EDPS Decision authorising, subject to conditions, the use of the administrative arrangement between the European Joint Undertaking for ITER and the Development of Fusion Energy and the ITER International Fusion Energy Organization - (Case 2021-0505)

1. INTRODUCTION

1.1. This decision concerns the authorisation of the Administrative Arrangement (AA) to be concluded between the European Joint Undertaking for ITER and the Development of Fusion Energy ('F4E') and the ITER International Fusion Energy Organization ('ITER') in the context of the implementation of the ITER Agreement[1] , notably as regards the hosting of F4E staff on the ITER site.

1.2. The EDPS issues this Opinion in accordance with Article 57(1)(n) and Article 58(3) (f) of Regulation (EU) 2018/1725[2] ('the Regulation').

1.3. This Decision is addressed to F4E.

2. BACKGROUND INFORMATION

2.1. On 6 April 2021, F4E submitted a request for informal consultation regarding the Administrative Arrangement (AA) to be concluded between F4E and ITER in the context of the implementation of the ITER Agreement, notably as regards the hosting of F4E staff on the ITER site. A draft version of the AA was attached and the informal advice of the EDPS was requested on the document.

2.2. On 6 May 2021 F4E informed the EDPS that the negotiations with ITER had been concluded and sent an up-dated version of the AA requesting formal authorization of the EDPS under Article 48(3) of the Regulation.

---

1 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 OJ L 358, 16.12.2006.

2 Regulation (EU) 2018/1725 of the European Parliament and 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, OJ, L 295, 21.11.2018, pp. 39-98.

2.3. Pursuant to Council Decision 2007/198/Euratom establishing F4E[3] and the ITER Agreement, the task of the joint undertaking is to provide the contribution of the European Atomic Energy Community (Euratom) to the ITER. This task requires an efficient cooperation between F4E and ITER acting in accordance with their mandates as defined by the applicable legislations. The contribution of F4E includes among others overseeing the preparation of the ITER project site, providing financial contribution, components, equipment, materials and human resources to ITER, procurement management, quality assurance procedures, preparing and coordinating scientific and technological research and development with the ITER Organisation or to carrying out other activities in line with the ITER Agreement. In this context, the parties need to set out the details of their cooperation in the implementation of the ITER Agreement in further international agreements, involving also exchange of personal data.

2.4. F4E and ITER have negotiated three international agreements, notably regulating issues pertaining to ITER's role as host of the site and detailed technical arrangements regarding F4E's contribution. The international agreements set out that 'transfers and other processing of personal data shall be subject to the F4E-ITER Data Protection Administrative Arrangement'. On the basis of the draft AA F4E and ITER plan to exchange personal data under their respective mandates, in the context of hosting F4E staff on the ITER site, without specifying further the categories of personal data at stake.

3. LEGAL ANALYSIS

3.1. Transfers of personal data to recipients outside the European Union ('the Union') may generate additional risks for data subjects, as the applicable data protection rules in the recipient's jurisdiction may be less protective than inside the Union.

3.2. Regulation (EU) 2018/1725 (EUDPR) permits transfers of personal data to third countries or international organizations subject to a two-steps test: first, the processing must be lawful and second, there must be a suitable transfer tool in place. The F4E transferring personal data to third countries or to an international organisation, in addition to complying with Chapter V of the Regulation, must also meet the conditions of the substantive provisions of the Regulation applicable to any processing. In particular, each processing activity must comply with the data protection principles enshrined in Article 4 of the Regulation, be lawful in accordance with Article 5 of the Regulation and comply with Article 10 of the Regulation in case of processing of special categories of personal data.

[3] 2007/198/Euratom: Council Decision of 27 March 2007 establishing the European Joint Undertaking for ITER and the Development of Fusion Energy and conferring advantages upon it OJ L 90, 30.3.2007

3.3. Chapter V of the Regulation provides for specific mechanisms and conditions for transfers of personal data by EU institutions and bodies, to a third country or an international organisation. These mechanisms and conditions aim to ensure that the level of protection of natural persons guaranteed by the EU data protection legislation is not undermined when their personal data is transferred outside the EU.

3.4. The first mechanism is the adoption by the European Commission of an adequacy decision recognizing that the third country or an international organisation provides a standard with regard to data protection that is essentially equivalent to that within the EU.[4] However, until now the European Commission has not adopted any adequacy decision concerning the ITER.

