FUSION FOR ENERGY

idm@F4E UID / VERSION
26JYLN / 2.3

VERSION CREATED ON / STATUS
29 October 2026 / Approved

EXTERNAL REFERENCE

NO MARKING

F4E Document

Record of Processing of Personal Data for Mission Management

Record of Processing of Data Protection for Mission Management in line with Data Protection Regulation 2018 1725.

Approval Process			
	Name	*Action*	*Affiliation*
Author	● **F4E.DI.PC.FN.EP**	**29 October 2026:signed**	**PCSCF**
Co-Authors	● **F4E.DI.PC.FN.FI**	**29 October 2026:signed**	**PCSCF**
Reviewers	● **F4E.DI.PC.LS**	**29 October 2026:recommended**	**PCSCF**
Approver	● **F4E.DI.PC.FN**	**29 October 2026:approved**	**PCSCF**
Read Access	**LG: DP Access Rights - Add, AD: IDM F4E.DI.CL Commercial Department, AD: IDM F4E.DI.CL.HD Head of Commercial Department, AD: BO CL-00-00-00 Commercial Department, AD: BO CL-00-00-HD Head of Commercial Department, AD: IDM_F4E_EXT_EXTENDED, AD: IDM_F4E_STAFF, AD: IDM_F4E_EXT_STANDARD, AD: IDM F4E.DI.C...**		

Original Document MD5#: 297F0507A85AF28C27DAAC7DD4F2A808

** Performed by ** Delegated Reviewer*
For Data Protection the names of the actors are omitted and can be consulted in IDM
Printed copies are not controlled. Confirm version status through the F4E document management system (idm@F4E)

Printed copies are not controlled. Confirm version status through the F4E document management system (idm@F4E)
Generated on #CoverPageDate#

Change Log			
Record of Processing of Personal Data for Mission Management (26JYLN)			
Version	***Latest Status***	***Issue Date***	***Description of Change***
v1.0	Approved	03 October 2013	
v1.1	Approved	07 October 2013	All Annexes included
v2.0	Approved	21 May 2020	Record of Processing of Personal Data for Mission Management in line with Data Protection Regulation 2018 1725. Comments received at working level from FIN, LSU/DPO, DMO, ICT have been incorporated.
v2.1	Approved	22 October 2025	The following changes have been implemented in this new version: - Updated department name and DP functional mailbox. - Improved formatting.
v2.2	Approved	26 November 2025	The following changes have been implemented in this new version: - The travel agency name has been updated. - Updated the name of the software application used for the organisation of the mission and the declaration of costs and the corresponding link to the Privacy Notice. - Improved formatting.
v2.3	Approved	29 October 2026	Change name of travel agency and include SUMMA

RECORD
Of data processing activity regarding the management of missions and reimbursement of mission costs, According to Article 31 Regulation 2018/1725[1]

NAME of data processing:
Mission management and reimbursement of costs related to missions.

Last update: October 2026

1) Controller(s) of data processing operation (Article 31.1(a))
Controller: Fusion for Energy (F4E) Project Control, Supply Chain & Finance Department representative: (HoD) PCSCF-Department-Controller@f4e.europa.eu Data Protection Officer (DPO): DataProtectionOfficer@f4e.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))	
The data is processed by F4E (responsible unit) itself	☒
The data is processed by a third party (e.g. contractor) (Art. 29 – Processor) :	☒

Contact point at external third party (e.g. Privacy/Data Protection Officer):

- PMO dedicated staff in charge of the calculation of reimbursements of travel missions. Contact: PMO-MISSIONS@ec.europa.eu.
  When data is transferred to the PMO, the processing carried out by this third-party processor is covered by their data protection policy and respective Privacy Notice. The Protection of Personal Data throughout this transfer is also described in the SLA between the PMO and F4E.
- AMERICAN EXPRESS – GLOBAL BUSINESS TRAVEL BV is the travel service provider under framework contract PMO-02-PR-2017-073, signed with PMO and in force since December 2018. F4E may obtain travel booking services through its SLA with PMO and the Memorandum of Understanding signed in May 2026.
- For the execution of financial transactions, (personal) data is processed through the Accrual Based Accounting System (ABAC) and SUMMA, which are systems run by DG Budget (budg-data-protection-coordinator@ec.europa.eu). The responsibilities of both F4E and DG Budget regarding Personal Data Protection are described in the Service Level Agreement and are partly laid out in section 3B below.

[1] Regulation 2018/1725 of 23 October 2018 "on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data". O.J 21.11.2018, L295/39.

3) Purpose and Description of the processing (Article 31.1(b))

Why is the personal data being processed? Specify the underlying reason for the processing and what you intend to achieve. Describe, summarise the substance of the processing.

