their information by sharing their IBAN and date of birth with FRA.

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other: ☒

- Registration via EUSurvey, administered by FRA:
  - IP addresses and technically necessary and security cookies
  - Metadata, such as the response timestamp
  - EUSurvey uses the Europa Analytics service for traffic statistics and analytics. For further information see the Europa Analytics website, where information can be found about the cookies and IP address collected by the European Commission website, as well as its cookies policy
- Anonymous feedback survey in EUSurvey at the end of the meeting. IP tracking is switched off, so no personal data is collected through it.
- Online participation via Microsoft Teams, if the meeting becomes hybrid: name, surname, e-mail, profession and organisation when connecting to the platform; cookies (Microsoft uses necessary cookies and optional social media, analytics and advertising cookies, which participants can reject in their web browser); and the image of speakers and participants who switch on their camera.
- Photographs of participants taken by FRA staff during the meeting, upon consent, which FRA may publish on its website and social media channels.
- Photograph and short biography of speakers and moderators, for inclusion in the agenda. The agenda is shared with the participants and with the Frontex Fundamental Rights Officer, ENNHRI and the Council of Europe.

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

Data concerning health and/or religious beliefs, such as dietary requirements and accessibility, necessary for the organisation of the catering services and access to the venue may be collected from participants, upon consent, if they have previously declared in the registration form that they have such special requirements.

The photo of speakers and moderators provided with the bio, as well as image of participants being photographed at the event might reveal racial or ethnic origin, health conditions and religious beliefs.

The personal data collected might reveal:

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 ☐

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?*

Designated **FRA** staff members ☒

A restricted number of FRA staff in the Institutional Cooperation and EU Charter Unit (Donor-funded Programmes and Enlargement Sector) and in the Justice, Digital and Migration Unit (Migration and Asylum Sector), responsible for organising the expert meeting, has access to the personal data. A restricted number of staff in the Administration Unit (Finance Sector) has access to the financial data when the reimbursement of travel or accommodation expenses is necessary. Assigned staff from the Administration Unit (Digital Services Sector) might have access to some personal data necessary to provide technical support.

Recipients **outside** FRA: ☒
(European Commission; Microsoft; the Frontex Fundamental Rights Officer, ENNHRI and the Council of Europe; other participants and other relevant bodies included in the functioning of the IMM; the general public, for published photographs)

European Commission, as provider of EUSurvey: the Commission may have access only to host and usage information of respondents to the registration form and the feedback survey.

Microsoft: if the meeting becomes hybrid, certain connection details and other metadata might be accessed by Microsoft 365 when connecting to the online meeting, as indicated in the respective FRA's data protection notice.

Frontex Fundamental Rights Officer, ENNHRI and the Council of Europe: with the participants' consent, FRA shares the participant list (name, surname, contact details, function/job title, name and type of the employer/organisation) with these organisations, with other participants and with other relevant bodies included in the functioning of the IMM, to facilitate communication between participants. The agenda, including the names, photographs and short biographies of speakers and moderators, is shared with the participants and with the three organisations. FRA shares the list with the Council of Europe at the end of the meeting.

General public: photographs published on FRA's website and social media channels, with the participants' consent, are accessible to the general public.

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 ☐

FRA does not share the contact details or other personal data of participants with the Council of Europe, except as described below.

Upon consent from participants, FRA will only share, at the end of the meeting, the list of participants (containing name, surname, contact details, function/job title, name and type of the employer/organisation) with the Council of Europe, which is an international organisation, on the basis of Article 50(1)(a) of Regulation (EU) 2018/1725. The agenda of the meeting, including the names, photographs and short biographies of speakers and moderators, is also shared with the Council of Europe.

If yes specify to which organisation: Council of Europe

[6] **Processo**r 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.

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"?

Personal data is kept after the meeting to carry out the follow-up activities and the related management. Information and personal data collected by FRA in the context of the organisation of this expert meeting will be kept for one year after the event.

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

Photographs published on FRA's website and social media channels will remain publicly available for as long as the relevant content is maintained online, in accordance with the retention periods of the respective platforms. Photographs taken during the event and not published will be deleted after the event.

Special categories of personal data relating to dietary and/or accessibility requirements will be deleted as soon as they are no longer necessary for the purpose for which they were collected, and in any event no later than one month after the end of the meeting.

The data related to the financial and legal identification form for business partners and the supporting documents needed for the reimbursement of participants are kept for a maximum of 10 years after the last transaction related to the data subject (see the related data protection notice).

For information about the retention periods of EUSurvey, please consult the privacy statement.

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 (MS 365)	☒

Servers of external provider) ☐

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 DFPE@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