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]: *Medical Advisor Booking App*

Reference number: DPR-2022-174
Creation date of this record: 15/12/2022
Last update of this record: 15/12/2022
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
Contact details: HR@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] ☒
The Medical Advisor, contracted by FRA though a public procurement procedure, acts as processor. Specific clauses on confidentiality and protection of personal data are

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?

included in the contract.

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 is to enable staff members to book an appointment with the FRA Medical Advisor directly, without sending requests via email, and for the FRA Medical Advisor to manage his/her appointment schedule. Staff can book an appointment in the Medical Booking App tool on Sharepoint (accessible from the FRA login profile) by selecting a date/time from the list of available appointment slots, selecting the type of appointment from a pre-defined drop-down list of categories (with no indication of medical data) and clicking "submit". Users can view and manage (cancel, change time) their own appointments within the app.

The Medical Advisor and the designated FRA staff can access the data in the back office of the Booking App by viewing a list of appointment slots and booked appointments. From here, the doctor can: access the staff member's contact details to contact them, change the duration of the appointment or cancel the appointment.

The provision of the Medical Advisor service is a measure to support the health and wellbeing of staff, as required by Articles 1e, 59 and 60 of the Staff Regulations and Articles 16, 59, 60 and 91 of the CEOS.

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.)	☐

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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	☒
Contact details: email address, office 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	☐
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	☐
Political opinions	☐
Religious or philosophical beliefs	☐
Trade union membership	☐
Genetic, biometric or data concerning health *(The appointment types are generic and selected from a drop-down list (e.g. annual medical result discussion, general consultation. Staff will be advised not to indicate any personal medical issues in the appointment title or text)*	☒
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 HR staff members responsible for handling medical issues and the relationship with the FRA Medical Advisor have access to the appointment schedule and the list of booked appointments (with staff member's name and FRA email address). The appointment types are generic and selected from a drop-down list (e.g. annual medical result discussion, general consultation). Staff will be advised not to indicate any personal medical issues in the appointment title or text that will be visible to HR.

Designated colleagues in DSF have access as IT system administrators for the purpose of maintenance of the tool.

Recipients **outside** FRA:
(please provide a generic/functional mailbox) ☒

The FRA Medical Advisor (medical.officer@fra.europa.eu) has access to the appointment schedule and the list of booked appointments (with staff member's name and FRA email address). The medical advisor's functional mailbox is accessible only to designated staff under the contract for medical services. The appointment types are generic and selected from a drop-down list (e.g. annual medical result discussion, general consultation). Staff will be advised not to indicate any personal medical issues in the appointment title or text that will be visible to HR.

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 ☐

[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.

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"?

Data on appointments in the preceding calendar year will be deleted manually by FRA staff in Q1 of the subsequent calendar year.

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): the appointment management tool is built using PowerBI apps in the FRA Sharepoint system	☒
FRA network shared drive	☐
Outlook Folder(s)	☐
CRM	☐
Hardcopy file	☐
Cloud (MS 365, see record here)	☒
Servers of external provider	☐
Other (please specify)	

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 HR@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:
Mention the legal basis which justifies the processing and assess that the purposes specified are purposes specified, explicit, legitimate.

[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.