

**RECORD OF PROCESSING ACTIVITY
ACCORDING TO ARTICLE 31 REGULATION 2018/1725¹
NOTIFICATION TO THE DATA PROTECTION OFFICER**

NAME OF PROCESSING OPERATION²: *Fieldwork of the project 'Fundamental rights implications of accessing digital data for criminal investigations'*

Reference number: DPR-2025-248 (to be completed by the DPO)
Creation date of this record: 18 November 2025
Last update of this record:
Version: 1

Part 1 (Publicly available)

1) Controller(s)³ of data processing operation (Article 31.1(a))
<p>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 responsible⁴ for the processing activity: Justice, Digital and Migration Unit Contact details: justice_security@fra.europa.eu Data Protection Officer (DPO): dpo@fra.europa.eu</p>

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

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?

When interviews take place online, limited personal data specified in section 5 may be processed by [Microsoft](#) or [Cisco Webex](#). Details about the processors can be found in the respective data protection notices.

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 the personal data is to collect information and data for a research project titled “Fundamental rights implications of accessing digital data for criminal investigations”.

This project is intended to provide FRA with research evidence that could support the ongoing discussions at the EU and national levels about access to digital data for criminal investigations, focusing in particular on workarounds available to law enforcement to access data from encrypted devices and communications. Among others, it should inform the preparation of the Technology Roadmap on Encryption, envisaged by the European Commission in the [ProtectEU Internal Security Strategy](#) for 2026.

The project consists of fieldwork accompanied by additional desk research. The fieldwork will involve interviews with practitioners involved in the use of encryption workarounds and other experts with particular experience in this field, with particular focus on the fundamental rights impact of existing and potential future workarounds. Interviewees will represent law enforcement, public prosecutors and judges in selected Member States; defence lawyers, legal, technical and civil society experts; as well as representatives of service providers targeted by law enforcement requests and companies providing decryption and related services.

To identify the contact details of the persons to be interviewed, FRA will use information gathered through authorities of the respective EU Member State or other organisations or entities, professional networks and by searching for publicly available information. All interviews will be conducted directly by FRA staff. Information from the interviews will feed into the ongoing discussions at the EU and national levels and a FRA report (foreseen to be published in 2026).

Personal data specified in section 5 below will be collected through consent forms that will be provided to interviewees before the interview, and during the interviews using a semi-structured questionnaire, which will be conducted by FRA staff through digital channels (e.g. video call) or face-to-face.

For accuracy and note taking purposes, interviews will be audio- and/or video-recorded upon interviewees’ consent.

In case an interview takes place online, FRA intends to use the online conferencing tools [Teams](#) or [Webex](#). Interviews taking place online will also be recorded and automatically transcribed using the AI powered features embedded in Teams or Webex, upon interviewees’ consent. More information on those AI features in [Teams](#) and [Webex](#) can be found under the respective links.

Exceptionally, if the interviewees cannot use any of these two online tools, we will consider using another tool they propose, which will be agreed individually before the interview takes place.

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 and organisation of the interviewees will not appear in the final report, which will be duly anonymised. Moreover, all recordings will be destroyed as indicated in section 8 below.

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

Whose personal data are being processed?

- FRA staff
- Non-FRA staff

Interviewees: law enforcement, public prosecutors and judges in selected Member States; defence lawyers, legal, technical and civil society experts; as well as representatives of service providers targeted by law enforcement requests and companies providing decryption and related services.

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)
- Contact details (email address, phone number)
- Education & Training details
- Employment details (position/function, organisation, work experience, opinions)
- 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 and automatically transcribed (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 in the course of interviews and through the image showed during the online interviews:

Racial or ethnic origin	<input checked="" type="checkbox"/>
Political opinions	<input checked="" type="checkbox"/>
Religious or philosophical beliefs	<input checked="" type="checkbox"/>
Trade union membership	<input type="checkbox"/>
Genetic, biometric or data concerning health	<input checked="" type="checkbox"/>
Information regarding an individual's sex life or sexual orientation	<input checked="" type="checkbox"/>
N/A	<input type="checkbox"/>

(c) Personal data relating to criminal convictions and offences (Article 11)

Criminal record (or similar, e.g. declaration of good conduct)	<input type="checkbox"/>
N/A	<input checked="" type="checkbox"/>

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	<input checked="" type="checkbox"/>
Designated staff members of FRA's Justice, Digital and Migration Unit and FRA staff working on the project.	
Recipients outside FRA:	<input checked="" type="checkbox"/>
For interviews taking place online, limited personal data as mentioned in section 5 may be processed by Microsoft or CISCO Webex.	

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

However, the online tools MS Teams and Webex used to carry out the interviews are from US based companies, therefore it cannot be completely discarded that limited personal data are transferred to the US. 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](#).

Furthermore, FRA is part of Microsoft ILA 2025 Data Protection Terms signed between the European Commission and Microsoft which includes a set of improvements specific to the data protection safeguards in place for M365. Personal data stored and processed by M365 within the EU and EFTA regions (EU Data Boundary). Transfers of personal data for M365 outside the EU or EFTA got strictly limited to specific purposes such as security, resiliency, and customer-initiated actions. Any (residual) transfers to non-adequate jurisdictions are limited to a small number of countries. All transfers must follow documented instructions.

More information concerning CISCO Webex can be found in section 8 of the data protection notice [here](#).

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)

Transfer subject to appropriate safeguards (Article 48.2 and .3), specify:

- a) A legally binding and enforceable instrument between public authorities or bodies.

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.

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 5 above, as well as the consent forms and audio/video recordings of the consent, will be kept for 18 months after the finalization of the fieldwork phase of the project (i.e., until 31 May 2027), to be able to use the data when drafting the report. All data held by FRA 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 here) | <input checked="" type="checkbox"/> |
| Servers of external provider | <input type="checkbox"/> |

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

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