



Record of processing of personal data
During Contract implementation (excluding processing during claims assessment),
according to Article 31 Regulation 2018/1725¹

NAME of data processing²: Processing during Procurement Contract/Grant Agreement implementation (excluding processing during claims assessment).

Last update: December 2025.

1) Controller(s) ³ of data processing operation (Article 31.1(a))
<ul style="list-style-type: none"> • <u>Controller: Organisational entity of Fusion for Energy (F4E)</u> • <u>Unit / Department responsible for the processing activity:</u> Project Control, Supply Chain and Finance Department • <u>Contact:</u> Project Control, Supply Chain and Finance Department Data Controller PCSCF-Department-Controller@f4e.europa.eu • <u>Data Protection Officer (DPO):</u> DataProtectionOfficer@f4e.europa.eu
2) Who is actually conducting the processing? (Article 31.1(a))
<p>The data is processed by F4E (responsible Department) itself <input checked="" type="checkbox"/></p> <hr/> <p>The data is processed by a third party (e.g. contractor) (Art. 29 – Processor) <input checked="" type="checkbox"/></p> <p>In certain cases, external persons may process personal data, as staff members of a Support Service Contractor who is performing activities under a Contract with F4E (e.g. Support to the Owner and Architect Engineer contractors for F4E construction projects). Contact information for the relevant third party processors can be attained by contacting the Project Control, Supply Chain and Finance Department Data Coordinator (PCSCF-Department-Controller@f4e.europa.eu)</p>

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.

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, see Article 28.

For the execution of financial transactions, (personal) data is further processed through the Accrual Based Accounting System (ABAC) which is a system ran by DG Budget (budg-data-protection-coordinator@ec.europa.eu). The responsibilities of both F4E and DG Budget regarding Personal Data Protection within ABAC are described in the [Service Level Agreement](#) and are partly laid out in section 3B below.

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, summarize 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.

Processing during the assessment of Contractors' claims/disputes is excluded from this record. Two separate Records ([F4E D 29XJDL](#) and [F4E D 29RKA4](#)) cover personal data collection and processing during the claim/dispute assessment processes. A separate Record ([F4E D 24GD29](#)) covers personal data collection and processing during the procurement/call phase prior to the signature of the Contract.

3A/ Purpose of the processing

This record covers processing of all personal data required during all F4E Procurement Contracts/Grant Agreements implementation, including FIDIC works based contracts (hereafter 'Contracts' will be used to refer to all those categories). This includes:

- Processing in support of cost and performance control, either:
 - o In the context of F4E's Contracts with clauses foreseeing the reimbursement of incurred costs (including staff costs), payments proportional to the performance of certain tasks by specified employees, or payments proportional to the engagement of certain human resources; or reimbursement of certain expenses incurred by their staff; or
 - o Processing required when introducing/negotiating Contracts changes and the proportional compensation for the contractors;
- Processing occurring as part of the evaluation of specific Contracts under Framework Contracts;
- Processing occurring as part of the Supplier Audits and/or Supply Chain Supervisions carried out by the Quality Assurance Unit;
- Any other processing that may be required during implementation of Contracts.

In the case of cost and performance control, personal data are collected and processed with the purpose of controlling Contractor's cost and performance during the implementation of Contracts. This processing is necessary to monitor the number of working hours spent by Contractors' staff,

to perform cost and productivity control and to assess Contract changes (for example, when substantiations are requested for reconciliation of expenses). Regarding the evaluation of specific Contracts under Frameworks Contracts, processing of personal data (eg. CVs) serves the purpose of selecting/indicating/identifying contractor's resources which will perform specific tasks.

This record furthermore covers any additional processing required with the purpose of supporting the implementation of Contracts, such as the carrying out of Supplier Audits and Supply Chain Supervisions.

3B/ Description of the processing

The processing starts with the signature of the Contract and ends with the payment of the last invoice/cost recognized or granted (notwithstanding in the case of audits or court proceedings as described in section 10). During Contract implementation, documentation including personal data (e.g. time sheets, CVs and/or impact assessment reports including personal data of data subjects) may be provided by the Contractor in the context of the normal performance of the Contract. This is done with the purpose(s) described above. Such documentation may also be requested during Contract amendment introductions/negotiations and/or during the carrying out of Supplier Audits and/or Supply Chain Supervisions.