3.5. In the absence of an adequacy decision, a transfer can take place through the provision of appropriate safeguards and on the condition that enforceable rights and effective legal remedies are available for individuals[5]. A legally binding and enforceable instrument between public authorities or bodies may provide for such appropriate safeguards.[6] Such safeguards may also be provided, subject to the authorisation from the EDPS, by inserting provisions into administrative arrangements between public authorities and bodies which include enforceable and effective data subject rights.[7]

3.6. The EDPB Guidelines on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679[8] for transfers of personal data between EEA and non-EEA public authorities and bodies (the 'EDPB guidelines')[9] set a list of minimum safeguards to be included in an administrative arrangement (AA). The criteria for appropriate safeguards under Article 48(3)(b) of the Regulation are the same as under Article 46(3)(b) of Regulation 2016/679. Therefore, the EDPB guidelines are relevant for AAs concluded between European institutions, bodies, offices and agencies ('EUIs') and public authorities in third countries, such as the present draft AA.

3.7. Based on the EDPB guidelines, the draft AA should include a series of guarantees. The EDPS is of the opinion that the draft AA provides sufficient guarantees as regards the definition of most key concepts, the principles of data accuracy and data

4 Article 47 of the Regulation.
5 Article 48(1) of the Regulation.
6 Article 48 (2) (a) of the Regulation.
7 Article 48 (3) (b) of the Regulation.
8 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 (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
9 EDPB Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.

minimisation and the termination clause. However, the draft AA does not meet all requirements of the following guarantees, as explained below.

Definitions

3.8. The draft AA already provides for the definition of key concepts[10] of the EU data protection legal framework (see Article 1 of the draft AA). If processed, the AA should be complemented with a definition of sensitive data in line with the Regulation. In line with recital 63 of the Regulation, the definition of onward transfers should be completed with recipients in other international organisations. Finally, a definition concerning "data sharing" for disclosures of personal data with other recipients within ITER should be added.

Purpose and scope

3.9. The draft AA shall define its purpose and scope in an explicit and specific way. In addition, it needs to clearly state the categories of personal data affected and the type of processing of the personal data, which is transferred and processed under the arrangement.

3.10. The EDPS notes that it is not sufficient to include these details in the data protection notice. The AA shall clearly provide for the specific types of personal data transferred, categories of data subjects affected, the type of processing of the personal data and the specific purposes for which that personal data is processed and transferred. The EDPS understands that the draft AA covers transfers of personal data in the context of three international agreements with ITER. Depending on the details:

i. one AA may cover all three international agreements, clearly detailing in separate annexes the transferred personal data, data subjects and purposes for each of the three international agreements. This option is in principle acceptable if the processing is not complex or large scale and does not concern sensitive data of vulnerable individuals.

or

ii. three AAs can be concluded (detailing in annex the transferred personal data, data subjects and purposes for the respective international agreement). This second option would help to ensure more clarity, legal certainty and more protection for data subjects in case of complex transfers and processing operations.

[10] EDPB Guidelines paragraph 16

3.11. The current wording of Article 3 of the draft AA does not provide for a specific, exhaustive set of purposes. It sets out that the purpose of the AA is 'to implement the rights and obligations pursuant to the agreements and arrangements referenced in Article 2 of this AA'. Article 2 refers 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 before the entry into force of the present Administrative Arrangement. It is not clear whether the AA refers to rights and obligations of the Parties or those of data subjects, but in any case such a purpose is too broad to ensure compliance with the Regulation.

3.12. The EDPS suggests including an annex which lists specific processing operations provided for by specific articles of the international agreements and arrangements, including per each processing operation details on specific purpose, types of personal data, categories of data subjects, recipients of that data, technical and organisational measures, any specific safeguards and measures for sensitive personal data, if applicable. The AA should foresee regular up-dates of the annex(es) with common agreement of the parties.

3.13. The EDPS underlines, that each transfer should be carried out for a specific purpose in line with the mandates of the parties. While the draft AA sets the purpose in a broader way by referring to international agreements between F4E and ITER, any request for transfer should set out the specific, explicit and legitimate purpose of the transfer in question. Requests for further processing should also set out their purpose, which should be in compliance with the original purpose for which the data had been transferred.

