[redacted]

Wojciech Rafał WIEWIÓROWSKI
European Data Protection Supervisor
Rue Wiertz 60
B-1047 Brussels - BELGIUM
e-mail: edps@edps.europa.eu

Sent by e-mail
Barcelona,

Reference: Case 2022-0471

Subject: Implementation of EDPS Decision concerning the Draft Administrative Arrangement for the Transfer of Personal Data between the European Joint Undertaking for ITER and the Development of Fusion Energy and the ITER International Fusion Energy Organization

Dear Mr Wiewiórowski,

Following the EDPS Decision authorising, subject to conditions, the use of the administrative arrangement between Fusion for Energy and the ITER International Fusion Energy Organization of 5 July 2021 and your letter of 2 May 2022 (case number 2022-0471), please find attached, as a result of the implementation of the above Decision, the *Agreement on the Transfer of Personal Data Between the European Joint Undertaking for ITER and the Development of Fusion Energy* (Fusion for Energy) *and the ITER International Fusion Energy Organization* together with the exchange of letters regarding Annex II of the Agreement.

I remain at your disposal to respond to any queries you may have.

Yours sincerely,

[redacted]

Signed electronically

Copy: *supervision@edps.europa.eu (EDPS);* [redacted]

Annex I: Agreement on the Transfer of Personal Data Between the European Joint Undertaking for ITER and the Development of Fusion Energy and the ITER International Fusion Energy Organization

Annex II: Exchange of Letters regarding Annex II of the Agreement on the Transfer of Personal Data between the European Joint Undertaking for ITER and the Development of Fusion Energy and the ITER International Fusion Energy Organization

LGA-2021-A-68 F4E_D_2SFNUQ

AGREEMENT ON THE TRANSFER OF PERSONAL DATA

BETWEEN

The European Joint Undertaking for ITER and the Development of Fusion Energy

AND

The ITER International Fusion Energy Organization

Hereinafter individually referred to as 'the Party' or collectively as "the Parties",

HAVING REGARD to the Agreement on the Establishment of the ITER International Fusion Energy Organization for the Joint Implementation of the ITER Project of 21 November 2006 between the European Atomic Energy Community (hereinafter “Euratom”), the Government of the People's Republic of China, the Government of the Republic of India, the Government of Japan, the Government of the Republic of Korea, the Government of the Russian Federation and the Government of the United States of America, and conferring the ITER Organization the legal capacity and status under international law (hereinafter “the ITER Agreement”);

HAVING REGARD to Council Decision of 27 March 2007 establishing the European Joint Undertaking for ITER and the Development of Fusion Energy (hereinafter “F4E”) and conferring advantages upon it (2007/198/Euratom);

HAVING REGARD to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, and in particular Article 48(3)(b) thereof;

HAVING REGARD to Data Protection Guidelines of the ITER International Fusion Energy Organization (hereinafter “IO”) (ITER_D_UXG6V6);

WHEREAS pursuant to the ITER Agreement, F4E is the EU body responsible for providing Euratom’s contribution to the ITER Project and IO is responsible, *inter alia*, for the coordination of the contributions of the ITER Members, including Euratom;

WHEREAS to ensure efficient international cooperation, the Parties, acting in accordance with their respective mandates, have signed, and will continue to sign, agreements and arrangements setting out the details of their cooperation in the implementation of the ITER Agreement, notably as regards the hosting of F4E staff on the ITER site;

WHEREAS to give effect to aforementioned agreements and arrangements, the Parties need to exchange personal data;

WHEREAS the Parties recognise the need, as defined by applicable laws, to safeguard individuals whose personal data are transferred and otherwise processed in the framework of their mutual cooperation by means of the appropriate safeguards specified in this Agreement;

WHEREAS the European Data Protection Supervisor authorised the Agreement on 5 July 2021 and the F4E Governing Board approved this Agreement on 10 December 2021.