The personal data are transmitted to F4E by electronic means, either by transfer of files, or by giving F4E access to Contractor's databases containing the information. F4E extracts the relevant subsets of information from the files and/or databases. In some cases, this may include Contractor's staff names and salary information, to the extent necessary in order to calculate hourly/daily costs for the specific staff member. In the case of cost and performance control, once the costs and performance indicators are calculated by F4E, any further use and dissemination of cost and performance information will occur in an anonymised form, deleting any personal information. In the case of CVs provided in the context of specific contracts, no further dissemination outside of evaluation activities occurs except in the case of Supplier Audits when CVs could on exception be included in the audit report to support decisions.

For the execution of financial transactions, (personal) data is processed through the Acrual Based Accounting System (ABAC) which is a system ran 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 System ABAC the necessary Identification Form, 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 within ABAC are described further in the [Service Level Agreement](#).

The Data Protection Record and Privacy Notice held by DG Budget can be found [here](#).

Furthermore, in the context of contract amendments, and in line with [F4E's Financial Regulation \(art. 31\)](#), information on recipients of funds financed from the budget of F4E shall be published having due regard for the requirements of confidentiality and security, in particular the protection of personal data: the name of the recipient; the locality of the recipient; the amount legally committed and the nature and purpose of the measure. The name of the recipient can be Personal Data in the case of legal persons which name identifies one or more natural persons. According to the threshold from [Directive 2014/24/EU](#) as referred to in [Regulation \(EU, Euratom\) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union \(recast\)](#), the aforementioned data will be published in the Official Journal of the European Union and/or on F4E's publicly accessible Industry Portal. Where personal data are published, this personal data shall be removed two years after the end of the financial year in which the funds were awarded. Data will only be processed to serve the appropriate purpose(s) as described above.

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 22 February 2021 (2021/281 Euratom), O.J. L 62, 23.02.2021, p.8, in particular Article 6 thereof.
 - Statutes annexed to the Council Decision (Euratom) No 198/2007 “establishing the European Joint Undertaking for ITER and the Development of Fusion Energy and conferring advantages upon it”, as last amended on 22 February 2021, in particular Article 10 thereof. [F4E Financial Regulation \(2GYA92\)](#), entered into force on 1 January 2020.
- (b) compliance with a *specific* legal obligation for F4E to process personal data⁴

⁴ The distinction between points (a) and (b) is that in point (a) F4E is given a task which requires the processing of personal data to fulfil it (e.g. staff appraisal), while in point (b), the legal basis directly requires F4E to process the personal data, without margin of implementation.

- (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 acting as Contractor's employees, Sub-Contractor's employees or other third economic operator's employees (e.g. service companies, suppliers, etc.) whose details are submitted in support of the substantiation of Contractor's costs and performance, the evaluation of Contracts under frameworks, Supplier Audits and Supply Chain Supervisions, or as part of any other aspects of Contract implementation that require processing of personal data.

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, and can in the context of the described purposes include:

- Name, date of birth, gender, personal numbers or other identifiers of general application, nationality, contact details (company and department, postal address, country of residence, business telephone number, mobile telephone number, fax number, e-mail address), signature;
- Professional and education information: CV's – work experience/employment history, education, training and academic background, personal skills and competences (language, technical skills);
- Functions, working hours, working place, salaries, time sheets, and other information or personal data provided under the Contract with the purpose of substantiating cost and performance elements;
- Identification Form.

The above is an illustrative listing without limitation to any other possible personal data that could be disclosed by the Contractor. Only relevant and necessary data for the Contract cost and performance control, evaluation of Contracts under Frameworks Contracts, Supplier Audits and

Supply Chain Supervisions, and other relevant aspects of Contract implementation may be collected and further processed. However, since the information is not provided on standard forms, the Contractor may supply information which might not be necessary for the purposes here described, for instance gender, age and nationality. Non-relevant data shall not be requested by F4E nor further processed in the context of the processes covered by the present record. The Personal Data listed above that are also further processed in ABAC 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 collected personal data:

