

**RECORD OF PROCESSING ACTIVITY  
ACCORDING TO ARTICLE 31 REGULATION 2018/1725<sup>1</sup>  
NOTIFICATION TO THE DATA PROTECTION OFFICER**

**NAME OF PROCESSING OPERATION<sup>2</sup>:**

**Consultation, cooperation and meetings with Member States' National Liaison Officers (NLOs) including the organisation of FRA-NLO Meetings**

Reference number: DPR-2023-192
Creation date of this record:
Last update of this record:
Version: 1

**Part 1 (Publicly available)**

<b>1) Controller(s)<sup>3</sup> of data processing operation (Article 31.1(a))</b>
Controller: European Union Agency for Fundamental Rights (FRA) Schwarzenbergplatz 11, A-1040 Vienna, Austria Telephone: +43 1 580 30 – 0 Email: <a href="mailto:contact@fra.europa.eu">contact@fra.europa.eu</a> Organisational unit <b>responsible<sup>4</sup></b> for the processing activity: Institutional Cooperation and Networks Unit Contact details: <a href="mailto:nlo@fra.europa.eu">nlo@fra.europa.eu</a> Data Protection Officer (DPO): <a href="mailto:dpo@fra.europa.eu">dpo@fra.europa.eu</a>

<sup>1</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725>

<sup>2</sup> **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.

<sup>3</sup> In case of more than one controller (e.g. joint FRA research), all controllers need to be listed here

<sup>4</sup> This is the unit that decides that the processing takes place and why.

2) Who is actually conducting the processing? (Article 31.1(a))<sup>5</sup>

The data is processed by the FRA itself

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

For managing the contact list of NLOs and to carry out the activities that FRA undertakes in the context of its cooperation with NLOs, FRA uses [Microsoft Office 365](#) cloud-based services. Therefore, Microsoft Ireland acts as FRA processor for this purpose. Moreover, for the organisation of meetings, FRA might use external contractors, which will act as FRA processors.

In addition, FRA or FRA processors might use different online tools/systems to organise meetings in the context of its NLOs activities (for example, [Lime Survey](#) or [Webex](#)), which will act also as FRA processors.

The contact point for all processing operations is the Agency.

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).*

We collect and maintain personal data of a contact group list entitled “National Liaison Officers” within FRA to support the cooperation and consultation of the Agency with this specific stakeholder.

National Liaison Officers (NLOs) are officially appointed to FRA as primary contact for their Member States. The contact group list, which includes NLOs, alternate and other operational contacts aims to:

- facilitate the interactions and exchange of information on activities between FRA and Member State’ governments, ministries and other national authorities through the NLOs;
- allow the organisation of meetings (in persons, virtual or hybrid) to inform NLOs about FRA work;
- allow FRA to organise the travel and accommodation of NLOs participating at the FRA-NLO meeting and/or the payment/reimbursement of the related costs in line with the FRA mission guide;
- facilitate the consultation of Member States through the NLOs on the FRA Programming document, FRA Annual Report, FRA External evaluation and other thematic consultations for FRA projects and activities;
- facilitate the organisation of online information sessions and/or webinars for ministries and other national authorities to present FRA tools and upcoming reports;
- allow FRA to send to NLOs additional information related to news, activities about FRA and its work, as well invitation to meetings or events of relevance for NLOs and/or Member States.

<sup>5</sup> Is the FRA itself conducting the processing? Or has a provider been contracted?

- support the regular exchange of communication by telephone or emails with NLOs about FRA work in compliance with the provisions in the Founding Regulation.

In line with the principle of transparency, NLOs are informed by FRA, following their nomination by their Member States, that the name and affiliated ministry of NLOs and alternate members shall be made public and shall be updated by the Agency on its web site for the duration of their function as NLO/alternate member.

The personal data is collected and processed as follows:

Upon their official nomination, the relevant ministry or national authority provides FRA with the contact information of the appointed NLOs (name, address, e-mail addresses, and phone number, title and function).

After receipt of the information on their nomination, the Agency informs NLOs about their role, an overview of activities concerned by NLOs and that their contact details (name, organisation, NLO function) will be published on FRA's website to comply with the Agency's transparency obligations.

For supporting the cooperation with NLOs and regular contacts, FRA centralises NLOs names, contacts details and affiliated organisation in an Excell list on DMS Sharepoint accessible to restricted number of FRA Staff directly in charge with the daily management of the cooperation with NLOs.

For the organisation of the NLOs meetings, including the travel and accommodation as well as catering arrangements, FRA or its processors might collect from you the personal data described in section 5 via the registration to the meeting.

For sharing and distributing documents, the Agency uses the following cloud based services on the basis of the inter-institutional framework contract for the provision of M365 services, of which the Agency is a part:

- MS Teams.
- FRA DMS SharePoint to maintain FRA master list of NLOs contacts and centralise documentations related to the day-to-day management of NLOs by the relevant unit in FRA.
- The NLO mailbox ([nlo@fra.europa.eu](mailto:nlo@fra.europa.eu)) for centralizing all email communications related to the FRA cooperation with NLOs.

Other online tools/systems used for the sharing of files, and/or online consultation or scheduling meetings which FRA or its contractors might use for the purposes of communicating with you or organizing meetings might also collect and process some personal data (such as IP addresses, cookies, metadata or information about your device). In particular, FRA uses:

- LimeSurvey (professional online survey tool, also used for registration to NLO meetings)
- Webex for online/hybrid NLO meetings and FRA online information sessions for national authorities.

In case other tools/systems are used by FRA or its contractors for specific meetings or other purposes, data subjects will be informed accordingly via the invitation to the meeting or the registration form.