HAVE AGREED AS FOLLOWS:

ARTICLE 1 – DEFINITIONS

For the purposes of this Agreement the following definitions apply:

a) **'personal data'** means any information relating to an identified or identifiable natural person ("data subject") within the scope of this Agreement; an identifiable natural person is one 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 of that natural person;
b) **'sensitive personal data'** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, operational personal data concerning health or concerning a natural person's sex life or sexual orientation;
c) **'applicable data protection law'** means for F4E all applicable legal acts governing the protection of personal data in the European Union (hereinafter "EU"), in particular Regulation (EU) 2018/1725 (hereinafter "EUDPR"); for IO this means all applicable rules and regulations put in place by the ITER Organization which relate to or impact on the processing of personal data;
d) **'transferring Party (data exporter)'** means the Party who transfers the personal data;
e) **'receiving Party (data importer)'** means the Party who agrees to receive personal data from the data exporter for further processing in accordance with this Agreement;
f) **'transfer of personal data'** means at least communicating, disclosing or otherwise making available personal data to the other Party, including access, disclosure, dissemination and transmission;
g) **'onward transfer'** for the purposes of the Agreement means transfer of personal data by the receiving Party to a controller, processor or other recipient in a third country or an international organisation ("third party");
h) **'sharing of personal data'** for the purposes of this Agreement means transfer of personal data by the receiving Party to other recipients within the receiving Party's organisation;
i) **'supervisory authority'** means an independent public authority which is established by law and responsible for monitoring the processing of personal data in a given jurisdiction, including, as regards F4E, the European Data Protection Supervisor (hereinafter "EDPS"), the supervisory authority of the EU institutions, bodies, offices and agencies;
j) **'controller'** means the Party or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data;
k) **'processor'** means the natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller;
l) **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated 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.

ARTICLE 2 – SUBJECT MATTER AND SCOPE

This Agreement applies to transfers of personal data between the Parties in the exercise of their respective responsibilities under agreements and arrangements concluded between the Parties in the implementation of the ITER Agreement following the entry into force of the present Agreement. The Parties agree to interpret data protection provisions of existing agreements and arrangements in light of the Agreement as regards data transfers and processing between the Parties. The Agreement shall be without prejudice to applicable data protection law.

ARTICLE 3 – PURPOSE OF THE PROCESSING

The purpose of the processing is to implement the Parties' rights and obligations pursuant to the agreements and arrangements referenced in Article 2 as further detailed in the Annex of this Agreement. The processing operations include the transfer of personal data between the Parties whether or not by automated means such as the collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

ARTICLE 4 – DATA PROTECTION PRINCIPLES AND SAFEGUARDS

With respect to the personal data subject to transfers covered by this Agreement, the Parties shall apply the following principles and safeguards in accordance with the applicable data protection law, internal policies and procedures.

a) Purpose limitation: The Parties shall limit transfers of personal data between the Parties as well as any further processing of such personal data by the Parties to what is strictly necessary for the purpose of implementation of the agreements and arrangements referenced under Art. 2 of the Agreement. Further processing by the Parties which is compatible with the original purpose set out in Article 2, such as, but not limited to further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for safety reasons in compliance with the applicable French laws, and subject to appropriate safeguards, is authorised. Further compatible use of the transferred data by the receiving Party shall be compatible with the original purpose, and shall be notified to the transferring body, which may oppose for specific reasons.

b) Data minimisation: The Parties shall transfer and process only personal data which are adequate, relevant, and not excessive in relation to the purpose set out in Article 2.

c) Accuracy: The transferring Party shall ensure that the personal data transferred is maintained accurate and, where necessary, kept up to date during the processing following the transfer, in coordination with the receiving Party. If a Party becomes aware that personal data it has transferred to, or received from, another Party is inaccurate, it shall notify the other Party without delay. The Parties shall erase or rectify inaccurate personal data without delay.

d) Storage limitation: The Parties shall ensure that personal data is kept in a form which permits identification of data subjects for no longer than necessary for the purpose set out in subparagraph a) and in any event no longer than the duration of the ITER Project.

e) Retention: The Parties will retain personal data for no longer than is necessary and appropriate for the purpose set out in subparagraph a) and in any event no longer than the duration of the ITER Project.