Principle of purpose limitation and prohibition of any further incompatible use

3.14. The arrangement needs to specify the purposes for which personal data is to be transferred and further processed. The receiving party shall process data only for the purpose for which data were exchanged and any further processing incompatible with the initial purpose of the exchange of data should be prohibited. The AA should also specify that transferred data cannot be used for any purpose other than those expressly mentioned in the agreement, except if the parties wish to allow the receiving public body to make another compatible use of the transmitted personal data. In such case, further use by the receiving public body shall only be permitted if compatible with the original purpose and previously notified to the transferring public body which may oppose for specific reasons.

3.15. In Article 4 (a) the draft AA refers to "safety reasons" without specifying if the term covers background checks[11], in which case it is more security reasons, or also processing for health and safety at work[12] (e.g. because of people may get in contact with substances hazardous to health). Both cases can be considered as processing for compatible purposes provided there is a clear legal basis for the processing (including in the law of the host country[13]) and the processing itself is necessary, proportionate and fair.

3.16. Article 4(a) shall further specify the law of the host country (French law) and set out the appropriate safeguards referred as conditions of further compatible use in relation to further processing for 'safety reasons'. In particular, the text shall set out that any further use of the transferred data by ITER shall only be permitted if compatible with the original purpose and previously notified to F4E which may oppose for specific reasons.

3.17. Moreover it is not clear from the draft AA whether further processing is carried out by the Parties or on their behalf only, or it also includes further processing by third parties. For the second case the text should refer to applicable rules set for onward transfers and in particular to the need for prior authorisation of the transferring party.

Principle of data accuracy and data minimisation

3.18. A transferring party should only transfer and the receiving party should process only accurate and up to date personal data that are adequate, relevant and limited to what is necessary for the purposes for which they are transferred and further processed. Each party should inform the other without delay if it becomes aware that transferred personal data is incorrect. The AA should ensure that, where it is confirmed that data transmitted or being processed is inaccurate, each party processing the data shall take every reasonable step to rectify or erase the information.

3.19. The draft AA does not set out the types of personal data or categories of data subjects affected. The EDPS recalls that it is the responsibility of the transferring

---

11 EDPS issued prior check opinion on background checks (security screening): 2012-1090, 2007-371, 2016-0894 (EEAS for EUIs, only notification published, not PC opinion)

12 EDPS issued prior check opinion on health and safety at work: 2007-505, 2007-325, 2007-372, 2007-378, 2007-0383, 2004-227

13 *Provided such law shall respect the essence of the fundamental rights and freedoms of individuals recognised by the EU Charter of Fundamental Rights and EU law, does not go beyond what is necessary and proportionate in a democratic society and offers an effective redress for the individuals concerned.*

party to ensure that the personal data transferred is relevant and limited to what is necessary for the specific purposes for which they are transferred. In addition, the EDPS recalls that transfers of personal data to third countries or international organizations are subject to a **two-steps test.** First, each processing operation shall be lawful in accordance with Articles 5 and 10 of the Regulation and as a second step Chapter V should be respected. F4E should **assess** carefully the **necessity** of the transfer, **on a case-by-case basis**, in order to guarantee that the principles of data minimisation and lawfulness are complied with.

Storage limitation principle

3.20. Personal data should be retained for no longer than is necessary for the purpose for which the data are processed in compliance with the applicable laws, rules and/or regulation governing the retention of such data. When a maximum retention period is not already set in legislation, such period should be set in the text of the arrangement.

3.21. The EDPS notes that the draft AA should foresee specific retention periods and the obligation for the receiving party to continue to process personal data in line with the AA even after termination of the AA. Personal data that are processed unlawfully or are no longer necessary for the purpose of processing shall be permanently deleted.

Security and confidentiality

3.22. The EDPS notes that Section 4(e) of the draft AA provides for a commitment to take appropriate technical and organisational measures[14] to protect personal data and provides for provisions for personal data breaches. The level of security of the measures shall be determined taking into consideration the risks, the state of the art and the related cost.

