PRIVACY NOTICE ON PERSONAL DATA PROTECTION REGARDING ACCESS CONTROL

The objective of this Notice is to inform you about the collection and processing of your personal data in line with the applicable Data Protection Regulation 2018/1725[1].

TABLE OF CONTENT

1. Why does F4E process my personal data? Whose data is processed?

The access control system in Fusion for Energy Barcelona has been put in place only for security and safety purposes (in order to know who is in the building or in the sensitive areas at any time). This access control is managed through the AEOS Enterprise System from NEDAP.

The data subjects receive an access card in order to be identified at any time.

A) For Officials, temporary agents, contract agents, SNEs, interims:
1) Data is first provided by HR through an email sent to Security Office and Security guards: personal number (only for Officials, temporary agents, contract agents), first name, last name, contract type, department, unit, taking up duties date, place of employment.
2) On the day of taking up duties, Security Guards check the ID or passport of the newcomer. They then fill in the personal data mentioned in point 1) above in the AEOS System.
3) The Security Officer or Security Gards take a picture of the newcomer and upload it in the AEOS System. Once all the personal data is registered in the system, the access card is printed by the Security Guards and given to the newcomer.

B) Contractors, trainees:
1) Data is first provided by F4E staff responsible for the contract/trainee through an email sent to Security Office and Security guards or through a user account creation ticket (ITSM): Company name (in case of contractor), first name, last name, contract type, department, unit, taking up duties date and end of contract date, place of employment.
2) On the day of taking up duties, Security Guards check the ID or passport of the newcomer. They then fill in the personal data mentioned in point 1) above in the AEOS System.
3) The Security Officer or Security Gards take a picture of the newcomer and upload it in the AEOS System. Once all the personal data is registered in the system, the access card is printed by the Security Guards and given to the newcomer.

C) Visitors:
1) Data is first provided by F4E staff responsible for the visit through an email sent to Security Office and Security guards: Company name, first name, last name, start and end date of the visit, floor where meeting is taking place, ID number.
2) On the day of the visit, Security Guards check the ID or passport of the vistor. They then fill in the personal data mentioned in point 1) above in the AEOS System. Moreover for additional Health and safety measures the email address and the telephone number might be requested.
3) Once all the personal data is registered in the system, the access card is given by the Security Guards to the visitor.

 Entrance to/exit from F4E premises:
Entrance/exit is granted only through monitored access points and is subject to authorisation of the F4E's Security Office. People are asked to badge clock-in/clock-out when entering/leaving the controlled areas, by using the personal access cards (a pocket-sized card with embedded integrated circuits) and communicate with a terminal via radio waves) in specific readers near the controlled areas, entrance of the building, entrance of each F4E floor.

 Entrance to a Restricted area:
Entrance is granted only through monitored access points and is subject to authorisation of F4E'sSecurity office. People are asked to badge clock-in when entering the sensitive areas.
The rooms considered as sensitive areas are the following: Willy Brandt-CSU storage, dual use storage, facility management office supplies storage, IT storage (2C), inventory withdrawal room (2F), FM storage (2E), UPS room, IT storage (8G), ICT service desk, HR storage, finance storage, ICT rooms, and medical service room.

2. What is the justification for 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.

(b) compliance with a *specific* legal obligation for F4E to process personal data[1] ☐

(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) ☐

3. Which data is F4E processing?

(a) **General personal data:**

For staff: photo, access card number, personal number, first name, last name and contract type. Department, Unit, taking up duties date, place of employment The data is registered during the accreditation at the reception. The photo printed on the card is taken at that moment and is also sent to HR to upload it in eHR (see eHR data protection notification F4E_D_23PX3P). The card contains a unique number which is linked to the card holder.

For external staff, visitors, trainees and contractors: photo (only for external staff, trainees and contractors), the first name, last name, email address, telephone number and company name. Id/passport number and place of employment are registered in the AEOS System and in the F4E Security drive during the accreditation at the reception.

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

n/a

[1] 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.

4. Who has access to my data?

The following recipients have access to the personal data processed:

- Security guards
- CSU process ownerHead of CS Unit
- HR Officer responsible
- Head of HR Unit
- Head of Administration
- AEOS responsible of the F4E contract may be consulted regarding if deemed necessary by the Appointing Authority for a specified case
- Another person internally may be consulted regarding if deemed necessary by the Appointing Authority for a specified case
- IDM Manager, if necessary for support
- ICT Officer responsible for the dedicated tool, if necessary for technical support

Also, if appropriate and necessary, for monitoring or inspection tasks, access may be granted to:

- Director of F4E
- Head of the Legal Service Unit, and/or responsible Legal Officer
- F4E DPO and Anti-Fraud & Ethics Officer
- IAC / IDOC

5. How long does F4E store my data?

Every year, by the end of December y+1, access control data are deleted:

- For staff, contractors and trainees after the end of the contract, or when they leave F4E
- For visitors, after the end of the visit

6. Does F4E intend to transfer my data to third countries or International Organizations?

n/a

7. What are my rights in relation to my data and how can I exercise them?

You have the right to access your personal data, to correct any inaccurate or incomplete data, to request restriction or erasure, or to object to the processing, pursuant to Articles 14(3) and 17-23 of Regulation 2018/1725.

Any request to exercise one of those rights should be directed to the Controller (Osmar.naredo@f4e.europa.eu). Where you wish to exercise your rights in the context of one or several specific processing operations or files, please provide their description and reference(s) in your request.

Exceptions based on Article 25 of Regulation 2018/1725 may apply. In that case, the data subject shall be informed of the principal reasons for applying such restrictions.

8. Contact details of the Data Protection Officer

You may contact the Data Protection Officer (DPO) of F4E (DataProtectionOfficer@f4e.europa.eu) with regard to issues related to the processing of your personal data under Regulation 2018/1725.

9. Right of recourse

You have the right of recourse to the European Data Protection SupervisorEDPS@edps.europa.eu), if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by F4E.

(Based on template version F4E_D_2CJF8A v1.8)

[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.
This Privacy Notice is in line with Article 14 and 15 of that Regulation (Principle of Transparency).