f) Integrity and confidentiality: The Parties shall take appropriate technical and organisational measures to protect personal data they receive against accidental or unlawful access, destruction, loss, alteration or unauthorised disclosure (e.g. encryption including in transit, pseudonymisation, marking information as personal data transferred from (the EEA) F4E, restricting who has access to personal data, providing secure storage of personal data, or implementing policies designed to ensure personal data are kept secure and confidential). The level of security of the measures shall be determined taking into consideration the risks to rights and freedoms of individuals, the state of the art and the related cost, but it cannot be lower than the level of protection required in accordance with the IT Security policy of the transferring Party. The Parties recognise that their respective IT Security Policies offer an equivalent level of protection. If the receiving Party becomes aware of a personal data breach, it will inform the transferring Party without delay, and, if feasible, not later than 48 hours after having become aware of it. The receiving Party shall use reasonable and appropriate means to remedy the personal data breach and minimise the potential adverse effects. Data subject shall be informed without delay by the transferring Party if a personal data breach results in high risks to their rights.

g) Transparency: The Parties shall provide information to the data subjects by means of a joint privacy statement indicating the identity and the contact details of the controller, the contact details of the data protection representatives of both Parties, the purposes of the processing, the categories of personal data concerned, the type of transactions, the categories of recipients of the personal data, intended transfer of personal data to a recipient in a third country, appropriate or suitable safeguards, the period for which the personal data will be stored, the data subject rights, how those rights can be exercised, relevant restrictions of data subject rights and available redress mechanisms. This privacy statement shall be published on the external websites of F4E and the ITER Organization. Upon request, the Parties shall provide data subjects with a confirmation as to whether their data have been transferred and on the particularities of the transfer. Individual information will be provided to data subjects by F4E in accordance with notification requirements and applicable exemptions and restrictions in Regulation (EU) 2018/1725 (as set forth in Articles 15, 16 and 25 of Regulation 2018/1725). The Parties will make available the relevant provisions of the Agreement providing for appropriate safeguards, considering also the need to protect sensitive or confidential information. Where necessary that data subjects know the content of the Agreement, at least a summary will be provided to them.

h) Accountability: Each Party may request the other Party to provide information on its compliance with this Agreement, notably as regards the application of the data protection safeguards set out in this Article. The Parties may provide information to their respective supervisory authorities regarding transfers and safeguards covered by this Agreement, respecting any conditions, which the other Party may have attached to such provision of information, notably as regards confidentiality.

i) Data subjects rights: The Parties shall take appropriate measures in accordance with the applicable data protection law and shall cooperate in their application to effectively protect the following data subject rights:

i. *Right of access by the data subject*: The data subject shall have the right to obtain confirmation as to whether or not personal data concerning him or her have been transferred under this Agreement and are being processed, and, where that is the case, access to the personal data, to specific information concerning the processing, including the purpose of the processing, the categories of personal data concerned, the recipients to whom personal data is disclosed, the envisaged storage period, the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing and redress possibilities as well as access and to the appropriate safeguards.
ii. *Right of information:* means a data subject's right to receive information on the processing of personal data relating to him or her in a concise, transparent, intelligible and easily accessible form.
iii. *Right of erasure*: means a data subject's right to have his or her personal data erased where the personal data are no longer necessary for the purposes for which they were collected or processed, and in any event no longer than for the duration of the ITER Project, or where the data have been unlawfully collected or processed.
iv. Right of rectification; means a data subject's right to have the data subject's inaccurate personal data corrected or completed without undue delay.
v. *Right to data portability*: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller under this Agreement, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, if necessary for objective reasons.
vi. *Right of objection:* means a data subject's right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, except in cases where there are compelling legitimate grounds for the processing that override the grounds put forward by the data subject or for the establishment, exercise or defence of legal claims.
vii. *Right not to be subject to automated decisions, including profiling:* means a data subject's right not to be subject to legal decisions being made concerning him or her based solely on automated processing.
viii. *Right to restriction of processing*: means a data subject's right to restrict the processing of the data subject's personal data where the personal data are inaccurate, where the processing is unlawful, where the personal data is no longer needed for the purposes for which they were collected or where the personal data cannot be deleted.

To exercise their rights as regards personal data transferred from F4E to the IO, data subjects shall address a request by email to the F4E Controller identified in the relevant privacy notice.
To exercise their rights as regards personal data transferred from IO to F4E, data subjects shall address a request by email to [data.protection@iter.org]. The transferring Party shall inform the data subject without delay, but at the latest within one month of receiving the request, on the action taken in response to the request or the decision not to take action. Any decision not to take action shall state the reasons and refer to the possibility to seek remedies in accordance with Article 5(3). The Parties may take appropriate steps, such as charging reasonable fees to cover administrative costs or declining to act on a request, where requests from data subject are manifestly unfounded, excessive or repetitive.

