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

NAME of data processing:

Management of user accounts in BA (Broader Approach) ICT applications

Last update: May 2021

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: Broader Approach Programme and Delivery Department o Contact: *badatacontroller@jt60sa.org* • 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):

[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.

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.

Creation, renewal of validity and deletion of user accounts in all Broader Approach ICT applications (Active Directory, Document Management System, Credit Management System, Trackers)

This procedure allows the creation of user accounts for BA ICT applications in order for users to be authenticated in the systems. Also it allows for the extension of validity and deletion of such created users.

For all applications, a periodic review of access rights on the user accounts is also performed.

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 *(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) ..... ☐

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

Whose personal data is being processed?

Any user (F4E staff and other users) authorised for accessing BA ICTapplications.

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:**
Identification data: first name, family name, company name, e-mail address, telephone number, displayed name (user name), F4E e-mail address, F4E fixed phone number, F4E mobile phone number, Office location and number.
(Not all data is collected and processed for all types of users (F4E staff, Externals, Contractor's staff, etc…)

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

None.

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:

- All authorised users of the database bound by the BA Agreement (e.g. Staff members of F4E , QST and Voluntary Contributors) can access personal data
- IDM (aka "DMS") Manager, if necessary for support
- ICT Officer responsible for the dedicated database, if necessary for technical support

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

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

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*: …*

COMMISSION IMPLEMENTING DECISION (EU) 2019/419

of 23 January 2019

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information

(notified under document C(2019) 304)

ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj

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.*
Ten years maximum after the termination of the work relationship.

11) Information/Transparency (Article 14-15) *Information shall be given in a concise, transparent and easily accessible form, using clear and plain language.*
See related Privacy Notice whose link is accessible from BA ICT applications.