



RECORD

Of processing personal data during procurement and grant procedures, according to Article 31 Regulation 2018/1725¹

NAME of data processing: Evaluation of the eligibility of economic operators to participate in the procurement/grant procedures in accordance with exclusion and selection criteria, and/or evaluation of the content of tenders/proposals against the award criteria.

Last update: December 2025.

1) Controller(s) of data processing operation (Article 31.1(a))
<ul style="list-style-type: none"> • <u>Controller:</u> Organizational entity of Fusion for Energy (F4E) • <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>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 unit) 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"/> Contact point at external third party (e.g. Privacy/Data Protection Officer):</p> <ul style="list-style-type: none"> • DPO EU-Supply: dataprotectionofficer@eu-supply.com EU-Supply is used for the submission of tenders/applications. EU Supply Privacy • In order to prepare and execute budgetary and legal commitments, (personal) data is further processed through the Acrual 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

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.

regarding Personal data Protection within ABAC are described in the [Service Level Agreement F4E-2019-SLA-71](#) 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, 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.

This record covers the processing of personal data during procurement and grant procedures. The processing of personal data as part of Procurement Contract/Grant implementation (excluding claims) is covered by a separate record ([F4E D 2GBTAX](#)). Some processing may also be necessary in preparation of the assessment of Contract claims/disputes, in order to prepare F4E's position with respect to the potential claim/dispute. Two separate records ([F4E D 29RKA4](#) and [F4E D 29XJDL](#)) cover data processing during these claim/dispute processes.

3A) Purpose of the processing

The personal data are collected and processed with the purpose to evaluate the eligibility of economic operators to participate in the procurement/grant procedure in accordance with exclusion and selection criteria, and/or to evaluate the content of tenders/proposals submitted during the procurement/grant procedure against the award criteria with the view to award the contract/grant agreement.

3B) Description of the processing

The personal data are collected from the tender/application or supporting documents submitted with a view to participating in procurement/grant procedures. These documents may contain personal data of Contractor's employees and/or of employees of third-party organizations (such as sub-contractors, services companies, or suppliers). The data are transmitted to F4E through the EU-Supply application called "CTM", or, in some cases, via e-mail or other electronic means, or on paper.

Negotiation meetings may be recorded and transcribed using the Copilot software tool, cover by [Privacy Notice Copilot \(3DGVMM\)](#).

Data processing covered by this record ends with the signature of the contract/grant agreement. In order to prepare and execute budgetary and legal commitments prior to Contract signature,

(personal) data are 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 further described in the Service Level Agreement F4E-2019-SLA-71.

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

Furthermore, in the context of the contract award, 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, inpersonal data: the name of the recipient; the locality of the recipient; the amount legally comitted and the nature and purpose of the measure. The name of the recipient can be Personal Data in the case of legal persons whose name identifies one or more natural persons. Depending on the instrument and the thresholds 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.

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 No 2007/198 (Euratom) 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 No 198/2007 (Euratom) of 27 March 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.

- Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council;

- Financial Regulation of Fusion for Energy, adopted by the Fusion for Energy Governing Board on 10 December 2019;

- 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).

(b) compliance with a *specific* legal obligation for F4E to process personal data²

(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 associated with the candidate/tenderer/applicant entities (including their staff and subcontractors), whose details are submitted in tender/proposal and related documents in view of participating in procurement/grant procedures.

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. The following data categories may be processed within procurement/grant award procedures:

² 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.

- Name, date of birth, gender, nationality, function, contact details (company and department, postal address, country of residence, business telephone number, mobile telephone number, fax number, e-mail and internet address, and signature);
- Certificates for social security contributions and taxes paid;
- Extracts from judicial records;
- Identification Form
- Passport/ID number; VAT number; membership in a trade or professional organization;
- Professional and education information: CV's – work experience/employment history, education, training and academic background, personal skills and competences (language, technical skills);
- Declaration of honour that the tenderer/applicant is not in one of the exclusion situation referred to in the Financial Regulation,
- Other personal data contained in the tender/application (credentials).

Only data relevant and necessary for the procurement/grant procedure are collected and further processed. The Personal Data listed above that are also further processed in ABAC can be found in the [Data Protection Record](#) held by DG Budget.

Since the information is not provided on standard forms, the candidates/tenderers/applicants, their staff and subcontractors, may supply information which might not be necessary for the purpose of selection or the award of grant or contract, for instance gender, age and nationality.

Non-relevant data shall not be requested by F4E nor further processed.

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)

Sensitive personal data processed are judicial records.

For their processing under Art. 10 EUDPR 2018/1725, the safeguards used are:

Appropriate safeguards ensure:

- Strict access control (only authorised personnel),
- Purpose limitation (data used only for specified legal purposes),
- Data minimisation (only necessary data is processed),
- Security measures (technical and organisational),
- Transparency and accountability (records of processing, impact assessments).

Technical security measures include:

- Access Control Systems: Role-based access ensures only authorised personnel can view or modify sensitive data.

- Secure Servers and Backups: Data is stored in secure EU-based data centres with backup systems to ensure availability.
- Multi-Factor Authentication (MFA): Used to verify user identity before granting access to sensitive systems.
- Threat Detection Tools: Antivirus, antimalware, and intrusion detection systems monitor for suspicious activity.

