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

NAME OF PROCESSING OPERATION[2]: FRA's Facilities Booking App

Reference number: DPR-2024-219 (to be completed by the DPO)
Creation date of this record: 14/06/2024
Last update of this record:
Version: 01

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 Unit Contact details: it.helpdesk@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?

The Booking app is using Microsoft365 cloud services, which acts as processor. All details including the DPIA on Microsoft 365 are provided in the related data protection documentation. More details can be found in the data protection record available here.

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 linked to the daily internal operations of the Agency in terms of booking meeting rooms and parking spaces as well as registration of external visitors using a Facilities Booking App hosted in FRA's SharePoint intranet site.

In particular, the Booking app collects the following data in terms of its functionalities:

1. FRA meeting rooms: The app lists the meetings scheduled in the user's Exchange calendar displaying the meeting title, date, time. It also stores the name of the user who booked the room. It then displays the available meeting rooms on the particular timeslot and allows the user to select a meeting room and reserve it. It then sends a confirmation email to the users' mailbox.
2. FRA Parking spaces: The app displays the available parking spaces on the specified date and requests the vehicle registration plate. This is needed in order to control that the mentioned vehicle is parked on the booked parking space. This is needed to avoid cases where a staff parks a vehicle without permission and also to provide needed information to traffic warrants when inspecting parking in the area.
3. Facilities Support: This feature allows staff to indicate any facilities needs regarding upcoming meetings such as coffee. It processes the name of the staff responsible for the meeting.
4. FRA visitors: Allows the registration of external visitors and processes the visitor's name, their company name (if applicable), timeframe. Registration is needed in case of an evacuation or similar urgency to know the number of externals present in the building as well as who they are. This is a requirement in terms of physical security to also check that the correct person is permitted to enter the premises.

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

Whose personal data are being processed?

FRA staff ☒

Non-FRA staff ☒

External visitors who are entering the Agency premises for meetings or appointments with Agency staff incl. maintenance of premises.

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 (e.g. postal address, email address, mobile and fax number) ☐

Education & Training details ☐

Employment details (name and type of employer/organisation may be indicated but it is not a mandatory field) ☒

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

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other (please give details):
The vehicles plate number is requested when booking a parking place to print the required certificate and ensure that the parked vehicle is one for which the booking took place. Also, this paper certificate is displayed on the vehicle so that fines are avoided during parking controls.

(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 ☐

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
(please specify which team and Unit-no need to mention specifically the names of colleagues) ☒

Designated staff from the Corporate Services unit have full access to all requests. Remaining FRA users can view the availability of the meeting rooms or parking spaces.

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

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:
The Booking app is based on Microsoft M365 services. These are configured to be provided within the EU data centres and they are under the EU boundary service provisions. It cannot be discarded that service-generated data (SGD – Audit logs) and diagnostic data could be transferred outside EU based on the internal processes of Microsoft to resolve technical issues. However, it is expected that by end of Q3 2024, such data will cease to be transferred when the need arises as part of the finalisation of the EU boundary service.

If transfers take place to the US, they will fall under the adequacy decision for the EU-US Data Privacy Framework adopted by the European Commission on 10 July 2023. If transfers take place to other countries outside the EU, if no adequacy decision exist, SCC and additional safeguards (e.g., end-to-end encryption) will be in place.

Transfer to international organisation(s)

[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.

Yes ☐

No ☒

If yes specify to which organisation:

Legal basis for the data transfer

☒ Transfer on the basis of the European Commission's adequacy decision (Article 47)
Although unlikely, it cannot be discarded that service-generated data (SGD – Audit logs) and diagnostic data could be transferred by MS 365 outside EU or to countries not covered by an adequacy decision, based on the internal processes of Microsoft to resolve technical issues. In such cases, appropriate safeguards are put in place in accordance with the MS enterprise agreement signed between Microsoft and the European Commission.
☒ 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 personI
☐ (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"?

The data is kept for the current year n plus one more year i.e. maximum 24 months. For example, if a registration of parking space was made on 01/01/200n then the data will be deleted on 31/12/200(n+1). If the booking is made on 01/12/200n then it will be kept until 31/12/200(n+1) i.e. 13 months.
This applies to all bookings.
The retention is required for potential follow up cases linked to visitors' presence in internally hosted meetings/events where participation needs to be confirmed, parking tickets etc. Also for security purposes to cover possible cases where security incidents could take place.

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 (MS365)	☒
Servers of external provider	☐

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 it.helpdesk@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