

Management of missions and authorized 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

The European Union Agency for Fundamental Rights (FRA or Agency) processes the personal data of a natural person in compliance with Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

This data protection notice explains FRA's policies and practices regarding its collection and use of your personal data, and sets forth your privacy rights. We recognise that information privacy is an ongoing responsibility, and we will update this notice where necessary.

1. [Why do we process personal data?](#)
2. [What kind of personal data is collected and further processed?](#)
3. [How is your personal data processed?](#)
4. [Who is responsible for processing your personal data?](#)
5. [Which is the legal basis for this processing operation?](#)
6. [Who can see your data?](#)
7. [Do we share your data with other organisations?](#)
8. [Do we intend to transfer your personal data to Third Countries/International Organizations](#)
9. [When will we start the processing operation?](#)
10. [How long do we keep your data?](#)
11. [How can you control your data?](#)
 - 11.1. [The value of your consent](#)
 - 11.2. [Your data protection rights](#)
12. [What security measure are taken to safeguard your personal data?](#)
13. [What can you do in the event of a problem?](#)
14. [How do we update our data protection notice?](#)

1. Why do we process personal data?

The purpose of the processing of your personal data¹ by FRA is to organise missions (travels away from the place of employment solely in the interests of the service) and 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)², 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).

2. What kind of personal data is collected and further processed?

In order to carry out this processing activity, the Agency (via MiPS) will collect only the following personal data necessary for the processing operation described above.

(a) General personal data:

Civil title, surname, first name, date of birth, login, personnel number, per id number, assignment, place of assignment, office address, business telephone number, business email address, 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 bank account number of the person going on mission or carrying out the authorised travel, 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 traveler 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:

In MiPS, data relating to the state of health of the staff member on mission may be processed. Data on a health problem affecting work-related travel may appear in MiPS if it is authorised to make a certain

¹ Categories of data subjects: All FRA staff, including temporary and contract staff, seconded national experts and trainees.

² 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.

travel arrangement and/or to use a certain means of transport (e.g. travel by 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 method of travel/recommended means of transport and the date of validity, without however indicating the specific medical reason justifying the derogation. If the person travelling 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 at the rate of 100 %. Any costs of vaccinations must be recorded in MiPS in order to be reimbursed at the rate of 100 %.

3. How is your personal data processed?

Information you provide us

You provide us with your personal data following your employment contract, which is encoded in Sysper (HR online tool managed by the European Commission). The relevant information is transferred to the MiPS (owned by the PMO) for the management of missions. This includes contact details, bank account number as well as the reporting officer who will be responsible for the approval of the mission request.

Moreover, you also provide your personal data and information related to your mission when introducing in MiPS your mission request, as well as your mission claim.

FRA provides the travel agency American Express Global Business Travel (GBT) with your first name, last name, title, user business email and the name of your travel arranger's (if applicable) in order GBT to create your traveller profile in its online booking tool.

Your date of birth have to be provided by you to GBT for your online and offline bookings. (For further information please refer to AMEX GBT's privacy statement: <http://privacy.amexgbt.com/gdpr>). This is necessary to comply with the national and international laws applicable to travels and air carriers.

GBT collects information about you in connection with your registration, use, purchase or inquiries about its services. It use your information to provide its services, process payments, operate its websites and applications, market products and services, create business insights and comply with law. GBT has a contract with FRA and shares your information with FRA, as well as with its affiliates, travel suppliers and vendors to book travel arrangements and provide its services. GBT do not sell or share information with third parties so that they can independently market their own products or services directly to you. For further information, we encourage you to read the latest version of the respective Privacy Statement (link provided under Section 4 below).

4. Who is responsible for processing your personal data?

The Agency is the legal entity responsible for the processing of your personal data and determines the objective of this processing activity. The Head of Corporate Services is responsible for this processing operation.

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

The following services providers act as processors of the Agency on the basis of a procurement contract:

- Travel Agency services (transport tickets, hotel reservations/car rental, etc.):

AMEX Global Business Travel (privacy statement: <http://privacy.amexgbt.com/gdpr>)

- Professional credit card services:

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

- Insurance company (general “assistance-insurance” and “mission/authorized travel life-invalidity”):

CIGNA (privacy statement: <https://www.cignahealthbenefits.com/en/privacy>)

Moreover, car rental companies that can be used by the Agency or the contractors 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 act as separate controllers for the personal data they process. To learn more on how these entities would process your data, we encourage you to read their respective privacy policies.

5. Which is the legal basis for this processing operation?

Missions (travels away from the place of employment solely in the interests of the service) and authorised travels are necessary for the management and functioning of the Agency. In particular, the legal basis for the processing can be found in Article 24.2 of [Regulation \(EC\) No. 168/2007](#) establishing the European Union Agency for Fundamental Rights (as amended by [Regulation \(EU\) 2022/555](#)), Articles 11, 12 and 13

of Annex VII of the Staff Regulations and Article 22 CEOS³ and [EB Decision 2018/01 adopting by analogy the Commission's general implementing provisions on mission expenses and authorized travel and the Mission's guide](#).

The legal basis for processing of personal data related to missions by the PMO can also be found in Commission Decision of 6 November 2002 establishing the Office for the Administration and Payment of Individual Entitlements C (2002) 4367.

Therefore, the processing is lawful under Article 5.1.(a) and 5.1.(b) of the [Regulation \(EU\) No 2018/1725](#).