Internal rules of the Parties adopted in accordance with applicable data protection law may restrict data subject rights, provided such a restriction is a necessary and proportionate measure notably to safeguard public health, safety or security.

j) Onward transfer: The receiving Party shall not further transfer personal data, except:

i. to competent French authorities responsible for liaison with the IO on health, safety, and security-related matters (e.g. Labour Inspector, Nuclear Safety Regulator (ASN), High Fonctionnaire of Defense and Security (HFDS), representatives of the Ministries of Foreign Affairs, Interior, Defense, and Energy), subject to the GDPR[1], where required by the ITER Agreement or the Agreement between the Government of the French Republic and the ITER Organization, upon prior written authorisation by the transferring Party provided that the principle of purpose limitation is respected and the receiving third parties commit to respect the same data protection principles and safeguards as included in the Agreement in the case of, but not limited to, background checks; or

ii. to authorise third parties listed in Annex II, such as Contractors of the receiving Party, where necessary for carrying out tasks on behalf of the receiving Party for the purpose of implementing the agreements and arrangements referenced in Article 2 of the Agreement, on condition that the principle of purpose limitation is respected and such third parties which are not subject to the GDPR commit to respect the data protection principles and safeguards of this Agreement; or

iii. if necessary for important reasons of public interest or for the vital interest of the data subject, as recognised by applicable data protection law, including, but not limited to health, safety or security matters, or for safeguarding against and the prevention of threats to public security, and the receiving Party notifies the transferring Party prior to the sharing of personal data; should prior notification not be possible, e.g. because it impinges on confidentiality obligations provided for by law, the receiving Party shall at least provide specific information as soon as possible after the onward transfer or sharing took place; the transferring Party should keep a record of such notifications from the receiving Party and provide its supervisory authority with this information upon request; if notification after the sharing is not possible, general information on the type of requests received over a specified period of time, including information about the categories of data requested, the requesting body and the legal basis for disclosure, should be provided to the transferring public body once a year.

ARTICLE 5 – OVERSIGHT MECHANISM

1. Each Party shall nominate a data protection representative who shall regularly monitor the application of the Agreement within his or her organisation, and assess whether the policies, procedures and practices continue to meet the needs of this Agreement, also in light of new applicable legislation, and/or whether such policies, procedures and practices or – alternatively – this Agreement, need to be amended to give full effect to each other, notably as regards the effective application of the safeguards set out in this Agreement.

2. A Party may request the other Party to conduct a review. The Parties shall respond to each other's enquiries concerning the effective implementation of the safeguards set out in the Agreement. Each Party conducting a review shall communicate the results of the

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

checks to the other and to the F4E-IO Transfer Monitoring Board referred to in paragraph 3. The parties shall inform each other without delay if they are unable to effectively implement the safeguards in the Agreement for any reason.

3. The Heads of Legal Affairs of the Parties, the internal auditor of IO and the data protection officer of F4E form the F4E-IO Transfer Monitoring Board (hereinafter the "Board") which shall oversee the implementation of the present Agreement. The Board shall work independently and free from instructions. It shall be provided with sufficient human, technical and financial resources. The receiving party is bound by the decisions of the Board.

ARTICLE 6 – REMEDIES

1. A data subject who considers that the processing under this Agreement of personal data related to him or her infringes the data protection principles or safeguards set forth in this Agreement, and who has not received a satisfactory response or resolution by first referring the issue to the representatives nominated under Art. 5(1), may lodge a complaint with the Board addressed to one of the data protection representatives within one month. The Board shall seek to resolve the complaint independently and impartially within two months from receiving the complaint. In case a data protection representative considers him or herself in a conflict of interest which could impair his or her independence in a case, he or she shall be substituted by another expert appointed by the Board. A complaint to the Board is, without prejudice to a data subject's right, under the applicable data protection law. The Board, by common agreement, may decide to request the opinion of an independent external expert.