When you (later on) intend to further process the data for another purpose, please inform the Data Subject in advance.

3A) Purpose of the Processing

Whenever Fusion for Energy staff members (hereafter "staff" or "staff members") are required to travel away from their place of employment for the needs of the service (eg. for congresses, conferences, seminars, workshops, meetings and other working appointments), this constitutes a mission.

Processing of personal data (eg. travel orders, processing visa applications, statement of expenses) occurs within the context of managing missions of Fusion for Energy staff members. The purpose is to make the appropriate arrangements for missions and to process expense claims related to missions.

3B) Description

Personal data from staff members are collected and processed through the corresponding travel orders submitted to the Mission Management system (MIPS+) for the participation of staff members in congresses, conferences, seminars, workshops, meetings and other working appointments, and through statements of expenses (cost declarations) for the reimbursement of eligible costs incurred during their mission.

Data is collected and processed only for the purposes described in the paragraph above, in accordance with PM-148 Reimbursement of Mission Expenses and within the procedure for missions as provided in the Guide to missions and authorized travel (255DGR). The MIPS+ software application is used for the organisation of the mission and the declaration of costs. Data is transferred to the PMO who executes the calculation of the settlement and is responsible for processing and checking mission expenses.

The Name of Staff on mission and the date and location of the mission is accessible to all staff through the 'F4E Staff Whereabouts' Reports on F4E's Integrated Reporting System. This Information will be accessible to all staff for the maximum of one month from the start of the mission.

For the execution of financial transactions, (personal) data is processed through the Accrual Based Accounting System (ABAC) and SUMMA, which are systems run by DG Budget.
For the provision of accounting and treasury services, DG Budget acts as the processor and F4E as the controller. For the processing of personal data with the purpose of registering in the Commission Financial Systems ABAC and SUMMA the necessary Legal Entities and Bank Account Files, DG Budget and F4E act as joint controllers.
Requests made by Data Subjects should first be directed to and dealt with by F4E. The responsibilities of both F4E and DG Budget regarding Personal Data Protection are further described in the Service Level Agreement.
The Data Protection Record and Privacy Notice held by DG Budget can be found here.

4) Lawfulness of the processing (Article 5(a)–(d)):

Mention the legal bases which justifies the processing

Processing necessary for:

(a) performance of tasks in the public interest attributed by EU legislation (including management and functioning of F4E) ☒

- Council Decision of 27 March 2007 "establishing the European Joint Undertaking for ITER and the Development of Fusion Energy and conferring advantages upon it" - 2007/198/Euratom, as last amended by Council Decision of 10 February 2015 (2015/224 Euratom), O.J. L 37, 13.2.2015, p.8, in particular Article 6 thereof;
- Statutes annexed to the Council Decision (Euratom) No 198/2007 (in its most recent amended version) "establishing the European Joint Undertaking for ITER and the Development of Fusion Energy and conferring advantages upon it", in particular Article 10 thereof;
- Council Regulation (EEC, Euratom, ECSC) No 259/68 (OJ L 56, 4.3.1968, p. 1) laying down the Staff Regulations of Officials (hereinafter "Staff Regulations") and the Conditions of Employment of Other Servants (hereinafter "CEOS") of the European Economic Community and the European Atomic Energy Community as subsequently amended, specifically Article 71;
- Commission Decision of 18.11.2008 on the General Implementing Provisions adopting the Guide to Missions for officials and other servants of the European Commission (C(2008) 6215 final)

(b) compliance with a *specific* legal obligation for F4E to process personal data ☐

(c) necessary for the performance of a contract with the data subject or to prepare such a contract ☐

(d) Data subject has given consent (ex ante, freely given, specific, informed and unambiguous consent) ☐

5) Description of the data subjects (Article 31.1(c))

Whose personal data is being processed?

Data subjects are natural persons who are Fusion for Energy staff members who are taking part in congresses, conferences, seminars, workshops, meetings, or in other working appointments outside their place of employment.

6) Categories of personal data processed (Article 31.1(c))

Please give details in relation to (a) and (b). In case data categories differ between different categories of data subjects, please explain as well.

(a) **General personal data:**

Personal data shall mean any information relating to an identified (directly or indirectly) or identifiable natural person. This information shall only be processed in the exercise of activities which fall within the mission management process, and can include:

- Name and surname
- F4E email address
- Department/Unit and personal number
- LEF and BAF
- Mission destination and details
- Declaration of conflict of interest regarding gifts or payments offered
- Hotel invoices, taxi receipts, parking receipts, telephone and/or internet bills, transport tickets (flight or boat boarding passes, train tickets if nominative, car hiring invoices) and any other proof of payment necessary for the reimbursement of any expenses in which the staff member may have incurred;
- Leave and leave destination;
- Signature and name of the Authorising Officer;
- Name and Phone Number of the Liquidator.
- Any other personal data provided in the MIPS+ application.

