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

NAME of data processing:
User data management using Microsoft Azure AD Federation

Last update:
28 November 2018

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

Controller: Fusion for Energy (F4E)

Unit **responsible** for the processing activity: ICT Unit

Process Owner's 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))

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): Mr Basile Lamure (Basile.Lamure@microsoft.com).

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

Why are the personal data being processed? Specify what you intend to achieve and the underlying reason for the processing. Describe the individual steps used for the processing.

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

Users with an F4E account are automatically allowed (without the need to authenticate) to access Microsoft cloud based solutions like Office 365 and Teams among others.

The technical solution is called federation with Microsoft Azure Active Directory. By implementing this solution, F4E aims at a seamless integration with Microsoft cloud based solutions.

Personal data processed:

- Name, Family name

- Username
- E-mail address and SIP address
- Office and F4E mobile telephone number
- Office location (floor and office number)

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 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) ☐

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 are being processed?

F4E staff, non-F4E staff (experts, consultants, trainees or seconded national experts and other external users) with an assigned F4E account.

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:**

- Name, Family name
- Username
- E-mail address and SIP address
- Office and F4E mobile telephone number
- Office location (floor and office 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 are 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:

- ICT Officers responsible for the systems used for the processing, for technical support, administration and maintenance tasks.
- Microsoft staff dealing with Azure AD Federation.

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

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

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

Data are transferred to third countries or International Organizations recipients:

Yes ☒

No ☐

If yes, specify to which country/IO: USA, Canada, Brasil, Australia, India, Japan, Korea, Singapore, China, South Africa, UAE.

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/Commission) ☒

Binding Corporate Rules ☐

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

Reference*:* See Data Protection section in document "Microsoft Volume Licensing Online Service Terms" (downloadable at: https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx)

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

Please specify where the data are stored (paperwise and/or electronically) during and after the processing. Specify how they are 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.

8 years from the creation of the Active Directory account according to F4E document on retention: https://idm.f4e.europa.eu/?uid=24BUD4 being the information detailed in point 6 here above assimilated to the information contained in Personal Files.

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 published in the ICT section of F4E Intranet. The link to the PN is also provided to the data subject at the time of the creation of the Active Directory account.