Organisational security measures include:

- Strict Access Protocols: Access to judicial records is granted only on a “need-to-know” basis.
- Staff Confidentiality Commitments: Personnel authorised to process sensitive data must sign confidentiality agreements or be bound by statutory obligations.
- Training and Awareness: Regular training sessions ensure staff understand data protection responsibilities and risks.
- Incident Response Plans: Procedures are in place to detect, report, and respond to data breaches or security incidents.

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).

Data is strictly limited to authorized personnel involved in the procurement or grant process, including:

- F4E Staff from the operational, procurement, financial and/or legal groups participating in the management of the selection of candidates/contractors/beneficiaries;
- External experts (including when appropriate IO staff) and contractors participating in the evaluation of tenders/applications when external expertise is required;
- The relevant Authorizing Officer;
- The members and chair of the F4E Procurement and Contract Committee (PCC), approving the award of contracts and grants above certain thresholds;
- Members of the decision-preparatory bodies of the Governing Board, and Members and chair of the Governing Board, consisting of representatives from all the members of F4E who are responsible for supervising its activities, including in selected cases reviewing the award of the contracts and grants;

- F4E IT staff, only when requested to provide technical 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 Authorization 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 Privacy Notice](#).

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

Data is 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 Organization (IO) may be involved in F4E's procurement and grant process.

Namely, data may be transferred to ITER IO staff during the evaluation process of tenders/applications: F4E acts as an independent controller; IO staff members may be appointed as experts in which case they may have access to personal data of tenderers; no personal data of tenderers are otherwise shared with the IO as an organization. Only in the case of a joint procurement both F4E and IO may be joint controllers if both organizations conduct the procurement procedure in an integrated procurement team.

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 DPS/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 organizational 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 tenders/applications, including any supporting documents submitted are kept by the relevant procurement officer or commercial manager 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 IT Storage system, if the information has been transmitted to F4E electronically, or
- 2) Locked in cupboards/offices with restricted access if the information has been transmitted in paper and/or hard copy form;
- 3) For Personal Data required to prepare and execute budgetary and legal commitments, these data are furthermore processed/stored on DGBudget’s ABAC System;
- 4) Personal Data is furthermore also stored in the EU-Supply CTM system ([EUSupply Privacy Notice](#)).

After the completion of the procurement or grant award procedure, the collected personal data and all related information are stored in the archives on the premises of F4E in conformity with F4E's Documentation Management Policy ([F4E D 24L87F](#)) and Procurement Documentation Management Policy ([F4E D 26LX3X](#)).

The F4E staff involved in 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 opening and evaluation committees (internal or external experts and contractors) as well as F4E staff not members of the Evaluation Committee, but being consulted, sign the [Declaration of absence of conflict of interest and of confidentiality](#).

Specific access rights to electronic files stored in IDM will be granted to the members of the team involved in the procurement and grant processes. The appropriate level of IDM data security is set in agreement with the IDM Administrator. F4E's computer network system 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.

Data processed through the EU-Supply application is moreover covered by the privacy policy held by the EU Supply PLC group ([EU Supply Privacy Notice](#)).

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 the procurement and grant processes 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. Personal Data provided as part of tenders that are subsequently rejected shall be stored for no more than 5 (five) years after the tender has been rejected.

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 or Court Proceeding if one started before the end of the above period.

The data retention obligations for IO are aligned with F4E's.

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. A Privacy Notice ([F4E D 2ANX4Q](#)) is published on F4E Net, F4E external website and the Industry Portal to document how F4E processes personal data during the procurement and grant

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:**
 - Exclusion databases (2, 4, 9)³;
 - Large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation) (1, 4, 5, 8);
 - Internet traffic analysis breaking encryption (1, 3, 8);
- **Indicative list of processing operations prima facie not requiring a DPIA:**
 - 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);
 - Standard staff evaluation procedures (annual appraisal);
 - 360° evaluations for helping staff members develop training plans;

³ The numbers refer to the criteria in the Threshold Assessment Form.

- Standard staff selection procedures;
- Establishment of rights upon entry into service;
- Management of leave, flexitime and teleworking;
- Standard access control systems (non-biometric);
- 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)

Annex I – Threshold Assessment whether a DPIA would be necessary

I Header	
Name of processing operation	[name]
DPO consultation	[date of feedback]
II Criteria for high risks	
<i>Criterion</i>	<i>Applicable? Yes [if so, describe how] / No [if borderline: why not?]</i>
<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>	No
<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>	No
<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>	No

<p><i>Examples: covert CCTV, smart CCTV in publicly accessible spaces, data loss prevention tools breaking SSL encryption.</i></p> <p><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.</p> <p><i>Examples: pre-recruitment medical exams and criminal records checks, administrative investigations & disciplinary proceedings, any use of 1:n biometric identification</i></p> <p><i>Counterexample: photos are not sensitive as such (only when coupled with facial recognition or used to infer other sensitive data).</i></p>	No
<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:</p> <p><i>Examples: European databases on disease surveillance.</i></p> <p><i>Counterexamples: internal phone directory of an EUI</i></p>	No
<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.</p> <p><i>Examples: covertly cross-checking access control logs, computer logs and flexitime declarations to detect absenteeism.</i></p> <p><i>Counterexample: transfer of personal file following a change of institution</i></p>	No
<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.</p> <p><i>Examples: children, asylum seekers.</i></p>	No

<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>	No
<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>	No
III Conclusion	
Number of 'Yes' ticked above	0
<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>	