

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

NAME of data processing:

H&S Management System – Procedure for the Risk Assessment and Preventive Measures (F4E_D_2DT8EJ)

Last update: January 2020

 Controller(s) of data processing operation (Article 3 	າ (Article 31.1(ຄ	pperation (Article 31	processing	of data	Controller(s	1)
---	-------------------	-----------------------	------------	---------	--------------	----

- Controller: Hans Jahreiss, Senior Manager responsible for H&S.
 - o Unit / Department responsible for the processing activity: H&S Coordinator
 - o Contact: h&sdataprotection@f4e.europa.eu
- Data Protection Officer (DPO): <u>DataProtectionOfficer@f4e.europa.eu</u>

2) Who is actually conducting the processing? (Article 31.1(a))
The data is processed by F4E H&S Coordinator itself
The data is processed by a third party (e.g. contractor) (Art. 29 – Processor) :

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.

Data 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 Risk Assessment and Preventive Measures (<u>F4E D 2DT8EJ</u>) is the main process of the H&S Management System. In order to properly assess the risks to which staff

members are exposed at F4E and prescribe the adequate relevant preventive and control measures, it is necessary to process certain personal data of the F4E Staff.

The processing will take place using a dedicated IT tool, which shall be filled by the H&S Coordinator according to the information (tasks carried out, risks faced & working conditions) provided by Middle Managers and F4E Staff. The individual Risk Assessments of F4E Staff shall be available to the H&S Coordinator, the relevant Middle Manager and the concerned staff member.

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)	
- F4E Health & Safety Policy (F4E_D_282GG4), in particular Article 6 thereof. (b) compliance with a <i>specific</i> legal obligation for F4E to process personal data	
(d) Data subject has given consent (ex ante, freely given, specific, informed and unambiguous consent)	

F4E_D_ Page 2/5

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

Whose personal data is being processed?

Every F4E staff member and seconded national expert shall have an individual Risk Assessment carried out.

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:

All F4E Staff shall have an <u>individual Risk Assessment</u> performed, which shall contain the following personal data in accordance with the model Risk Assessment contained in the IT Tool:

 Name of the staff member; unit and/or department to which the staff member belongs; tasks carried out by the staff member; H&S-related trainings undertaken; location where the staff member performs his/her tasks.

(b) Sensitive personal data (Article 10):

In the event the Medical Advisor communicates to the H&S Coordinator the need of implementing certain preventive measures for one staff member, the <u>individual Risk Assessment</u> of the concerned staff member shall be updated accordingly.

The Medical Advisor shall not communicate the specific medical condition that led to the need of implementing certain preventive measures, however by communicationg the measures, the H&S Coordinator could deduct the medical condition that led to them.

e.g. Medical Advisor informs the H&S Coordinator that the staff member X cannot work in heights of more than 5 meters (Risk Assessment needs to be updated with the preventive measure 'Avoid working in heights of more than 5 meters) – H&S Coordinator can deduct that the staff member X suffers from vertigo.

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:

- Senior Manager responsible for H&S
- H&S Coordinator
- Middle Manager of the concerned staff member

F4E_D_ Page 3/5

- Medical Advisor
- IDM Manager, if necessary for support
- ICT officer responsible for the development and maintenance of the IT Tool

Also, only if appropriate and necessary for monitoring or inspection tasks, access may be given to: Head of Admin. (Process Owner), 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:				
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.

F4E_D_ Page 4/5

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.

Once a staff member leaves F4E, his/her individual Risk Assessment shall be stored for a period of 20 years and shall no longer be available in the IT Tool. This retention period responds to:

- · Individual Risk Assessments are a unique source of evidence and information in case of future claims made by a former staff member.
- There is often a long period between exposure and onset of ill health of the staff member.

In case of radiation exposed workers, personal data shall be kept for a period of 30 years in accordance with Council Directive 2013/59/EURATOM of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation.

11) Information/Transparency (Article 14-15)

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

A Privacy notice shall be issued and available for F4E Staff on F4E Net.

F4E_D_ Page 5/5