

RECORD
of processing activity¹
according to Article 31 Regulation 2018/1725²

NAME of data processing³:

Processing of personal data regarding COVID-19 cases

Last update: March 2021

| |
|---|
| 1) Controller(s)⁴ of data processing operation (Article 31.1(a)) |
| <ul style="list-style-type: none"> • Controller: Organisational entity of Fusion for Energy (F4E) <ul style="list-style-type: none"> ○ Unit / Department responsible⁵ for the processing activity: Administration Department ○ 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))⁶ |
| <p>The data is processed by F4E (responsible unit) itself <input checked="" type="checkbox"/></p> <hr/> <p>The data is processed by a third party (e.g. contractor) (Art. 29 – Processor) : <input checked="" type="checkbox"/></p> <p>Contact point at external third party (e.g. Privacy/Data Protection Officer):</p> <p>Gabinete SME Contact Point: dpo@gsmeep.com</p> <p>Gabinete SME Processor's Privacy Statement: https://www.gsmeep.com/es/aviso-legal/</p> |

¹ Please consult the relevant **EDPS guideline** in your sector, if it exists: https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en

² 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.

³ **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.

⁴ In case of more than one controller, see Article 28.

⁵ This is the unit that decides that the processing takes place and why.

⁶ 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.

The objective of the processing of personal data is to guarantee the continuity of the service in case of a suspected / confirmed COVID-19 case within the organisation, as well as ensure public health and protect F4E staff and externals by limiting the spread of the COVID-19.

"Externals" mean all persons working for F4E at F4E premises whose relationship with F4E is not governed by the Staff Regulations / CEOS staff (eg. Temporary agency workers, contractors staff, SNEs, trainees, etc.) who have access to F4E premises at any of its locations, work on site, are in physical contact with F4E staff).

The general principles of necessity and proportionality still apply when F4E exercises its duty of care for staff. F4E is accountable for necessity and proportionality and limits its processing to what is necessary.

Management of COVID-19 cases

According to the protocol for the management of COVID-19 cases (F4E_D_2L9MWP), F4E staff and externals are requested to inform the F4E Medical Advisor of their COVID-19 related symptoms or diagnose. The Medical Advisor will collect the necessary health data from the data subject (e.g. symptoms, specific health conditions, test results) in order to provide adequate medical advice and recommend appropriate H&S measures. The concerned staff member or external will also inform the Medical Advisor about any close contact with other F4E employees so that they can be duly informed.

In case the concerned staff member or external was in close contact with other F4E employees prior to the start of the symptoms or positive diagnose, the Medical Advisor will communicate the close contacts they must remain at home and inform the health authorities about their situation (if the concerned staff member or external has already been tested positive) or wait until the outcome of the test (if the concerned staff member or external has COVID-19 symptoms).

In particular, the Medical Advisor will email those F4E staff members and externals who have had contact with the person tested positive or with COVID-19 symptoms, requesting them to continue / arrange teleworking and contact the health authorities. Close contacts will inform their line managers about the request from the Medical Advisor to work from home.

The H&S Coordinator will be informed of the work-related close contacts in order to investigate any eventual breach of the H&S measures in place, check possible gaps in the measures, adopt new H&S measures or modify the existing ones.

The Medical Advisor will inform the H&S Coordinator of the number of COVID-19 cases in F4E without disclosing any names or medical data.

In the event a confirmed case does not / cannot provide sufficient or reliable information to the F4E Medical Advisor on work-related close contacts or presence in the premises, the Medical Advisor could disclose the name of the infected person **under the need to know principle** in order to trace possible close contacts and for public health reasons. In such case, the infected person will be previously informed that its name will be disclosed solely for the prevention and control of COVID-19 within the organisation. In accordance with art. 5.1 (a) and (e) of Regulation 2018/1725 the processing of data without consent is lawful where it is necessary for the performance of a task carried out in the **public interest** or to **protect the vital interests** of the data subject or **of another natural person**.

~~Exceptionally and only for public health reasons, the name of the infected person might have to be disclosed by the Medical Advisor under the need to know principle in order to implement additional H&S measures aiming to protect the health of other F4E colleagues. If necessary, such disclosure could be done even without the consent of the infected person.~~

In case the Medical Advisor decides so, CSU will collect and disclose him/her the names of F4E staff members and externals who have been in certain areas of F4E premises in order to trace those persons who might have had contact with an infected person. The data protection rules concerning the use of cameras within F4E buildings are contained in the RECORD of processing the video-surveillance system with a Closed Circuit Television (CCTV) (F4E_D_24ENL5).

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 10 February 2015 (2015/224 Euratom), O.J. L 37, 13.2.2015, 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 10 February 2015, in particular Article 10 thereof;
 - Protocol for the management of suspected and confirmed COVID-19 cases at F4E (F4E_D_2L9MWP)
- (b) compliance with a *specific* legal obligation for F4E to process personal data⁷
- (c) necessary for the performance of a contract with the data subject or to prepare such a contract (*state which is the contract as basis for the necessary processing*)
- (d) Data subject has given consent (ex ante, freely given, specific, informed and unambiguous consent)

Describe how consent will be collected and where the relevant proof of consent will be stored

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?

⁷ 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.

F4E staff members and externals

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 of the staff members or externals with COVID-19 symptoms or tested positive, unit / team, place of employment, date of presence and exact location within F4E premises and name/s of the colleagues in close contact prior to the symptoms or diagnose.

(b) **Sensitive personal data** (Article 10)

COVID-19 symptoms, positive diagnose by an external doctor, current health conditions or pathologies.

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:

Medical data:

- F4E Medical Advisor (Gabinete SME)
- F4E Nurse (Gabinete SME), who belongs to F4E’s medical service and provides support to the Medical Advisor

Administrative data:

- F4E Medical Advisor,
- F4E Nurse,
- H&S Coordinator, when informed of work-related close contacts
- Line Manager of the staff member in close contact with a confirmed / suspected case and requested to work from home,
- HoU/responsible officer(s) in Corporate Service Unit (CSU), Security Officer, when requested to trace the presence of staff members or externals in the premises,
- 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., Head of the Legal Service Unit and/or responsible Legal Officer, F4E Data Protection Officer and Anti-Fraud & Ethics Officer, 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:

F4E may be asked to disclose personal data to those competent national authorities, which have to process them in line with the applicable national legislation, i.e. 6(1)(e) + 9(2)(i) GDPR. Disclosures is justified under Article 9(1)(a) of Reg. 2018/1725. While all European Union Institutions (EUIs) themselves are entitled to take some measures to protect their staff, they have to stay within the remit of their role as employers. This means that they should not try take over tasks that are properly in the remit of the competent national public health authorities.

If personnel are or have been present at the ITER Site in Cadarache, France, in order to coordinate the contractors' efforts in line with the French Government recommendations, F4E may - out of urgency and under exceptional circumstances - need for public health reasons transfer personal data to the ITER IO, who is in direct contract with French national authorities: IO Data Protection Guidelines (ITER_IDM_UXG6V6) and IO SHS Data Protection Guidelines (ITER_IDM_WT7JUL).

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

Reference: ITER_IDM_UXG6V6; ITER_IDM_WT7JUL

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.

F4E will keep the personal data processed for no longer than and for what the purposes described in section 3 require. F4E will delete the data once no longer necessary and when the situation of the COVID-19 pandemic allows so, unless it is required to keep the data further for reasons of public health protection.

11) Information/Transparency (Article 14-15)

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

A Privacy Notice is published in F4E intranet and on the external website of F4E.