2. Notwithstanding the right to lodge a complaint to the Board, a data subject who considers that the processing under this Agreement of personal data related to him or her infringes the data protection principles or safeguards set forth in this Agreement has the right to seek remedies in accordance with the applicable data protection law:

    a) Data subjects may lodge a complaint with F4E as a controller, with the EDPS as data protection supervisory authority and have also the right to effective judicial remedy before the Court of Justice of the European Union.
    b) In relation to the processing carried out by the ITER Organization, data subjects may lodge a complaint with the ITER Organization data protection representative referred to in Article 5(1), and then may seek redress by lodging a complaint under Article 5(3) of the Agreement and have the right to seek alternative dispute settlement before the Permanent Court of Arbitration whose decisions are binding.

    The Parties shall commit to handle complaints in a timely manner, to inform each other about the outcome and to settle disputes or claims in a timely fashion. The Parties can commit to be liable for damages through unlawful processing of the personal data if that is established by the independent review. In the event a data subject seeks remedies, the Parties shall cooperate to resolve the matter. If the transferring Party is of the view that the receiving Party has not acted in accordance with this Agreement, the transferring Party may suspend the transfer of personal data to the receiving Party until the issue is satisfactorily addressed by the receiving Party.

ARTICLE 7 - AMENDMENTS AND TERMINATION

1. The Parties may amend the Agreement by mutual agreement in writing based on recommendations by the Board.

2. A Party shall be entitled to terminate this Agreement at 3 months' written notice to the other Party. By the date the termination becomes effective, the receiving Party shall cease processing and shall destroy all personal data received from the transferring Party. The transferring Party may authorise the receiving Party to continue processing personal data already transferred in compliance with the principles and safeguards in this Agreement for a period set in advance. In this case, the receiving Party shall destroy the personal data by the date the period expires.

ARTICLE 8 – PRIVILEGES AND IMMUNITIES

This Agreement shall not be construed as a renunciation, whether explicit or implicit, on the part of the ITER Organization of the privileges and immunities granted under the Agreement on the Privileges and Immunities of the ITER International Fusion Energy Organization for the Joint Implementation of the ITER Project of 21 November 2006.

ARTICLE 9 – SETTLEMENT OF DISPUTE

Any dispute between the Parties under the Agreement shall be settled in accordance with Article 25 of the ITER Agreement.

ARTICLE 10 – ENTRY INTO FORCE

This Agreement shall enter into force upon signature by both Parties on the date the last signature.

Done in two originals in English.

For the ITER Organization:

Mr Bernard BIGOT

Director-General

[redacted]GOT
neral

Digitally signed by Bernard BIGOT
Date: 2021.12.17 11:51:23 +01'00'

Signature:

For Fusion for Energy:

M Digitally signed by: Johannes Schwemmer
Location: Barcelona
Di Date: 16/12/2021 23:11:57

D [redacted]
Director

FUSION FOR ENERGY

Signature:

ANNEX I:
LIST OF PROCESSING OPERATIONS REQUIRING TRANSFERS OF PERSONAL DATA FROM FUSION FOR ENERGY (F4E) TO ITER ORGANIZATION (IO)

TYPE OF PROCESSING	PURPOSE	TYPE OF PERSONAL DATA
Contract Implementation (excluding processing during claims assessment)	As a rule, transfer of the personal data to IO occurs in anonymised format (i.e. after having removed all personal data). In certain cases, upon explicit request by IO (e.g. for auditing purposes or nuclear safety inspections), the transfer may include personal data.	• Name, date of birth, gender, personal numbers or other identifiers of general application, nationality, contact details (company and department, postal address, country of residence, business telephone number, mobile telephone number, fax number, e-mail address), signature; • Professional and education information: CV's – work experience/employment history, education, training and academic background, personal skills and competences (language, technical skills); • Functions, working hours, working place, salaries, time sheets, and other information or personal data provided under the Contract with the purpose of substantiating cost and performance elements; • Bank account
Procurement and Grant Procedures	Personal data may be transferred to IO staff during the evaluation process of tenders/applications.	• Name, date of birth, gender, nationality, function, contact details (company and department, postal address, country of residence, business telephone number, mobile telephone number, fax number, e-mail and internet address, and signature); • Certificates for social security contributions and taxes paid; • Extracts from judicial records; • Bank account; • Passport/ID number; VAT number; membership in a trade or professional organisation;

