EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

NAME OF PROCESSING OPERATION[2]: "Remote biometric identification for law enforcement purposes: selected use-cases"

Reference number: DPR-2024-210
Creation date of this record: 26 April 2024
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: Justice, Digital and Migration Unit. Contact details: rbiproject@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 third parties:	☒
FRA's external contractor **AWO Belgium**, located at Sq. de Meeûs 35, 1000 Bruxelles, Belgium, acting as FRA's processor. Data protection focal point: privacy@awo.agency.	

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?

Moreover, AWO will use the services of the following sub-processors:

- IPSOS – to conduct a small-scale quantitative survey with rights-holders
  Registration: France
  DP contact point: Chief Privacy Officer, Mr. Rupert van Hüllen. Rupert.vanhullen@ipsos.com
  Link to data protection notice: https://www.ipsos.com/en/privacy-data-protection
- Microsoft - providing office, email and cloud services as well as MS Teams as online video conference tool in case interviews take place online
  Registration: US
  DP contact point: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-data-protection-officer
  Link to data protection notice: https://privacy.microsoft.com/en-us/data-privacy-notice
- Zoom – as online video conference tool in case interviews take place online and respondents cannot use MS Teams
  Registration: US
  DP contact point: Data Protection Officer, privacy@zoom.us.
  Link to data protection notice: https://explore.zoom.us/en/privacy/
- Individual experts – individual experts sub-contracted by AWO to carry out parts of the research process, where needed (e.g., country experts for a particular country);
  DP contact point: AWO DP focal point will receive requests directed to individual experts and forward them to the relevant individual, as relevant
- Keepit – providing backup services to AWO
  Registration: Denmark
  DP contact point: DPO, dpo@keepit.com
  Link to data protection notice: https://www.keepit.com/privacy-policy/

The contractor was selected by FRA following a public procurement procedure.

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 main purpose of the processing is to provide the Agency with research evidence on the actual operation of selected use-cases of remote biometric identification (RBI's) in the context of law enforcement in six Member States (France, Germany, Greece, Hungary, Italy and The Netherlands), and the related fundamental rights implications.

The results delivered by this research will be the basis for drafting a FRA comparative report that will complement FRA's wider body of research on artificial intelligence, big data and fundamental rights.

To this aim, personal data will be processed in the context of:

- Conducting desk research to provide high-level analysis of RBI use cases for law enforcement purposes, their fundamental rights impact and legislative/regulatory framework in the six selected EU Member States;

- Conducting semi-structured face-to-face interviews with stakeholders from national law enforcement agencies, technology providers, data protection authorities, national human rights institutions, civil society organisations and rights holders. Most of the interviews will be conducted in person and the answers will be anonymised. If necessary, the contractor might also carry out interviews via video calls (MS Teams or, alternatively, Zoom) in agreement with the respondents and upon approval by FRA;
- Conducting two small-scale quantitative surveys on the rights holders' perception related to the use of RBIs by law enforcement. 300 interviews are planned to be carried out in 6 public locations where RBIs are used in 2 different Member States;
- Managing correspondence with prospective interviewees;
- Drafting a single report that introduces the use of RBIs by law enforcement agencies in the EU and presents the findings related to the selected use cases.

The fieldwork activities will be carried out by FRA's contractor **AWO Belgium**, acting as FRA's processor on its behalf for this processing operation. For further information on the data collection, please see the data protection notice.

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

Whose personal data are being processed?

FRA staff ☐

Non-FRA staff ☒

Data subjects are:

1. the interviewees selected by AWO for the research from national law enforcement agencies, technology providers, data protection authorities, national human rights institutions, civil society organisations and rights holders;
2. the participants in the two small-scale surveys on rights holders' perception regarding law enforcement use of RBIs;
3. the individuals who will be observed in the course of the non-participant observations.

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, or in the case of small-scale surveys, demographic information (age bracket, gender)) ☒

Contact details (email address, mobile number). ☒

Education & Training details ☐

Employment details (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 ☐

Goods or services provided ☐

Other (please give details): ☒

- If the interviews with the relevant persons from national law enforcement agencies, technology providers, data protection authorities, national human rights institutions, civil society organisations and rights holders take place online via Teams or Zoom, these tools will process additional personal data such as Device Information, Content and Context from Meetings, Usage Information Regarding Meetings, Unique identification numbers and signatures. For a more detailed overview of the data processed by Microsoft and Zoom, please see the Microsoft Products and Services Data Protection Addendum (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1&year=2024) and Zoom's Privacy Statement and Data Processing Addendum (https://explore.zoom.us/en/privacy/, https://explore.zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf).
- To facilitate the production of the interview summaries, and only with the explicit consent of the interviewees, in-person interviews will be recorded onto a secure device owned by the researcher and remote interviews will be recorded or automatically transcribed (using the MacWhisper). Where consent is provided, interviewees' voice will be processed.
- Information disclosed during the interviews: this is the information that interviewees will disclose to interviewers in the course of interviews.

(b) **Special categories of personal data** (Article 10)
The personal data collected during the responses provided by the interviewees and participants in the focus groups as well as in the non-participant observations and small-scale survey 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 ☐

- Should the interviews take place online, racial or ethnic origin, political opinions and/or religious or philosophical beliefs might be incidentally revealed by the image when participants switch on their cameras.