Only relevant and necessary data for the mission management and the reimbursement of costs may be collected and further processed.
The staff list (name, surname and F4E email address) must be shared with AMEX/GBT to create staff profiles in advance, ensuring access to mission booking services when needed and enabling staff to go on mission, as described in the FWC.
Any additional personal data (such as a telephone number or passport number) required to book travel services will be provided directly by mission performers through their personal area in the AMEX/GBT online booking tool.
The Personal Data listed above that are also further processed in ABAC and SUMMA can be found in the Data Protection Record held by DG Budget.

(b) **Sensitive personal data** (Article 10)
No sensitive personal data is processed.

7) Recipient(s) of the data (Article 31.1 (d))

Recipients are all people to whom the personal data is disclosed ("need to know principle"). Not necessary to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).

The following recipients may have access to the personal data processed:

- The hierarchical superior to whom mission requests are transmitted electronically for approval;
- The travel agency contracted to work with F4E;
- PMO dedicated staff, according to the Service Level Agreement concerning the collaboration of The European Joint Undertaking for ITER and the development of Fusion Energy (F4E) with the Office for Administration and Payment of Individual Entitlements (PMO);
- F4E Finance Unit;
- IDM Manager, if necessary for support; The supporting ICT officers (for provision of technical assistance to the MIPS+ software application);
- For Personal Data further processed through ABAC and SUMMA:

    - All F4E staff on the financial circuit have access to the data on ABAC and SUMMA. The extent of this access depends on the access rights which are set on a strict need to know basis. A list of specific access rights can be obtained by contacting F4E Local Authorisation Manager (LAM) by addressing pcscf-department-controller@f4e.europa.eu;
    - On the side of DG Budget the relevant recipients are described in DG Budget's Data Protection record.

- For personal data published in the IRS reports (as describe in Section 3B), all staff have access to this data.

Also, if appropriate and necessary for monitoring or inspection tasks, access may be given to: F4E Director, Head of Admin., DPO and Anti-Fraud & Ethics Officer, Head or responsible officer of LSU, IAC, IDOC.

8) Transfers to third countries or International Organizations (Article 31.1 (e))

If the personal data is transferred outside the EU, this needs to be specifically mentioned, since it increases the risks of the processing operation (Article 47 ff.).

Data is transferred to third countries or International Organizations recipients:

Yes ..... ☐

No ..... ☒

If yes, specify to which country/IO:

If yes, specify under which safeguards and add reference :

Adequacy Decision (from the Commission)..... ☐

Memorandum of Understanding between public authorities/bodies..... ☐

Standard Data Protection Clauses (from the EDPS/Comission)..... ☐

Binding Corporate Rules ..... ☐

Others, e.g. contractual/agreements (subject to authorisation by the EDPS) ..... ☐

Reference*: N/A*

9) Technical and organisational security measures (Articles 31.1(g) and 33)

Please specify where the data is stored (paperwise and/or electronically) during and after the processing. Specify how it is protected ensuring "confidentiality, integrity and availability". State in particular the "level of security ensured, appropriate to the risk".

- Data is submitted to, and stored electronically in MIPS+ as part of the travel orders and statements of expenses. For the MIPS+ software application specific measures were adopted to prevent any unauthorized operation according to the related System Security Plan. Access to mission files is granted only to the missioner, the relevant Authorishing Officer, Delegations, and to staff of the Finance Unit covering specific roles in the mission management processes. Documents supporting the settlement of the missions are furthermore stored in restricted access folders of F4E's IT Storage system.
- For Personal Data required to carry out financial transactions, these data are furthermore processed/stored on DG Budget's ABAC and SUMMA Systems.

When data is transferred to the PMO, the processing carried out by this third-party processor is covered by their data protection policy and respective Privacy Notice. The Protection of Personal Data throughout this transfer is also described in the SLA between the PMO and F4E.

When data is transferred to AMERICAN EXPRESS - GLOBAL BUSINESS TRAVEL BV, the processing carried out by this third-party processor is conducted in accordance with EU Regulation 2018/1725 (EUDPR), as provided for in Article II.9 of framework contract PMO-02-PR-2017-073.

ABAC and SUMMA are secured online systems run by DG Budget. The specific security measures can be found in their Data Protection Record.

Outcome of the consultation with ICT and DMO:
Outcome above after consultation with ICT and DMO.

10) Retention time (Article 4(e))

How long is it necessary to retain the data and what is the justification for this retention period? If appropriate, differentiate between the categories of personal data. If the retention period is unknown, please indicate the criteria for determining it.