For supporting the cooperation with National Liaison Officers (NLO) and regular contacts, FRA centralises NLOs names, contacts details and affiliated organisation in an Excell

list on DMS Sharepoint accessible to restricted number of FRA Staff directly in charge with the daily management of the cooperation with NLOs. NLOs emails and contact details are shared internally with FRA staff to facilitate contacts between FRA and the respective NLOs for the purpose of the cooperation.

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

*Whose personal data are being processed?*

- |  |                                     |
|--|-------------------------------------|
| FRA staff  | <input type="checkbox"/>            |
| Non-FRA staff<br>(National Liaison Officers, alternates, and other operational contacts) | <input checked="" type="checkbox"/> |

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

*Please tick all that apply and give details where appropriate*

##### (a) General personal data

Personal details   
Civil title, first name and surname. For organising travel and accommodation in the context of FRA-NLO meetings, participants might be required to provide date of birth, ID or passport number to FRA or to FRA's external contractor responsible for the organisation of the meeting. Collecting such data might be necessary in those cases to comply with the national and international laws applicable to travels and air carriers

Contact details   
(e-mail address, phone, mobile numbers (as optional), postal address)

Education & Training details (CVs)

Employment details   
(function/title, name and type of the employer/organisation)

Financial details (financial identification form, bank account information only when FRA organises the reimbursement of travel to join the FRA-NLO meetings.)

Family, lifestyle and social circumstances

Goods or services provided

(b) Other:

- Information regarding their appointment as EU Charter Focal Point or FREMP delegate in the Council of the EU, as this is of relevance for FRA work.
- Image, messages, chat, questions, FRA documents, audio and/or video recordings of the participants in case meetings take place online or in a hybrid format, or audio-recording in case of face-to-face meetings for the purposes of minutes-taking.
- Image, messages, chat, questions, FRA documents, audio and/or video recordings of the participants to the FRA online information sessions when recording of the session is specifically indicated in the invitation.
- IP addresses and/or cookies of participants and other metadata may also be collected by the online tool used in case the meetings take place online or in a hybrid format.

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

The personal data collected reveal:

Racial or ethnic origin.   
 Racial or ethnic origin might be revealed by the image and video recording, in case of online or hybrid meetings

Political opinions

Religious or philosophical beliefs

Religious or philosophical beliefs be revealed by the image and video recording, in case of online or hybrid meetings. Food preferences might also reveal religious beliefs, only in the context of catering and/or dinners offered during in person meetings organised by FRA

Trade union membership

Genetic, biometric or data concerning health

Food preferences indicated by the participants might reveal health conditions, only in the context of catering and/or dinners offered during in person meetings organised by FRA, or limited information on health conditions, such as special accommodations requirements for persons with disabilities, that need to be taken into account for organising the venue of NLOs to a FRA meeting.

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? 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

A restricted number of FRA staff responsible for the NLOs activities has access to your contact details. A restricted number of staff in Corporate Services (Finance Sector) has access to the financial data when the reimbursement of travel and accommodation expenses is necessary. Assigned staff from Digital Services (Corporate Services) might have access to some personal data necessary to provide technical support.

In case of reimbursement of costs for travels to NLOs, financial or legal identification forms are transferred to the European Commission (DG Budget) in order to validate data subjects' details in the European Union's accounting system ABAC. Data is processed in this regard in line with FRA's data protection notice [here](#).

Recipients **outside** FRA:

Moreover, restricted staff of FRA contractors, which are bound by specific contractual clauses for any processing operations of NLOs' personal data on behalf of FRA, and by the confidentiality obligations deriving from Regulation (EC) 2018/1725) might have access to some personal data as indicated in the respective data protection notices referred to above.

#### 7) Transfers to third countries or international organisations (Article 31.1 (e))<sup>6</sup>

*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

However, the transfer of limited personal data (diagnostic data) outside the EU and EEA might occur when using MS Teams and other online tools/systems mentioned above to perform the tasks related to the NLOs participation in FRA activities. We refer to the respective data protection notices for more information.

**If yes, specify to which country:**

<sup>6</sup> **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.

***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 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"?*

We keep NLOs' data for the duration of their role as National Liaison Officer or alternate plus one year

Information and personal data collected by FRA in the context of the organization of meetings (namely, list of participants) will be kept for one year after the meeting. Personal data collected by FRA's contractors in the context of meeting will be deleted after the end of the respective specific contract.

Information and personal data collected by FRA in the context of consultations with the NLOs will be retained until one year after the end of the consultation.

The data related to the Financial and Legal identification form is kept for a maximum of 10 years after the last transaction of data related to the data subject (please refer to the relevant data protection notice [here](#)).

Audio and/or video recordings are stored in a FRA Institutional Cooperation and Networks Unit project library (which is accessible only to designated FRA staff) in FRA's data management system (DMS) for 6 months. In this respect, please see [FRA's privacy notice regarding the use of Microsoft Office 365](#).

Information concerning the event on the FRA corporate website will be retained for five 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?**

- |                                  |                                     |
|----------------------------------|-------------------------------------|
| Document Management System (DMS) | <input checked="" type="checkbox"/> |
| 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 ( <a href="#">MS 365</a> ) | <input checked="" type="checkbox"/> |
| Servers of external provider     | <input checked="" type="checkbox"/> |

If some of the activities are outsourced by FRA (for instance, the organisation of NLO meetings) some personal data might be stored on FRA's external contractors' servers, which are deemed to implement technical and security measures in accordance with the data protection clauses under the respective contracts.

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: [nlo@fra.europa.eu](mailto:nlo@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))<sup>7</sup>: Processing necessary for:  
*Mention the legal basis which justifies the processing and assess that the purposes specified are purposes specified, explicit, legitimate.*

---

<sup>7</sup> 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 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.