- F4E staff members in charge of commercial cost and performance control activities for the Contract implementation within which the personal data is disclosed or who may be consulted if deemed necessary for a specific case regarding Contract implementation. This includes, but is not limited to: Commercial Manager, Commercial Management Officers, Financial Assistants, Financial Officers, Cost Controllers, FIDIC Engineer and his/her Representatives;
- If necessary for monitoring, evaluation, inspection or auditing tasks, access may be given to: Heads of Units/Departments responsible for Contract implementation (e.g. PCSCF, Procurement, Finance, Project Management, Legal);
- If necessary for supporting and data analysis tasks: Members of the F4E team, who are not F4E staff, acting as Support to the Owner and who are involved in the cost and performance control process;
- In the case of a Supplier Audit: staff from the Quality Assurance Unit, relevant staff from the PM Department, the affected Programme team and all certified auditors within F4E;
- In the case of Supply Chain Supervisions: staff from the Quality Assurance Unit and the affected Programme team;
- F4E IT staff, when asked to provide technical support; F4E IDM Manager, if necessary for support;
- For Personal Data further processed through ABAC:
 - All F4E staff on the financial circuit have access to the data on ABAC. 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.

Also, if appropriate and necessary for monitoring or inspection tasks, access may be given to: e.g. 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 may be transferred to third countries or International Organizations recipients:

Yes

No

If yes, specify to which country/IO:

F4E is the Euratom's Domestic Agency for ITER and therefore operates within the scope of the international treaty regulating the ITER Project. Staff of the ITER International Organisation (IO) may be involved in F4E's contract implementation, in the framework of the implementation of the Procurement Arrangements (PA) between F4E and IO and/or of other provisions of the ITER treaty (e.g. for activities related to Nuclear Safety and ITER operational licensing). Transfer of data to IO may also occur in the context of the evaluation of specific Contracts under framework, or other aspects/parts of Contract implementation if required.

As a rule, transfer of the personal data of Contractors staff to IO occurs in anonymised format (i.e. after having removed all personal data). Therefore, the normal transfer of data to IO as part of the described processes occurs through normal e-mail communication.

In certain cases, upon explicit request by IO (e.g. for auditing purposes or nuclear safety inspections), the transfer may include personal data. In these cases, the transfer will be performed by means of encrypted file transmission by e-mail to the appointed contact person at IO. The transfer shall only occur if the personal data is necessary for cases for which IO's access and/or monitoring rights are foreseen under the PA or any other agreement between Euratom, F4E and IO. In such cases, IO Data Protection Policy shall cover the personal data.

Reference: F4E-IO Data Protection Arrangement: [F4E_D_2SFNUQ - F4E-ITER IO Data Protection Agreement](#)

If yes, specify under which safeguards and add reference:

Adequacy Decision (from the Commission)	<input type="checkbox"/>
Memorandum of Understanding between public authorities/bodies	<input type="checkbox"/>
Standard Data Protection Clauses (from the EDPS/Commission)	<input type="checkbox"/>
Corporate Rules	<input checked="" type="checkbox"/>
Others, e.g. contractual/agreements (subject to authorization by the EDPS) Data Processing Agreement	<input checked="" type="checkbox"/>

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".

All documents containing personal data are kept by the responsible staff members, and are:

- 1) Either stored under restricted-access folders of F4E's electronic documentation management system (called IDM) and/or in restricted access folders of F4E's IT Storage system (O: Drive) and/or in SGTi (the contractual communication tool between the Contractors, the Engineer and the Employer), if the information has been transmitted to F4E electronically, and/or
- 2) Locked in cupboards/offices if the information has been transmitted in paper and/or hard copy form, and/or
- 3) For Personal Data required to carry out financial transactions, these data are furthermore processed/stored on DGBudget's ABAC System.

After the completion of the relevant activities, and in any case after the conclusion of the Contracts implementation, the collected personal data and all related information shall be stored by F4E in conformity with its Documentation Policy ([F4E D 24L87F](#)).

The F4E staff involved in the personal data collection and processing shall be reminded of the confidentiality and data protection obligations stemming from the Staff Regulation and the Data Protection Regulation EU 2018/1725. Members of the team, as well as non-F4E staff, involved in the cost and performance control and other implementation processes shall sign a [Declaration of Confidentiality](#). Specific access rights to electronic files stored in IDM and SGTi will be granted to the members of the team involved in the cost and performance control and other implementation

processes. The appropriate level of IDM data security is set in agreement with the IDM Administrator. The IDM system itself is secured in accordance with the ICT Information Systems Security Policy ([F4E D 2AMU6N](#)) and the System Security Plan for IDM ([F4E D 2CVKW5](#)) document. F4E's IT Storage system is also secured in accordance with the ICT Information Systems Security Policy ([F4E D 2AMU6N](#)), with specific access rights granted to the relevant team members.