- Moreover, although there is no intent to process special categories of personal data for the abovementioned purposes, there is a possibility that such personal data may be communicated by interviewees to AWO in the course of interviews.

(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 from Justice, Digital and Migration Unit has access to your personal data as described in Section 5 above.

Recipients **outside** FRA: ☒

Restricted staff at FRA's processor AWO will have access to the personal data, along with the following sub-processors:

- IPSOS – to conduct a small-scale quantitative survey with rights-holders
- Microsoft - providing office, email and cloud services
- Zoom - providing communication services
- *Individual experts – individual experts sub-contracted by AWO to carry out parts of the research process, where needed (e.g., country experts for a particular country);*
- *Keepit – providing backup services to AWO.*

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:

[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.

Although AWO Belgium will store data collected for this processing activity in servers located in Microsoft data centers within the EU by using the Microsoft Advance Data Residency package, the personal data might be accessed by some of the lead researchers on this project from the United Kingdom Microsoft servers, since the UK is where those members of the project team are located. Nevertheless, any transfer of data to the UK falls under the EU-UK adequacy decision adopted by the European Commission on 28 June 2021.

Moreover, as Microsoft and Zoom are US based companies and they are subject to US Surveillance laws, a transfer of limited personal data cannot be completely discarded. Such transfers, if any, fall under the adequacy decision for the EU-US Data Privacy Framework adopted by the European Commission on 10 July 2023.

France
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 relevant European Commission's EU-UK adequacy decision (Article 47) and EU-US Data Privacy Framework.

☐ 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"?

Category of personal data	Category of data subjects	Retention period
Personal and contact details	(Prospective) interviewees and participants in non-participant observations	For AWO: Three months [from the end of the project] For FRA: One year [from the end of the project] – AWO will transfer all the data in this regard to FRA in case it would be needed for the finalisation of the FRA report (to revert back to interviewees).
Information Disclosed During the Interview/Non-Participant Observation/Survey	Interviewees	Will be used to inform the report and kept by AWO for one year from the end of the project, in case further clarifications would be needed for the preparation of the final FRA report.

		The reporting templates (summary records of the conversations) and report, which will not contain any personal data, will be archived by FRA.
Audio recording for in-person and online interviews	Interviewees AWO staff	If audio recording is used the audio files will be deleted by AWO in three months [from the end of the project]. The data will be stored for purposes of drafting the report. FRA will receive these only upon request, for quality management purposes. If FRA receives any such files, they will be deleted at the latest in one year after the end of the contract.
Transcripts	Interviewees AWO staff	If interviews are transcribed the transcripts will be deleted by AWO in three months [from the end of the project]. The data will be stored for purposes of drafting the report. FRA will receive these only upon request, for quality management purposes. If FRA receives any such files, they will be deleted at the latest in one year after the end of the contract.
Small-scale surveys	Survey respondents and subcontractor (IPSOS)	Personal data collected directly from survey respondents will be pseudonymised by IPSOS and provided to AWO and FRA as an anonymised dataset, with no risk or prospect of the re-identification of data subjects. IPSOS will not collect names or other data that could be used to directly identify individual respondents, though it would theoretically be possible be identify the

		individual concerned if their responses to survey questions regarding age bracket sex/gender were matched to metadata concerning the survey and external datasets placing named individuals in the survey location. IPSOS will delete all individual survey responses as soon as the anonymised dataset has been satisfactorily received by FRA and AWO. We expect this validation period to take no longer than one month.

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 ☒

The contractor uses Microsoft - providing office, email and cloud services (Data is stored in France).

Other (please specify): ☒

Cyber Essentials: AWO secured its Cyber Essentials Plus in 2021. All AWO staff are trained to ensure a high level of cyber security. All equipment is deployed with hardened macOS and iOS and secured with SSO and Yubikey multifactor authentication. Our Managed Security Service Provider provides sandboxed patching within a one-week window.

All machines have WithSecure anit-virus software installed. All login attempts into the services used are tracked via our SSO platform. Passwords are stored and maintained using an encrypted password manager. Internet connections are secured through CloudFlare's Zero Trust service.

AWO backups the data stored in its Microsoft cloud instances using a third party service called KeepIt; and data is stored in the Netherlands.

Data protection: AWO has appointed a data protection focal point whose responsibilities include providing advice on data protection requirements for research projects. AWO also has contractual measures in place for cross border data transfers with its suppliers, including Standard Contractual Clauses for transfers to countries recognised as not having an adequate level of data protection. Additionally, AWO staff are trained to ensure a high level of data protection awareness and data protection.

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 Project Data Protection notice: e-mail to privacy@awo.agency

AWO established the following as preferred channels to receive data subjects requests to exercise their rights (DSRs): the mailbox privacy@awo.agency, and the registered address Sq. de Meeûs 35, 1000 Bruxelles, Belgium. All requests are managed in line with our "Data subject request response plan".

Upon receiving a data subject request related to the project at the privacy@awo.agency or via any other mean, AWO staff charged with managing DSRs will reach out to the contact point within the Agency to inform about the request and ask for instructions on how to manage it.

Data subjects can also reach out directly to FRA with an email to: rbiproject@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