3.23. However, the EDPS observes that the draft AA does not provide for concrete security measures. The EDPS is of the view that the AA should be completed with concrete additional safeguards considering the specific circumstances of the transfer and risks to rights and freedoms of individuals. In particular, the draft AA shall foresee at least that the level of protection required by the IT security policy of F4E is not diminished. It should also set out the obligation to inform data subjects if a personal data breach results in high risks to their rights and freedoms.

[14] See EDPB Guidelines paragraphs 25 and 26.

Right to transparency

3.24. The parties to an AA must ensure that the draft AA contains clear wording describing the transparency obligations of the parties, which include both a general information and individual information to data subjects. First, a **general information notice** should be made publicly available on F4E's and ITER's websites in relation to the processing carried out. This notice should include the transfer, the type of entities to which data may be transferred, the rights available to data subjects under the applicable legal requirements, including how to exercise those rights and information about any applicable restrictions on the exercise of such rights, available redress mechanisms and the contact details for submitting a dispute or claim. The AA should explain how this notice should be provided to data subjects and if individual notice needs to be provided.

3.25. The parties must commit to make the AA available to data subjects on request and to make the document or the relevant provisions providing for appropriate safeguards publicly available on their website. To the extent necessary to protect sensitive or other confidential information, the text of the AA may be redacted prior to sharing a copy or making it publicly available. Where necessary to allow the data subject to understand the content of the AA, the parties must provide a meaningful summary thereof.

3.26. The EDPS notes that the current wording of the Article 4(f) of the draft AA on transparency does not specify all elements that should be included in the general notice to the data subjects. At the same time, the obligation of publishing the text of AA on the website of F4E can cover these requirements.

3.27. It should be noted that for the transferring public body, a general information notice on their website will not suffice. **Individual information** to data subjects should be made by the transferring body in accordance with the notification requirements of Articles 15 and 16 of the Regulation.

3.28. The AA can provide for some exceptions to such individual information. These exceptions are limited and should be in line with the ones provided under Article 16(5) of the Regulation, for example where the data subject already has the information or where the provision of such information proves impossible or would involve a disproportionate effort.

3.29. The EDPS underlines that the general information provided on the websites of F4E and ITER cannot substitute individual information to data subjects and that the wording of the AA should be changed accordingly.

3.30. The AA shall also provide for the commitment of the parties to make available the text of the AA or the relevant provisions providing for appropriate safeguards, considering also the need to protect sensitive or confidential information. Where necessary that data subjects know the content of the AA, at least a meaningful summary should be provided to them.

Data subjects' rights

3.31. Data subjects should be able to obtain confirmation of whether their data have been transferred. They should also be provided with access to their personal data upon request. In addition, data subjects may request that their data are rectified, erased, blocked or restricted and where relevant the they have the right to oppose to the data processing on grounds relating to his or her particular situation. Any restriction to these rights has to be provided by law and is allowed only to the extent and for as long as this is necessary to protect confidentiality pursuant to professional secrecy or other legal obligations. The arrangement should furthermore specify when these rights can be invoked and include the modalities on how the data subjects can exercise these rights before both parties as well as on how the parties will respond to such requests. The arrangement shall also provide for an effective and enforceable right to redress for data subjects.

3.32. The AA shall set out an obligation for the transferring public body to provide information to the data subject, once their personal data have been transferred, on the action taken on their request without undue delay by setting an appropriate time limit (e.g. one month). Information shall also be provided to the data subject without delay by setting an appropriate time limit (e.g. within one month of receipt of the request), if the parties do not take action on the request of the data subject, including the reasons for not taking action and on the possibility of lodging a complaint and of seeking a judicial remedy.

3.33. If relevant to the agreement in question, the AA should, as a general principle, contain a clause stating that the receiving public body will not take a decision based solely on automated individual decision-making, including profiling, producing legal effects concerning the data subject in question or similarly affecting this data subject. Where the purpose of the transfer includes the possibility for the receiving public body to take decisions solely on automated processing in the sense of Article 24 of the Regulation, this should only take place under certain conditions set forth in the AA, such as the need to obtain the explicit consent of the data subject.

3.34. The EDPS notes that the current wording of Article 4(h) does not provide for the list of data subject rights as set out in the Regulation[15], for the modalities on how data subjects can exercise the rights of access, rectification, erasure, restriction of processing and to object as well as on how the parties will respond to such requests. The AA does not set out an obligation with a time limit for the transferring public body to provide information without delay on the action taken on the request of the data subject exercising his/her rights. The AA does not provide for an obligation to inform the data subject within a set time limit about not taking action on his /her request either. The draft AA should either prohibit taking decisions based solely on automated individual decision making or provide for the necessary safeguards in the text.

