

**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>: – Interviews with technical experts and diverse users/experts for FRA’s project on the ‘Digitalisation of justice: fundamental rights guidance’ (FRANET Service Request 33)**

Reference number: DPR-2024-217
Creation date of this record: 08 May 2024
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>
<p>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: Justice, Data and Digital Unit          Contact details: <a href="mailto:justice_security@fra.europa.eu">justice_security@fra.europa.eu</a>          Data Protection Officer (DPO): <a href="mailto:dpo@fra.europa.eu">dpo@fra.europa.eu</a></p>

<b>2) Who is actually conducting the processing? (Article 31.1(a))<sup>5</sup></b>
<p>The data is processed by the FRA itself <input checked="" type="checkbox"/></p> <p>The data is processed also by a third party (contractor) <input checked="" type="checkbox"/></p>

<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.

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

7 FRANET contractors through an existing framework contract. Please find the contact details [here](#). Contact point at external third party:

Austria - European Training and Research Centre for Human Rights and Democracy - ETC Graz

Estonia - Tallinn University

France- French Institute for Human Rights and Civil Liberties

Italy - Giacomo Brodolini Foundation

Latvia - Baltic Human Rights Society and Riga Graduate School of Law

Poland - Helsinki Foundation for Human Rights

Portugal - Centre for Social Studies

The above FRANET contractors may use different sub-processors (i.e., experts acting as subcontractors, companies providing online conference tools, etc.) to implement the respective specific contract. Data subjects will be informed accordingly in the respective data protection notice and/or consent form.

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

*Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).*

The purpose of the processing of the personal data is to collect information and data for a research project on the *Digitalisation of justice: fundamental rights guidance*.

This project is intended to provide FRA with research evidence on the actual operation of selected use-cases of digitalisation in the justice field, in seven EU Member States (Austria, Estonia, France, Italy, Latvia, Poland and Portugal). It will serve to increase the understanding of fundamental rights challenges as well as promising practices that have emerged in Member States as they digitalise their justice systems, as well as how digitalisation affects the work of justice professionals. Based on the research findings, FRA will develop guidance that will help Member States to ensure high standards of fundamental rights protection via digitalisation at national level. In this way, the Agency hopes to inform the implementation of current and future EU policy and law relating to the digitalisation of justice.

This project consists of a mix of fieldwork and desk research (Service Request 33). The fieldwork will involve interviews with technical experts and diverse users (mostly legal practitioners such as judges, prosecutors, lawyers or law enforcement officials), in Austria, Estonia, France, Italy, Latvia, Poland and Portugal carried out by **FRANET**<sup>6</sup>

---

<sup>6</sup> FRANET contractors covering all EU Member States have been selected by FRA following a public procurement procedure to provide data collection and research services on fundamental rights issues.

contractors across the aforementioned 7 Member States. The information from the interviews will feed into the preparation of a report to be published in 2025.

FRANET contractors will use information gathered through the desk research component of the project (SR 33) to identify persons to be interviewed. They may also use other channels and find the contact details of the persons to be interviewed via their own networks, FRA networks (subject to receiving consent for sharing their contact details with the FRANET contractors) or other organisations and authorities of the respective EU Member State.

The personal data specified in section 5 below will be collected through the consent forms that will be provided to the interviewees before the interview, and during the interview, which will be conducted in person or through digital channels, e.g. internet and/or telephone or video call by FRA's FRANET contractors in the 7 countries covered by the research. Written consent form can be replaced by an audio/video recording of the consent.

For accuracy and note taking purposes, interviews will be audio- and/or video-recorded upon your consent (and in the case of two of the pilot interviews, fully transcribed). Participation is voluntary. Interviewees can discontinue their participation at any time or refuse to answer any question without consequence of any kind and without giving a reason.

Moreover, at any point during the interview, interviewees can indicate that they do not wish to be recorded.

The names of the interviewees will not appear in the final report. Moreover, all recordings will be destroyed as indicated in section 8 below.

In case an interview takes place online, FRANET contractors are requested to inform interviewees before the interview takes place about which online conference tool they will use for the interview and to provide a link to the tool's website where the tool's data protection policy can be found.

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

*Whose personal data are being processed?*

FRA staff

Non-FRA staff (please specify e.g. Roma community, judges, etc.)

Interviewees: Technical/IT professionals working for Justice ministries, police, courts or prosecution services / Diverse end users or experts (people working for justice systems that use the digital tools/systems in the selected use cases – could be judges, prosecutors, law enforcement, lawyers/legal counsels or other individuals/representatives of bodies or organisations that represent individuals (as complainants or victims) affected by the particular use case. This could also include NGOs or NHRBs supporting people in accessing justice / Other experts with direct knowledge or experience of the use case at the heart of the interview.

#### 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 (name, surname, gender, age range).

Contact details (email address, phone number).

Education & Training details

Employment details (e.g. work experience, languages, name and type of the employer/organisation, address of the employer/ organisation)

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

Family, lifestyle and social circumstances (this type of personal data might be incidentally revealed by the responses given during the interviews and/or by the image if the interviews are carried out online and videorecorded).

Goods or services provided

Other (please give details):

- If the interviews with the relevant persons take place online, IP addresses, cookies, metadata or information about participants' devices might be collected by the online tools used to carry out the interview.
- As the interviews will be video and/or audio recorded (upon consent) for accuracy and note-taking purposes, voice and/or image of the participant will be processed.

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

Although there is no intent to process special categories of personal data for the abovementioned purposes, there is a possibility that personal data – such as below - may be communicated incidentally by interviewees to FRANET in the course of interviews and through the image showed during the online interviews:

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



Designated staff members of FRA's Justice, Digital and Migration Unit and FRA staff working on the project .

Recipients **outside** FRA:



Designated staff of the FRANET contractors carrying out the interviews as well as potentially selected staff of the respective sub-processors as indicated in section 2

7) Transfers to third countries or international organisations (Article 31.1 (e))<sup>7</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, if the online tool used by the respective FRANET contractor to carry out the interviews are from a US based company, it cannot be completely discarded that limited personal data is transferred. Such transfer, if any, will fall under the adequacy decision for the EU-US [Data Privacy Framework adopted by the European Commission on 10 July 2023](#).

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

**Transfer to international organisation(s)**

Yes

<sup>7</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.

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 defence 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"?*

The personal data referred to in section 2 above, as well as consent forms and audio/video recordings, will be kept for 24 months after the final date of implementation of the project indicated in the respective FRANET contracts, to be able to use the data when drafting the comparative report. All data held by FRA and contractors will then be deleted. Anonymised research material, e.g. reporting templates, will be kept indefinitely.

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 (MS 365, see record <a href="#">here</a> )  | <input checked="" type="checkbox"/> |
| Servers of external provider  | <input checked="" type="checkbox"/> |
| Other: The data is stored by FRANET contractors in the EU and not transferred outside EU. |                                     |

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 [justice\\_security@fra.europa.eu](mailto:justice_security@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