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

NAME OF PROCESSING OPERATION[2]: Call for expressions of interest 2022 for the members of the Scientific Committee of FRA

Reference number: DPR-2020-166 (to be completed by the DPO)
Creation date of this record: 28/07/2022
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) 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: Corporate Services (CS), HR Sector Contact details: selection-scientific-committee@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	☒
The data is processed also by a third party (contractor) [mention the third party]	☐

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?

(Specify if they are processors or joint controllers)

Contact point at external third party (e.g. Privacy/Data Protection Officer – use functional mailboxes, not personal ones, as far as possible): *Name/Surname/Email address*

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 carry out the selection of the members of the FRA's Scientific Committee. The Scientific Committee is one of the bodies of the Agency as defined in Article 14, paragraph 1 of the Council Regulation (EC) 168/2007 establishing the European Union Agency for Fundamental Rights, amended by Council Regulation (EC) 2022/555, according to which the Management Board of the Agency shall appoint the members of the Scientific Committee following a selection procedure.

Annex I of the Rules of Procedure of the Agency describe the process for the selection of the members of the Scientific Committee.

The Agency uses for processing the applications the Limesurvey tool. The Agency only process the personal data that the applicants provide during the application by filing in the forms in the tool. No personal data, cookies or IP addresses are stored by the tool.

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

Whose personal data are being processed?

FRA staff ☐

Non-FRA staff (nationals of an EU Member State applying for the position of member of the Agency's Scientific Committee.) ☒

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, date of birth, gender, nationality, address, ID/passport copy of selected candidates) ☒

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Contact details (postal address, email address, mobile)	☒
Education & Training details (education, training skills, languages, letter of motivation	☒
Employment details (work experience, languages, name and type of the employer/organisation, address of the employer/ organisation)	☒
Financial details (financial identification form, bank account information for selected candidates)	☒
Family, lifestyle and social circumstances	☐
Goods or services provided	☐
Other (please give details):	

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

Racial or ethnic origin	☒

(Selected candidates are required to provide copies of their ID/passport documents, which include pictures. This might reveal their 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? 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:
Data can be accessed by the staff dealing with the selection of members of the Agency's Scientific Committee and the FRA staff who are members of the pre-selection panel, namely, the Director and the Heads of Unit ☒

Recipients **outside** FRA: ☒

The recipients are:

- The members of the pre-selection panel who are not FRA staff, namely one representative of the Council of Europe and two observers from the Management Board
- Selection Panel composed of the Agency's Executive Board (only for the shortlisted candidates)
- FRA Management Board members, only for the shortlisted candidates)
- European Parliament LIBE Committee – only for the shortlisted candidates and upon their prior consent requested by email. This is in accordance with Article 14 of Regulation 168/2007 and recital 21 of Regulation 2018/1725.

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 ☒

[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.

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"?

Unsuccessful candidates' personal data is stored for a period of 2 years year after the closure of the file (appointment) for the 11 selected candidates and for the candidates on the reserve list. The successful candidates' personal data (and of the candidates on the reserve list) is kept for 5 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)	☒
FRA network shared drive	☒
Outlook Folder(s)	☒
CRM	☐
Hardcopy file	☒
Cloud (give details, e.g. cloud provider)	☐
Servers of external provider	☒

Applications are processed via the Agency's IT recruitment tool Limesurvey, hosted at the data centre of FRA's web hosting contractor.

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 selection-scientific-committee@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 5.1.(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 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.

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) ☒

Article 14 of Regulation (EC) No. 168/2007 establishing the European Union Agency for Fundamental Rights, amended by Regulation 2022/555 (FRA Founding Regulations).
The procedure for the selection of the members of the Scientific Committee is established in Annex I of the Rules of Procedure of the Agency.
Therefore, the processing is lawful under Article 5.1.(a) of Regulation 2018/1725.

(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 ☒

Since the participation in the call for expression of interest is not mandatory, the processing is lawful under Article 5.1(d) of Regulation 2018/1725 because "the data subject has unambiguously given his or her consent" by submitting his/her application.

(e) necessary in order to protect the vital interests of the data subjects or of another natural person ☐

With regards to special categories of personal data, the processing is lawful under Article 10.2(a) (the data subject has given explicit consent) and Article 10.2(b) of the Regulation 2018/1725.

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 Data Protection notice.
3. The processing is regularly reviewed, and where necessary the documentation and the Data Protection 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)

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 Data Protection 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 FRA applies standard security measures to safeguard integrity, availability and confidentiality of personal data and avoid any potential disclosure, access, alteration, destruction or loss of personal data.

The security measures embrace organisational and technical measures.
Organisational measures include:

- ICT and Data Management Policy
- Internal rules on the use of the internet
- Internal rules on data retention
- Staff training on data protection
- Risk assessment of the processing operations

Technical measures include:

- Cybersecurity
- Physical security
- Report mechanism for security issues
- Control of access to electronically held information
- Password policy
- Encryption or pseudonymisation
- Data breach policy

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

Selection files are kept in hard copy in accordance with the Agency's retention policy and stored in locked safes in the HR offices, accessible only to designated HR staff members with a key.
☒ 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
Click here to enter text.

15) Other linked documentation

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

Data protection notice

Responsible	Signature	Date
Head of Unit		

Constantinos Manolopoulos
Head of Corporate Services