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]: MANAGEMENT OF MISSIONS AND AUTHORISED TRAVELS OF FRA STAFF, INCLUDING MIPS (MISSION PROCESSING SYSTEM), OBT (ONLINE BOOKING TOOL) AND CONTRACTS: TRAVEL AGENCY(S), MISSION ASSISTANCE AND INSURANCE AND PROFESSIONAL CREDIT CARD

Reference number: DPR-2022-153
Creation date of this record: 01/03/2022
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: Head of Corporate Services Unit
Contact details: missions@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	☒

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 data is processed also by a third party (contractor) ☒

As owner of the online tool MiPS, the PMO (PMO-MIPS@ec.europa.eu) acts as joint controller.

To assure the best accountability and efficiency of its mission management the FRA uses external services providers selected based on a procurement procedure. These contractors are the travel agency (transport tickets, hotel reservations, car rental); the insurance company for mission/authorised travel insurance policy (a general "assistance-insurance" and a "mission/authorised travel life-invalidity"), and the company for delivery of the professional credit cards:

- AMEX Global Business Travel (http://privacy.amexgbt.com/gdpr) ,
- CIGNA (https://www.cignahealthbenefits.com/en/privacy),
- AirPlus International Corporate (https://www.airplus.com/editorial-files/common-media/documents/product-privacy-statements/english/airplus-privacy-statement-corporate-card-with-private-liability-europe-en.pdf)

Moreover, car rental companies that can be used for business travel, transport companies (airlines, railways, taxis etc), hotels and/or other accommodation facilities (guest rooms, apart-hotel) and any other organisation that may be called upon to intervene due to the specificity of the mission/ authorised travel act as separate controllers.

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 your personal data by FRA is to organise missions (travels away from the place of employment solely in the interests of the service) and the authorised travels and the payment and/or reimbursement of the related costs, in line with the Mission guide.

In order to ensure the most cost-effective management of the missions of its staff, FRA relies on the European Commission Pay Master Office (PMO),[6] owner and manager of the online tool MiPS - and on external service providers.
The mission management activity is broken down into internal operations carried out by PMO and FRA and other operations carried out by contractors selected following procurement procedures (travel agency services, mission assistance and insurance services and professional credit card services), namely:

- AMEX Global Business Travel (http://privacy.amexgbt.com/gdpr)
- CIGNA (https://www.cignahealthbenefits.com/en/privacy)

[6] Service Level Agreement concluded with the PMO (2020). Decision delegating Appointing Authority and Authority Authorised to Conclude Contracts of Employment Powers. Ref. Ares(2020) 7458287 – 09/12/2020.

- AirPlus International Corporate (https://www.airplus.com/editorial-files/common-media/documents/product-privacy-statements/english/airplus-privacy-statement-corporate-card-with-private-liability-europe-en.pdf)

The process consists of:

- Creation of the mission order by the person carrying out the mission in MIPS, or a delegated assistant, and validation in accordance with the visa chain applicable to the FRA (confirmation and signature of the actors of the workflow and approval of the authorizing officer)

- Reservation and purchase of transport tickets (plane, train, etc.), reservation of the accommodation (hotel, etc.), if necessary and possible reservation of the rental car, by the person carrying out the trip or by person(s) to whom a delegation has been given or through the FRA's approved travel agency.

- Possible use of the credit card (mixed-use, professional and / or personal credit card) made available to the mission performers or the person making the trip to settle any expenses incurred on mission. The person carrying out the trip is covered by an insurance and assistance contract signed by the Commission on FRA's behalf.

- Establishment of the declaration of expenses, signature by the competent authorising officer and transmission to the PMO via MIPS for liquidation and payment of mission expenses.

- Introduction of the declaration of expenses by the person carrying out the mission, or a delegated assistant, within 3 months from the return date from the working assignment outside the normal working place.

- Supporting documents relating to the declaration of mission expenses must be obligatorily scanned and downloaded in MIPS.

- Verification and signature of the actors of the workflow and approval of the authorising officer.

- Electronic sending of the file, via the MIPS application, to the PMO for calculation.

- Calculation of the mission by the PMO.

- During the liquidation phase during which the PMO reviews the supporting electronic documents, the person carrying out a "mission" must keep the original paper documents to provide them to the PMO at the request of the latter for various reasons (electronic copy not readable, random control, ...).

- Ex-ante control by the PMO. An alert message informs each officer in working travel that he / she has been selected as part of this check and is requested to submit to PMO2 the original supporting documentation for this assignment. The documents sent to the PMO will be kept and archived by the PMO. If the file is non-compliant, the interested officer is contacted individually by the PMO 2.