The processing of the special categories of personal data mentioned under section 2(b) above is lawful as the conditions of Article 10(2)(b) of Regulation 2018/1725 are met, namely, the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law insofar as it is authorised by Union law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

6. Who can see your data?

Recipients within FRA:

-Designated FRA staff members

More specifically, a restricted number of FRA staff members, who are internally in charge of the missions, can access the personal data, i.e. the Finance and Contracting, 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:

-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

³ Staff Regulations of Officials and the Conditions of Employment of Other Servants (Regulation 1962/31 of 1 January 1962 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community).

-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.

FRA contractors are bound by a specific contractual clause for any processing operations of your data on behalf of FRA, and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU Member States ('GDPR' Regulation (EU) 2016/679).

7. Do we share your data with other organisations?

No. In case that we need to share your data with third parties, you will be notified to whom your personal data has been shared with.

8. Do we intend to transfer your personal data to Third Countries/International Organizations

The travel agency (AMEX-GBT) providing the service may be required to transmit data concerning the travel agent/authorized traveller to a country outside the EU. Personal data is transferred to the US (where the main operational 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 organize travel, booking information is shared with airlines, hotels and other travel suppliers around the world.

These transfers are based on Article 48 of [Regulation \(EU\) No 2018/1725](#) (appropriate safeguards). Such appropriate safeguards shall consist of binding corporate rules, codes of conduct or certification mechanisms pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679. 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'.

9. When we will start the processing operation?

We will start the processing operation the moment you enter a mission request.

10. How long do we keep your data?

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

11. How can you control your data?

Under Regulation 2018/1725, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information. You are not required to pay any charges for exercising your rights except in cases where the requests are manifestly unfounded or excessive, in particular because of their repetitive character.

We will reply to your request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

You can exercise your rights described below by sending an email request to missions@fra.europa.eu.

11.1. The value of your consent

Since the participation of FRA staff members in missions and authorised travel is mandatory in accordance with the Staff Regulations and CEOS, you are not required to provide your consent. .

Nevertheless, you have consented to provide your personal data to PMO.2, for the present processing operation.

11.2. Your data protection rights

a. Can you access your data?

You have the right to receive information on whether we process your personal data or not, the purposes of the processing, the categories of personal data concerned, any recipients to whom the personal data have been disclosed and their storage period. Furthermore, you can have access to such data, as well as obtain copies of your data undergoing processing.

b. Can you modify your data?

You have the right to ask us to rectify your data you think is inaccurate or incomplete at any time.

c. Can you restrict us from processing your data?

You have the right to restrict the processing of your personal data. If you do, we can no longer process them, but we can still store them. In some exceptional cases, we will still be able to use them (e.g. with your consent or for legal claims). You have this right in a few different situations: when you contest the accuracy of your personal data, when the Agency no longer needs the data for completing its tasks, when the processing activity is unlawful, and finally, when you have exercised your right to object.

d. Can you delete your data?

You have the right to ask us to delete your data when the personal data are no longer necessary for the purposes for which they were collected, when you have withdrawn your consent or when the processing

activity is unlawful. In certain occasions we will have to erase your data in order to comply with a legal obligation to which we are subject.

We will notify to each recipient to whom your personal data have been disclosed of any rectification or erasure of personal data or restriction of processing carried out in accordance with the above rights unless this proves impossible or involves disproportionate effort from our side.

e. Are you entitled to data portability?

Data portability is a right guaranteed under Regulation 1725/2018 and consists in the right to have your personal data transmitted to you or directly to another controller of your choice.

In this case, this does not apply for two reasons: I) in order for this right to be guaranteed, the processing should be based on automated means, however we do not base our processing on any automated means; II) this processing operation is carried out in the public interest, which is an exception to the right to data portability in the Regulation.

f. Do you have the right to object?

When the legal base of the processing is “*necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body*” which is the case in most of our processing operations, you have the right to object to the processing. In case you object, we have to stop the processing of your personal data, unless we demonstrate a compelling reason that can override your objection.

g. Do we do automated decision making, including profiling?

Your personal data will not be used for an automated decision-making including profiling.

12. What security measures are taken to safeguard your personal data?

The Agency has several security controls in place to protect your personal data from unauthorised access, use or disclosure. We keep your data stored on our internal servers with limited access to a specified audience only.

In order to protect your personal data, the FRA and the PMO have put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

External contractors are bound by a specific contractual clause for any processing operations of the data subjects’ data on behalf of the FRA, and by the confidentiality obligations deriving from the transposition of the General Data Protection Regulation in the EU Member States (‘GDPR’ Regulation (EU) 2016/679).

The data inserted in the MIPS computer application that underpins the "mission" process are recorded on protected databases. The storage units are housed in the Commission Data Centre (DG DIGIT A.3). Periodical backup of all the data is performed. Electronic files will be destroyed by the DIGIT only on express request from the PMO.

Any data processor used also have appropriate technical and organisational measures in place.

Please refer to the latest version of the relevant [Commission's privacy statement](#).

13. What can you do in the event of a problem?

a) The first step is to notify the Agency by sending an email to missions@fra.europa.eu and ask us to take action.

b) The second step, if you obtain no reply from us or if you are not satisfied with it, contact our Data Protection Officer (DPO) at dpo@fra.europa.eu.

c) At any time you can lodge a complaint with the EDPS at <http://www.edps.europa.eu>, who will examine your request and adopt the necessary measures.

14. How do we update our data protection notice?

We keep our data protection notice under regular review to make sure it is up to date and accurate.

END OF DOCUMENT