Online data, e-mails and hard copies/supporting documents are retained for ten (10) years from the date of the closure of the mission file. Documents may be retained until the end of a possible audit or Court Proceeding if one started before the end of the above period.

In accordance with the record held by DG Budget, Personal Data further processed through ABAC and SUMMA might be retained by DG Budget for up to ten (10) years after the last transaction.

A longer conservation period may equally apply in order to cover periods in case of a dispute or appeal.

Data related to travel bookings is stored in the travel agency's booking system in accordance with EU data protection law.

11) Information/Transparency (Article 14-15) *Information shall be given in a concise, transparent and easily accessible form, using clear and plain language.*
A specific Privacy Notice (F4E_D_29KVHD - Privacy Notice on Personal Data for Mission Management) is published on F4E Net, F4E's external website and in the MIPS+ web application.

Risk Identification - Positive or (indicative) negative list whether a Data Protection Impact Assessment (DPIA) is required (Article 39) *N/A*

- **Positive list of processing operations <u>prima facie requiring</u> a DPIA**:
  o Exclusion databases (2, 4, 9)[2];
  o Large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation) (1, 4, 5, 8);
  o Internet traffic analysis breaking encryption (1, 3, 8);
 	
- **Indicative list of processing operations prima facie <u>not</u> requiring a DPIA**:
  o Management of personal files *as such* (Some procedures resulting in adding information to the personal file may require DPIAs, but not the repository of personal files as such);
  o Standard staff evaluation procedures (annual appraisal);
  o 360° evaluations for helping staff members develop training plans;
  o Standard staff selection procedures;
  o Establishment of rights upon entry into service;
  o Management of leave, flexitime and teleworking;
  o Standard access control systems (non-biometric);
  o Standard CCTV on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in publicly accessible space).

Thank you for completing the Record.
If necessary, proceed with the Threshold Assessment for a DPIA (Annex I)

[2] The numbers refer to the criteria in the Threshold Assessment Form.

Annex I –Threshold Assessment whether a DPIA would be necessary

I Header	
Name of processing operation	[name]
DPO consultation	[date of feedback]
Approval	[name and date]
II Criteria for high risks	
Criterion	*Applicable? Yes [if so, describe how] / No [if borderline: why not?]*
1. Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting. *Examples: a bank screening transactions in accordance with applicable law to detect possibly fraudulent transactions; profiling staff members based on all their transactions in EUI's case management system with automatic reassignment of tasks.* *Counterexamples: standard appraisal interviews, 360° evaluations for helping staff members develop training plans.*	N
2. Automated-decision making with LEF or similar significant effect: processing that aims at taking decisions on data subjects *Example: automated staff appraisal ('if you're in the lowest 10% of the team for the number of cases dealt with, you'll receive a "unsatisfactory" in your appraisal, no discussion')* *Counterexample: a news site showing articles in an order based on past visits of the user.*	N
	N

3. Systematic monitoring: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces. This may cover video-surveillance but also other monitoring, e.g. of staff internet use. *Examples: covert CCTV, smart CCTV in publicly accessible spaces, data loss prevention tools breaking SSL encryption.* *Counterexample: open CCTV of garage entry not covering public space*	
4. Sensitive data: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for identification purposes, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or otherwise considered sensitive. *Examples: pre-recruitment medical exams and criminal records checks, administrative investigations & disciplinary proceedings, any use of 1:n biometric identification* *Counterexample: photos are not sensitive as such (only when coupled with facial recognition or used to infer other sensitive data).*	N
5. Data processed on a large scale, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage: *Examples: European databases on disease surveillance.* *Counterexamples: internal phone directory of an EUI*	N
6. Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject. *Examples: covertly cross-checking access control logs, computer logs and flexitime declarations to detect absenteeism.*	N

Counterexample: transfer of personal file following a change of institution	
7. Data concerning vulnerable data subjects: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified. *Examples: children, asylum seekers.* *[Counterexample: EUI staff are not automatically considered as vulnerable vis-à-vis their employer concerning standard procedures laid down by the Staff Regulations]*	N
8. Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. *Examples: machine learning, connected cars, social media screening of applicants for posts.* *Counterexamples: 1:1 biometric access control using fingerprints*	N
9. Preventing data subjects from exercising a right or using a service or a contract. *Examples: exclusion databases, credit screening* *Counterexample: determination of rights upon entry into service (e.g. expatriation or dependent child allowances)*	N
III Conclusion	
Number of 'Yes' ticked above	0
Assessment: In general, if you tick two or more of the criteria in the list, you should carry out a DPIA. If you consider that in the specific case at hand, risks are not 'high' even though you have two or more 'yes', explain and justify why you think the processing is in fact not 'high risk'.	