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

NAME of data processing:
H&S Management System – Procedure for the Coordination between F4E and other Undertakings (F4E_D_ 2DTLUL)

Last update: March 2020

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

- Controller: Hans Jahreiss, Senior Manager responsible for Health & Safety
  - Unit / Department **responsible** for the processing activity: *H&S Coordinator*
  - Contact: h&sdataprotection@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):

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.

Personal Data are processed as a consequence of the implementation of the H&S Management System, which comprehends the H&S Policy (F4E_D_282GG4) and the 8 H&S Procedures developing it.

The Procedure for the Coordination between F4E and Other Undertakings (F4E_D_2DTLUL) establishes the coordination processes to be followed by F4E and external organisations / companies when working at the same premises.

F4E and external organisations shall exchange H&S-related information in the following cases:

- F4E Staff going on mission to external sites (in some cases, external sites may require the provision of certain H&S documentation before an F4E staff access its premises, e.g. Training certificates or Fitness to Work certificates)
- External workers accessing F4E premises (different rules apply for BCN, CAD and GAR; the rules are not part of this Procedure)

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;

- Council Directive of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (89/391/EEC), in particular Article 6.4 thereof;

- F4E Health & Safety Policy (F4E_D_282GG4), in particular Article 8 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?

F4E staff members and seconded national experts (SNEs).

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.

Whenever a staff member is going on mission to an external site, F4E shall liaise with the external site in order to check the H&S requirements to access and/or perform activities at its premises. Should the external site require the provision of specific H&S documentation, it shall be provided before the mission takes place.

(a) **General personal data:**

- Surname, name of the F4E staff member going on mission, H&S Trainings undertaken and PPE provided, Health Surveillance certificates.

.

(b) **Sensitive personal data:**

Not Applicable.

7) Recipient(s) of the data (Article 31.1 (d)) – Who has access to the personal data?

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,Court, EDPS).

The following recipients have access to the personal data processed:

- H&S Coordinator
- Line Manager
- H&S Officer of the external site whenever the provision of H&S related documentation is required.
- IDM Manager, if necessary for support
- ICT officer responsible, if necessary for technical support.

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

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:

In the event an external company / organisation requests the provision of certain H&S documentation in order to access its premises, F4E shall provide the requested H&S documentation of the concerned staff member (e.g. H&S Training certificates, Fit to Work certificates) before s/he is sent on mission.

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*:* Not Applicable

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.

Risk Assessments containing the PPE and H&S Trainings of staff members shall be stored for a period of 20 years once the staff members leaves F4E. This retention period responds to:

- There is often a long period between exposure and onset of ill health of the staff member.

11) Information/Transparency (Article 14-15)

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

Information shall be given through the corresponding Privacy Notice available to all F4E Staff and national experts seconded to F4E.