RECORD
of processing activity
according to Article 31 Regulation 2018/1725[1]

NAME of data processing[2]:
Creation/Renewal/Deletion of accounts in F4E IDM suite of applications for external users.

Last update: July 2021

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: Fusion for Energy (F4E) Unit / Position of Process Owner **responsible[4]** for the processing activity: DT Unit / Administration Department DP-ICT@f4e.europa.eu : Iacopo Ianniello - Head of DT Unit Data Protection Officer (DPO): DataProtectionOfficer@f4e.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))[5]	
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):	☐

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.

4 This is the unit that decides that the processing takes place and why.

5 Is F4E itself conducting the processing? Or has a provider been contracted?

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.

Creation, renewal of validity and deletion of accounts in F4E IDM suite of applications for external users.

Accessible applications include IDM document management, DACC and Contract Tracker (CTS).

This procedure allows the creation of external user accounts for F4E IDM suite of applications in order for external users to be authenticated in the system. Also it allows for the extension of validity and deletion of such created users.

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;

- Staff Regulations of Officials (SR) and the Conditions of Employment of Other Servants of the European Communities (CEOS), in particular *[if applicable, Article… of the Staff Regulations regarding...]*

(b) compliance with a *specific* legal obligation for F4E to process personal data[6] ☐

[6] 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) ☐

Consent should be considered as the exception, applicable in the absence of another legal basis. In those cases, e.g. in the case of photos or subscription to newsletters, ensure that the request for consent is presented in an intelligible (clear and plain language) and easily accessible form, and complies with the requirements of Art. 7.

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

Whose personal data is being processed?

External users aiming at accessing F4E IDM, CTS, DACC applications for work relationship purposes with F4E.

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:**
Identification data: first name, family name, Company name, Office Address, e-mail address, telephone number.

(b) **Sensitive personal data** (Article 10)
None.

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 have access to the personal data processed:
Selected members of the DT Unit in charge of the processing.

All active users accessing the mentioned systems can access some pf the Personal Data (first name, family name, e-mail address).

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, IAS, ECA, 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".

Security measures are implemented to ensure integrity, confidentiality and availability of information. The default provisions include backups, centralized logging, software updates and continuous vulnerability assessment and follow-up. Specific provisions resulting from the characteristics of the information system may lead into the implementation of encryption, two factor authentication among others found relevant following a risk analysis.

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.

Ten years maximum after the termination of the work relationship.

External users´ Personal data retention time is linked to the retention period of the documents they are connected to.

11) Information/Transparency (Article 14-15)

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

See related Privacy Notice whose link is displayed in the mentioned systems.

Also see F4E public web site.
