

RECORD
of processing activity
according to Article 31 Regulation 2018/1725¹

NAME of data processing²:

Creation, Deletion and Management of accounts in ICT systems

Last update: July 2021

1) Controller(s)³ of data processing operation (Article 31.1(a))

- Controller: Organisational entity of Fusion for Energy (F4E)
 - Unit / Department **responsible⁴** for the processing activity: *DT Unit*
 - Contact: *DP-ICT@f4e.europa.eu*
- 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):

ITER IO, data.protection@iter.org

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 and deletion of accounts in F4E Microsoft Windows environment as well as creation and deletion of e-mail accounts in all F4E ICT applications.

It includes both local (from within F4E ICT network) and remote connection.

In particular, this procedure allows the creation of user accounts for F4E ICT applications in order for users to be authenticated in the systems. Also, it allows for the extension of validity and deletion of such created users.

For some applications periodic review of access rights on the user accounts is also performed.

Moreover, for F4E staff and contractors at Cadarache site, on top of the above, creation and deletion of accounts in ITER IO IT environment including access to:

- ITER IO e-mail system,
- ITER IO client computing systems (laptops),
- ITER IO IT ancillary services (including: voice calls, printing, shared folders storage area, etc.).

Through F4E ticketing system and/or e-mail messages, the DT Unit is informed about the upcoming taking up of duties of new colleagues or start of contract of students, experts, external contractors or members of F4E Governing Board.

The DT Unit staff manually proceeds to the following:

- Creation of Microsoft Windows account in Microsoft Windows Active Directory,
- Creation of mailbox in F4E e-mail system,
- Creation of profile in F4E Skype for Business environment,
- Creation of profile in F4E eHR Database (only for staff members).

In a similar way, termination of employment/contract/collaboration is communicated to the DT Unit and the above accounts are closed down.

Moreover, in the case of the Cadarache site, equivalent operations are performed on ITER IO systems by ITER IO IT staff.

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;
- (b) compliance with a *specific* legal obligation for F4E to process personal data⁶.....
- (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?

All F4E staff, insourced and outsourced external persons, students and internship, staff of contractors and suppliers working both at F4E Barcelona premises and at Cadarache site, members of F4E Governing Board and similar committees that have access to F4E suite of applications and tools and to whom ICT equipment has been assigned.
In general any user authorised at accessing F4E ICT applications.

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.

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, displayed name, e-mail address, phone number (fixed and/or mobile), Office location and number, start date of contract, contract type, end date of contract. Company name and location. Personnel number, grade and position.

(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:

F4E DT responsible officers in charge of the processing.
ITER IO IT responsible officers in charge of the processing (only for F4E staff and contractors based at the Cadarache site).

The following categories have only access to a subset of the identification data, in general only name, family name and email address:

- All F4E staff accessing F4E information systems
- All students, experts, staff of external contractors, members of F4E Governing Board accessing one or more F4E information system.
- All third parties receiving e-mail messages from F4E staff, students, experts, external contractors and members of F4E Governing Board entitled to have an F4E e-mail address.

Also, only 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: ITER 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:

[F4E_D_2RLYZR - F4E-ITER IO Data Protection Agreement](#)

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.

Maximum two years after closure of the account.

11) Information/Transparency (Article 14-15)

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

Related Privacy Notice published in F4E web site and Intranet pages.