

Specific privacy statement

This statement applies to the **administration of missions and authorised travel**, and explains how the personal data of Commission staff are used and how confidentiality is ensured, according to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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/EC¹. It also contains the legal information required under Articles 15 and 16 of this Regulation.

Why do we collect information about you?

In the course of managing your missions/authorised travel, the Commission must process some of your personal data. These data, together with any other information you may provide if you consider it appropriate to do so for a specific purpose, will be used by the travel agency, transport firms, hotels, car hire companies, credit card companies, insurance companies and any other entity which the Commission (or you) may come into contact with during the organisation of your missions/authorised travel.

We use your details to arrange travel, accommodation and, where necessary, assistance for staff on mission/authorised travel, and to pay the resulting expenses.

The processing of the data is based on Article 71 of the Staff Regulations, Articles 11 to 13 of Annex VII to the Staff Regulations, and Commission Decision C(2017) 5323 final of 27/09/2017 on the general provisions for implementing Articles 11, 12 and 13 of Annex VII to the Staff Regulations of Officials (mission expenses) and on authorised travel

https://myintracomm.ec.europa.eu/hr_admin/en/missions/Documents/guide-to-missions-and-authorised-travel-en.pdf).

To obtain the best value for money, the Commission uses outside service providers who process some of the data on behalf of the Commission or for their own purposes. These are:

- the travel agency responsible for issuing tickets and booking hotels;
- the credit-card-issuing financial institution or bank;
- car hire companies that may be used when on mission;
- transport companies;
- insurance companies;
- hotels and other assimilated accommodation providers.

The outside companies used by the Commission to organise your missions/authorised travel are required to handle these data and certain other information. In their handling of personal data, these firms must apply the rules on privacy set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016².

¹ OJ L 295, 21.11.2018, pp. 39–98.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1) .

What information is collected?

The information required is as follows:

- Member of staff on mission/authorised travel: Title, surname, first name, personnel number, post (DG/Directorate/Unit), place of employment, office address, office telephone number, office e-mail address;
- Information concerning the mission/authorised travel: Place(s) of mission/authorised travel and transit, expected times of departure and return to the place of employment, means of transport used, name of hotel, bill(s), start and end times of professional commitments at the place of mission, bank account number, budget heading to which the mission/authorised travel will be charged, MIPS mission/authorised travel number and confirmation number generated at the time of signature of the mission order/travel authorisation for approval by the authorising officer.
- Other details may be provided in certain circumstances by persons going on mission/authorised travel, if they wish to receive more personalised service, mainly through their traveller profile (*a travel agencies' tool englobing information which is necessary and/or useful for the management of commands; this information is formatted and/or structured by the agencies themselves*): a mobile telephone number; their nationality, the date and place of issue of their passport and its expiry date; the passport and credit card number; the details of a person who may be asked to make reservations on their behalf; any preferences as regards the conditions of the trip which they might wish to be automatically taken into consideration, seat + meal.

To ensure that the quality of the service provided by the agency is constantly monitored, any e-mail correspondence addressed to persons going on mission/authorised travel is copied to the Missions Department.

To whom is your information disclosed?

- Your information is passed on to your management, the authorising officer, the administrative staff dealing with it, the settlements officers, the on-line support team, the service providers referred to above and other persons where required.
The agency receives the basic information required for it to fulfil its contract. This information is destroyed at the end of the contract. Other information may be transmitted directly by the official to the agency. In the course of its work, the agency may be required to send your information to a country outside the EU.
- EEAS (security reasons): to add automatically staff members to the lists of evacuation while on mission/authorised travel in a delegation;
- HR DS – Security Directorate ;
- The control and investigation bodies:
 - IAS, Court of Auditors, IAC
 - OLAF, IDOC
 - European Ombudsman, EDPS.

How can you obtain access to information concerning you, check its accuracy and, if necessary, correct it?

As a data subject you may at any time exercise your rights under Articles 14 to 24 of the Regulation by contacting the data controller. Furthermore, if you wish to obtain specific details pertaining to a mission/authorised travel you can contact the PMO officer responsible for handling the mission/authorised travel indicated on the mission statement or the functional mailbox PMO-MISSIONS@ec.europa.eu.

You can also consult personal data held on you by the travel agency, the bank or financial institution which issued your credit card and the insurance company:

Link to AirPlus International Corporate privacy statement:

<https://www.bcc-corporate.be/bundles/webcreator/Themes/bcc-corporate/pdf/bcc-privacy-statement-en.pdf?v4.0.6>

Link to AMEX Global Business Travel privacy statement: <http://privacy.amexgbt.com/gdpr>

Link to CIGNA privacy statement: <https://www.cignahealthbenefits.com/en/privacy>.

How long do we keep your information?

All mission/authorised travel expenses are digitised in MIPS, e-domec compliant system.

In agreement with DG BUDG (see Ares note Ares(2013)2548764):

- the retention period for the digitised documents is 7 years;
- the retention period for originals kept by the staff member having gone on mission/authorised travel is the date of the payment (unless there is a disagreement);
- the retention period for originals that have been part of a conformity check sampling (recall of the original documents kept by the staff member having gone on mission/authorised travel) is 7 years.

What security measures are taken to prevent any abuse of your information or access to it by unauthorised persons?

Data are stored in the Commission's Data Centre in Luxembourg and are therefore protected by a number of measures introduced by the Directorate-General for Informatics to protect the integrity and confidentiality of the Commission's electronic products.

Access to personal data is protected by means of access rights which are strictly limited in accordance with the "need to know" principle and are based on the duties entrusted to access holders.

Overall responsibility for implementing the rules on data protection and granting access rights is assumed by the "controller". He is the person who, in both organisational and practical terms, decides who in the various domains has what right of access to which part of the system. The paper archives are stored in specially designated premises.

Contact points if you have questions or complaints about personal data processing

Controller: The Head of Unit PMO.2

HR's Data Protection Coordinator: HR-DATA-PROTECTION-COORDINATOR@ec.europa.eu

The Commission's Data Protection Officer: DATA-PROTECTION-OFFICER@ec.europa.eu

You can also contact the European Data Protection Supervisor: edps@edps.europa.eu