Restrictions on onward transfers

3.35. The EDPS notes that onward transfers by the receiving body are as a rule excluded. In particular, the EDPS welcomes that according to the draft AA transfers to other members of ITER, are not allowed.

3.36. Article 4(i) foresees four exceptions allowing onward transfers of personal data. However, these provisions do not fully comply with the Regulation and require some amendments to provide for the minimum set of safeguards as set out in the EDPB Guidelines.

3.37. Indeed, onward transfer or sharing of personal data[16] to a third party can take place only with the express prior written authorization of F4E, provided that the principle of purpose limitation is respected and the receiving party commits to respect the same data protection principles and safeguards as included in the AA. The receiving entity should provide sufficient information on onward transfers or sharing of personal data before requesting the authorisation of the transferring public body. In particular, the type of personal data, the reasons and purposes for which it considers necessary to transfer or to share the personal data. Therefore, a list of third parties, setting out also the types of personal data and the purpose for which it is necessary to share or transfer the data should be annexed to the draft AA. Article 6 of the draft AA may set out that the annex may be up-dated without a formal amendment (only the list or respective annex will be modified by common agreement and signed by the parties), provided that including the new recipient does not have a substantial impact on the effectiveness of the safeguards set out in the AA.

---

15 Articles 17-23 of the Regulation.

16 See EDPB Guidelines paragraphs 41-48.

3.38. Article 4(i)(i) of the draft AA, allows transfers to competent French authorities where required by the ITER Agreement, either based on 'prior written consent' or without prior approval based on the consent of the concerned individual or in case of 'foreseeable transfers' related to 'background checks'. To ensure coherence with the Regulation and EDPB Guidelines, the text in Article 4(i)(i) should refer to "authorization" of the transferring body, instead of its "consent", as the term "consent" is associated with the indication of the data subject's agreement to the processing of personal data relating to him or her. Allowing onward transfers or sharing of personal data in general, without the prior written authorization of the transferring body solely on the basis of informed consent of data subjects is not fully in line with the Regulation. Moreover, the referred "routine of foreseeable transfers" should be described in details as explained above, if necessary in an annex to the AA, which should also list authorised recipients.

3.39. Article 4(i)(ii) allows transfers to contractors of ITER provided that they are either subject to the Regulation 2016/679[17] ('the GDPR') or commit to respect the data protection principles and safeguards of this AA. The AA should include that authorized processors or subprocessors will respect in all cases the same data protection principles and safeguards as included in the AA. While compliance with the GDPR may be used as an element to demonstrate compliance with the provisions of the Regulation, it is not sufficient that processors or subprocessors are only subject to the GDPR without respecting the specific safeguards included in the AA.

3.40. Article 4(i)(iii) sets out that data may be transferred to a third party for important reasons of public interest or for the vital interest of the data subject, including, health, safety or security matters, or to prevention of threats to public security[18]. The EDPS notes that the article sets out some exceptional circumstances in which personal data may be shared in line with Article 50 of the Regulation. As recommended by the EDPB guidelines[19] the draft AA should also provide for an obligation of the receiving party to notify F4E, before the sharing takes place. If that is not allowed because of legal obligations of ITER, F4E should be notified as soon as possible after the transfer took place. Should ex-post notification not be possible either, 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 F4E at regular intervals.

---

17 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 (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016

18 This provision must be interpreted strictly in line with the 2/2018 EDPB Guidelines on derogations of Article 49 under Regulation 2016/679

19 EDPB Guidelines paragraph 46.

3.41. Article 4(i)(iv) allows onward transfers based on informed consent of the data subjects setting out the risks related to the transfer. In the absence of details on the types of personal data exchanged and the categories of data subjects concerned, on the basis of the sixth recital of the draft AA, the EDPS understands that only personal data of F4E staff members will be transferred to ITER. Therefore, relying solely on the informed consent of the data subject is problematic for several reasons.