		• Professional and education information: CV's – work experience/employment history, education, training and academic background, personal skills and competences (language, technical skills); • Declaration of honour that the tenderer/applicant is not in one of the exclusion situation referred to in the Financial Regulation (in relation with F4E's Implementing Rules); • Other personal data contained in the tender/application (credentials).
Procurement Arrangements and Task Agreements with IO	The Personal data of F4E staff is transferred to ITER IO upon ITER IO's request in the framework of the negotiation and implementation of the Procurement Arrangements and Task Agreements.	• Name • Function • Business telephone number • Business e-mail address
ITER Site access	The personal data processed are those necessary to obtain a badge to access the ITER site.	The data processed for a badge is the following: • Copy of valid ID; • Title of meeting or tasks on site and contact person on site; • Site entrances, buildings or rooms needed; • Personal data: name, surname, maiden name, sex, date of birth, birth country, nationality, birth department (only for French citizens), signature; • Referred company (company inviting the requester to the visit); • Start and end date of the visit. SIPSI (Système d'information sur les prestations de service internationales), only if posted worker.
Provision of ICT user support and of ICT equipment	Personal data needed to assign ICT equipment and to handle support requests.	First name, family name, displayed name, e-mail address, phone number (fixed and/or mobile), office location and

	Personal data that may be stored on IO computers.	number, start date of contract, contract type, end date of contract. No sensitive personal data. Note: During the processing of end-user's requests and reported incidents, the end-user may share with the ICT Service Desk technician some personal data like the one that may be contained in a document or e-mail body. Such Personal Data may in principle belong to any category, it will strictly be used with the goal to give support to the user and in any case the Service Desk technicians will never specifically ask for accessing any such information.
Account creation/ IO email address creation	Personal data needed to create the account and the mailbox. Personal data sent or received via IO email address.	First name, family name, displayed name, e-mail address, phone number (fixed and/or mobile), office location and number, start date of contract, contract type, end date of contract. No sensitive personal data.
IO access to the F4E Deviation Amendment and Contract Changes Platform (DACC)	Personal data may be transferred regarding deviation amendments and contract changes.	Names, job positions and contact details (e.g. phone number) of the legal representatives of the contractors, of the employees of the contractors and of F4E Staff members.
Claim assessment process under F4E works contracts	Personal data could exceptionally be transferred in the claim assessment procedure, in the framework of the implementation of F4E contracts by Staff of IO.	• Name, date of birth, gender, personal numbers or other identifiers of general application, nationality, contact details (company and department, postal address, country of residence, business telephone number, mobile telephone number, fax number, e-mail address and internet address) and signature;

		• Functions, working hours, working place, salaries, time sheets, other information or personal data provided under the works contracts.
Claim assessment process (Non-FIDIC contracts)	Personal data could exceptionally be transferred in the claim assessment procedure, in the framework of the implementation of F4E contracts by Staff of IO.	• Name, date of birth, gender, personal numbers or other identifiers of general application, nationality, contact details (company and department, postal address, country of residence, business telephone number, mobile telephone number, fax number, e-mail address and internet address) and signature; • Functions, working hours, working place, salaries, time sheets, other information or personal data provided under the works contracts.
Schedule submission to IO	Personal data concerning F4E Staff member who owns a schedule.	Name of the person who owns a schedule (F4E Staff member).
Risk register submission to IO	Personal data concerning the risk owner and of the risk action owner.	Name and F4E e-mail address of the risk owner and of the risk action owner.
Primavera access	Personal data requested by PM Department (both internal and external staff) to have access to IO Primavera P6.	Name and F4E e-mail address.
Request of JIRA account	Personal data may be transferred by JIRA, tool used by IO to track issues raised by users.	Name and e-mail addresses of anyone raising an issue (it could be both external or F4E staff).
Communication with IO (e.g. via email / paper letters)	Personal data exchange with IO.	All the information exchanged with IO, which may include personal data.
Management of Covid-19 cases	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,	**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

	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.	within F4E premises and name/s of the colleagues in close contact prior to the symptoms or diagnose. **Sensitive personal data:** COVID-19 symptoms, positive diagnose by an external doctor, current health conditions or pathologies.