- Sending of a Payment Request by MIPS to FRA's ABAC.

- Verification and payment by FRA.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

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

Whose personal data are being processed?

FRA staff ☒
All FRA staff: temporary and contract staff, seconded national experts, trainees.

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

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 (civil title, name, surname, date of birth, login, personnel number, per id number) ☒ ,

Contact details (business telephone number, business email address) ☒

Education & Training details ☐

Employment details (assignment, place of assignment, office address) ☒

Financial details (bank account number) ☒

Family, lifestyle and social circumstances ☐

Goods or services provided ☐

Other (please give details):
- Login, personnel number

- Location(s) of mission and transit, the scheduled departure and return time to the place of employment, the means of transport used, the name of the hotel, the invoice(s), the start and end time of professional commitments at the mission locations, the budget line to which the mission will be charged, the MIPS mission number and the confirmation number generated at time of signature for the approval of the authorizing officer.

Other optional data may be voluntarily provided by the person going on mission or carrying out the authorised travel in order to receive a more personalized service, in particular through their traveller profile (travel agency management tool containing information necessary and/or useful for processing orders and formatted and/or structured by them): mobile phone number, nationality, place of issue and expiry date of the passport, passport number, credit card, contact details of the person who can be called upon to make reservations for the project manager and any preferences in terms of travel conditions, seat and meal.

(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 ☒

Data concerning a health problem affecting business travel, the indication of a problem may appear in MiPS in the cases described as follows:
In the event of authorisation to adopt a certain mode of travel and/or a certain means of transport (e.g., traveling by plane in business class) in derogation from the common rules, a comment must be added to the file on the basis of a certificate from the institution's medical service which must be uploaded in MiPS. The medical certificate must indicate the mode of travel/ means of transport recommended and the date of validity without reporting the specific medical reason which justifies the exemption.
If the person making the trip requires an accompanying person for medical reasons (e.g., in the case of a visually impaired person), the mission expenses relating to his/her accompanying person are recorded in MiPS in order to be reimbursed to 100%.
Any vaccination costs must be registered in MiPS in order to be reimbursed at 100%.

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) ☒

A restricted number of FRA staff members, who are internally in charge of the missions, can access the personal data, i.e., the Finance, HR and IT within the Corporate Services Unit, the staff to whom mission performers gave their delegation to act on their behalf, the Authorising Officers and the Director of the Agency.
Moreover, in order to process the payments to the travel agency, financial actors may have access to a limited number of data uploaded with the commitment/payment documentation in the eWorkflow application in DMS.

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

- Within the EU organization
The European Commission's PMO staff in charge of missions and authorized travel, but also certain members of other units of the PMO and the EC who ensure the monitoring and maintenance of computer systems, the handling of legal issues and internal control. EEAS (security reason, for every mission out of the EU); HR (security issues, complaint handling); SG (questions on access to documents); SJ (legal issues); Control and investigation bodies: IAS, IAC, OLAF, IDOC, European Ombudsman, EDPS, CJEU

- Outside the EU organisation
Service providers involved in the mission management, namely: the travel agency, the insurance company, the credit card company, the companies that organize travels, hotels, transport (plane, train, etc.), car rental companies and any other service providers potentially used in the field of transport and accommodation.

7) Transfers to third countries or international organisations (Article 31.1 (e))[7]

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 ☒

The travel agency providing the service (AMEX-GBT) may be required to transmit data concerning the travel agent / authorised traveller to a country outside the EU. Personal data is transferred to the US (where the main operational data centres of the travel agency are situated) for business operation purposes. Furthermore, as travel is inherently global, transfers of personal data outside of EU and EEA could occur, depending on the travel location. In order to organise travel, booking information is shared with airlines, hotels and other travel suppliers around the world.

[7] **Processo**r 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.

Transfers of the travel agency within its 'corporate family' are based on Art. 48(2)(d) of the Regulation (EU) 2018/1725 - Binding Corporate Rules (BCRs). Transfers are also based on Article 50(1)(b) of the Regulation (EU) 2018/1725, since 'the transfer is necessary for the performance of a contract between the data subject and the controller.

No ☐

If yes, specify to which country:

US

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.

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"?

The data collected for mission management are kept for a maximum of 7 years from the moment of its collection. Once the legal deadline has expired, the file is deleted.

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) ☒
(incl. storage of commitment/payment documentation in the eWorkflow application in DMS)

FRA network shared drive ☐

Outlook Folder(s) ☒
Exchange of emails with the travel agency/mission insurance requests, designated staff members from the relevant project team, etc.

CRM ☐

Hardcopy file ☐

Cloud (give details, e.g. cloud provider) ☐

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 missions@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