ABAC is a secured online system ran by DGBudget. The specific security measures can be found in their [Data Protection Record](#).

Have ICT and the DMO been consulted during the establishment of the processing?

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.

- Documents related to cost and performance control, evaluation of specific Contracts under Framework Contracts, and to implementation generally (except Supplier Audits and Supply Chain Supervisions), which may contain personal data of Contractor's and third party organization's employees shall be stored for no more than 7 (seven) years after payment of the final instalment of the Contract.
- For Supplier Audits the retention period is 10 (ten) years after payment of the last instalment of the Contract.
- Personal Data Processed as part of the Supply Chain Supervisions can be retained for the entire duration of F4E's activities.
- In accordance with the [record](#) held by DG Budget, Personal Data further processed through ABAC might be retained by DG Budget for up to ten (10) years after the last transaction.
- Where personal data are published in the Official Journal of the European Union and/or on F4E's publicly accessible Industry Portal as described in section 3B, this personal data shall be removed two years after the end of the financial year in which the funds were awarded.
- Documents may be retained until the end of a possible audit (other than the aforementioned audit) or Court proceeding if one started before the end of the above period.

11) Information/Transparency (Article 14-15)

Information shall be given in a concise, transparent and easily accessible form, using clear and plain language.

Information to data subjects is provided at different stages of the life cycle of each F4E Contract, in the respective contractual provisions on data protection contained in the F4E Contract and during the implementation of the F4E Contract if processing of any personal data is required under the Contract.

A specific Privacy Notice ([F4E_D_2GBPF](#)) is published on F4E Net, the Industry Portal and on F4E's external website.

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

Not applicable

- **Positive list of processing operations prima facie requiring a DPIA:**
 - o Exclusion databases (2, 4, 9)⁵;
 - 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 not 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).

⁵ The numbers refer to the criteria in the Threshold Assessment Form.

Annex I –Threshold Assessment whether a DPIA would be necessary

Only proceed to the threshold assessment if your planned processing operations fall under neither of the two lists above.

I Header	
Name of processing operation	[name]
DPO consultation	[date of feedback]
II Criteria for high risks	
Criterion	Applicable? Yes [if so, describe how] / No [if borderline: why not?]
<p>1. Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting.</p> <p><i>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.</i></p> <p><i>Counterexamples: standard appraisal interviews, 360° evaluations for helping staff members develop training plans.</i></p>	[Y (how?) / N]
<p>2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects</p> <p><i>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')</i></p> <p><i>Counterexample: a news site showing articles in an order based on past visits of the user.</i></p>	[Y (how?) / N]
<p>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.</p>	[Y (how?) / N]

<p><i>Examples: covert CCTV, smart CCTV in publicly accessible spaces, data loss prevention tools breaking SSL encryption.</i> <i>Counterexample: open CCTV of garage entry not covering public space</i></p>	
<p>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. <i>Examples: pre-recruitment medical exams and criminal records checks, administrative investigations & disciplinary proceedings, any use of 1:n biometric identification</i> <i>Counterexample: photos are not sensitive as such (only when coupled with facial recognition or used to infer other sensitive data).</i></p>	[Y (how?) / N]
<p>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: <i>Examples: European databases on disease surveillance.</i> <i>Counterexamples: internal phone directory of an EUI</i></p>	[Y (how?) / N]
<p>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. <i>Examples: covertly cross-checking access control logs, computer logs and flexitime declarations to detect absenteeism.</i> <i>Counterexample: transfer of personal file following a change of institution</i></p>	[Y (how?) / N]
<p>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. <i>Examples: children, asylum seekers.</i></p>	[Y (how?) / N]

<i>[Counterexample: EUI staff are not automatically considered as vulnerable vis-à-vis their employer concerning standard procedures laid down by the Staff Regulations]</i>	
<p>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.</p> <p><i>Examples: machine learning, connected cars, social media screening of applicants for posts.</i> <i>Counterexamples: 1:1 biometric access control using fingerprints</i></p>	[Y (how?) / N]
<p>9. Preventing data subjects from exercising a right or using a service or a contract.</p> <p><i>Examples: exclusion databases, credit screening</i> <i>Counterexample: determination of rights upon entry into service (e.g. expatriation or dependent child allowances)</i></p>	[Y (how?) / N]
III Conclusion	
Number of 'Yes' ticked above	[n]
<p>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'.</p>	