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

NAME of data processing:
Office automation and collaboration software tools by Microsoft (Office 365)

Last update: October 2020

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

- Controller: Organisational entity of Fusion for Energy (F4E)

    o Unit / Department **responsible** for the processing activity: *ICT / Administration*

    o 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 (M. Capra, ICT) itself – DP-ICT@f4e.europa.eu :....................☒

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): Microsoft Ireland Operations Limited, Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117 - Basile.Lamure@microsoft.com

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.

---

[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.

Provision of software applications that allow the execution of daily work by F4E staff and external insourced contractors' staff.

The Microsoft Office 365 suite of applications will include, but is not limited to: word processing, electronic spreadsheet, e-mail, shared storage, collaboration and communication software tools.

Normal usage of such tools may result in storage and processing of personal data e.g.: e-mail addresses, names, etc.

Fusion for Energy and Microsoft may process information stored and exchanged through Office365, including personal data, for the following key business processes:

1. Identity and access management of Office365 applications

2. Personal data breach management

3. Security event and incident monitoring and logging

4. Data subject rights management

5. Customer support management

6. Data access management

7. Collaboration and file exchange

8. Site administration

9. External access management

10. Conducting virtual meetings and teleconferences

11. Chat-based collaboration

12. Project and task management

13. Activity notification to end-user

14. Exchange of email

15. Processing of diagnostic data

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) .... ☐

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

Whose personal data is being processed?

Any user of the MS Office365 suite of programs as well as Data Subjects recipients of communications, Data Subjects referred-to by the users like, as an example, in the text of an e-mail.

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, e-mail address, office and F4E mobile telephone numbers, Office number.
Any Personal Data collected from the users like, as an example, the one that may be contained in the text of an e-mail sent by means of the MS O365 tools.

(b) **Sensitive personal data** (Article 10)
Collected by F4E within the scope here covered: none.
However, users may have the electronic systems process any sensitive data they may provide like, as an example, the one that may be contained in the text of an e-mail sent by means of the MS O365 tools.

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 (listed at point 6 a. above):

- staff members,
- any non-F4E staff receiving e-mails, joining a conversation, invited to on-line meetings, specific Teams or similar,
- Microsoft technical officers, if requested for technical support.

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, 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: USA

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*:* Standard Contractual Clauses embedded in the Microsoft Online Services Terms, Microsoft Privacy Policy (http://privacy.microsoft.com) and additional GDPR-specific clauses in the Microsoft Online Services Terms.

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 2 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.