ANNEX II: LIST OF AUTHORISED THIRD PARTIES

(to be established by exchange of letters)

Route de Vinon-sur-Verdon - CS 90 046 - 13067 St Paul Lez Durance Cedex – France

Director-General

Mr. Pietro BARRABASCHI
Director
Fusion for Energy

By email only

Saint-Paul-lez-Durance, 28 July 2022

Reference: DG/2022/OUT/0233 (7ZQM44)

Subject: List of Annex II of the Agreement on the Transfer of Personal Data Between the IO and F4E

Dear Pietro,

Following the signature of the Agreement on the Transfer of Personal Data Between The European Joint Undertaking for ITER and the Development of Fusion Energy And The ITER International Fusion Energy Organization, referenced LGA-2021-A-68 / F4E_D_2SFNUQ, entered into force on 17 December 2021, and as agreed, I am writing to you to provide the list of authorised third parties that shall be part of Annex II to the Agreement:

The authorized third parties/entities identified by the IO which could be concerned by onward transfer, meaning receive personal data from F4E while being in a third country or in an international organization are the following:

1. Microsoft Azure

If we identify other entities later, we will inform you to keep this list updated.

Yours sincerely,

[redacted]
Eisuke TADA
Director-General, *interim*

Tada Eisuke
2022.07.29
02:41:52
+02'00'

Eisuke Tada
Director-General, *interim*
ITER Organization

Copy:
[redacted]

FUSION FOR ENERGY

idm@F4E UID / VERSION
2XBMEG / 1.0

VERSION CREATED ON / STATUS
24 October 2022 / Approved

EXTERNAL REFERENCE

F4E Document

List of Annex II of the Agreement on the Transfer of Personal Data Between the IO and F4E-Formal F4E Reply

Following the signature of the Agreement on the Transfer of Personal Data Between The European Joint Undertaking for ITER and the Development of Fusion Energy And The ITER International Fusion Energy Organization, referenced LGA-2021-A-68 /F4E_D_2SFNUQ, entered into force on 17 December 2021;

Exchange of letters (2/2) to agree on Annex II "List of Authorised 3rd Parties" to the Agreement on the Transfer of Personal Data Between the IO and F4E)

Approval Process			
	Name	*Action*	*Affiliation*
Author	[redacted]	**24 October 2022:signed**	**ADM**
Co-Authors			
Reviewers			
Approver	[redacted]	**26 October 2022:approved**	**ITERP**
RO	[redacted]		
Read Access	**LG: DP Team, LG: Trainee, AD: IDM_F4E, project administrator, RO**		

Original Document MD5#: 0BE7746E18B6A072070A4A101A2605D5

** Performed by ** Delegated Reviewer*

Change Log			
List of Annex II of the Agreement on the Transfer of Personal Data Between the IO and F4E-Formal F4E Reply (2XBMEG)			
Version	***Latest Status***	***Issue Date***	***Description of Change***
v0.0	In Work	24 October 2022	
v1.0	Approved	24 October 2022	-

FUSION FOR ENERGY

Mr Pietro BARABASCHI
Director-General
ITER Organization
Route de Vinon-sur-Verdon
13067 St Paul Lez Durance Cedex - FRANCE

Created: Barcelona, 24 October 2022

By email only

Subject: List of Annex II of the Agreement on the Transfer of Personal Data Between the IO and F4E

Dear Pietro,

I have the honour to acknowledge receipt of the letter with the Reference: DG/2022/OUT/0233 (7ZQM44) of 28 July 2022 from Mr. Eisuke Tada, in his capacity as interim Director-General of the ITER Organization, which reads as follows:

'Following the signature of the Agreement on the Transfer of Personal Data Between The European Joint Undertaking for ITER and the Development of Fusion Energy And The ITER International Fusion Energy Organization, referenced LGA-2021-A-68 / F4E_D_2SFNUQ, entered into force on 17 December 2021, and as agreed, I am writing to you to provide the list of authorised third parties that shall be part of Annex II to the Agreement:

The authorized third parties/entities identified by the IO which could be concerned by onward transfer, meaning receive personal data from F4E while being in a third country or in an international organization are the following:

1. Microsoft Azure

If we identify other entities later, we will inform you to keep this list updated.'

I have the honour to inform you that, as a result of the clarifications provided by your services over the past months and the confirmation that personal data transferred from F4E to the ITER IO is only transferred onwards to the entity listed in your letter, Fusion for Energy is in agreement with the contents of your letter.

Please accept the assurance of my highest consideration.

Signed electronically in IDM,
approval date on cover-page

For Fusion for Energy
Jean-Marc Filhol
Director *ad interim*

Copy: [redacted]