3.42. First, it should be underlined that according to Article 50(2) of the Regulation, public authorities are not able to rely on derogations to transfer personal data based on the informed consent of the data subject[20] in the exercise of their public powers[21]. According to Council Decision 2007/198/Euratom the task of F4E is to provide Euratom's contribution, including human resources to the ITER project. Second, in case of processing and transfer of personal data of F4E staff members, and in line with the two-steps test mentioned under point 3.2, the consent cannot be a valid legal basis for the processing of personal data. According to the 5/2020 EDPB Guidelines on consent under the GDPR[22] there is an imbalance of power in the employment context, given the dependency of employees and its effect on their ability to give consent freely. Therefore, for the majority of data processing at work, the lawful basis cannot and should not be the consent of the employees due to the nature of the relationship between employer and employee. Consequently Article 4(i)(iv) should be deleted.

3.43. However, should there be other types of personal data processed outside of employment context and not falling within the scope of the exercise of public powers of F4E, the text should be completed as follows: 'iv. *where the prior informed consent of a data subject has been obtained, after having been informed of the purpose(s) of the onward transfer, the identity and contact details of recipient(s), the countries to which personal data is transferred and whether they provide an adequate level of protection, and the possible risks of such transfers transfer to the data subject due to the lack of appropriate data protection safeguards for the onward transfer. In this case, the receiving Party shall inform the transferring Party of the onward transfer and, at the request of the transferring Party, shall provide a copy of the information provided to the data subject.*'

Sensitive data

3.44. The EDPS observes that is not clear from the draft AA if sensitive data[23] is processed or not. Furthermore, Article 4(e) of the draft AA provides only for a general

---

20 Article 50(1)(a) of the Regulation.

21 See also point 2.1 of the EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

22 See paragraph 21 of the EDPB Guidelines 05/2020 on consent under Regulation 679/2016

23 EDPB Guidelines paragraph 49

commitment to take appropriate technical and organisational measures to protect personal data. It is not clear from the draft AA whether additional safeguards, have been added or considered in relation to transfers of sensitive personal data. Considering the circumstances of the transfer, in particular the nature and categories of personal data transferred as well as the entities involved in the processing, further suitable and specific measures will need to be added to the draft AA to safeguard and enhance the level of protection for individuals, in case sensitive data is transferred. In particular, the draft AA should foresee that the level of protection required by the IT security policy of F4E is not diminished. For example it may also provide for additional minimum safeguards, such as: (a) encryption of the data in transit, including the context of personal data breaches, using state of art encryption algorithms and standards (b) marking of data by ITER as personal data transferred; and (c) specialized training for ITER staff processing data transferred from F4E.

Redress

3.45. Data subjects should continue to benefit from redress mechanisms after their data have been transferred to a third country or to an international organisation. These redress mechanisms must provide recourse for individuals who are affected by non-compliance with the provisions of the administrative arrangement and thus the possibility to lodge complaints regarding such non-compliance and to have them resolved. In particular, the data subject must be ensured an effective route to complain to the public bodies or international organisations that are parties to the administrative arrangement and to an independent oversight mechanism. Moreover, a judicial remedy including compensation for damages should be available. Alternative dispute settlement mechanisms (quasi-judicial, binding mechanisms such as arbitration or alternative dispute resolution mechanisms such as mediation, which would guarantee an independent review and bind the receiving public body) should be provided if judicial remedies are not guaranteed in the third country or because of the specific status of the receiving party.

3.46. The public body transferring the personal data could also commit to be liable for compensation of damages through unlawful processing of the personal data if that is established by the independent review. Exceptionally, other, equally independent and effective redress mechanisms could be put in place by the arrangement, for instance effective redress mechanisms implemented by international organisations.

3.47. In order to ensure effective and enforceable rights, the arrangement should contain assurances from the entity receiving the EEA personal data that individual rights as well as administrative and judicial redress are fully provided by its domestic law and can be exercised by EEA individuals under the same conditions as it is the case for citizens and residents of the concerned third country. International organisations

should provide assurances about individual rights provided by their internal rules, as well as the available redress mechanisms.

3.48. If this is not the case, individual rights should be guaranteed by **specific commitments from the parties, combined with procedural mechanisms** to provide redress to the individual. Such procedural mechanisms can include commitments of the parties to inform each other of requests from EEA individuals, of the outcome of handling these requests and to settle disputes or claims in a timely fashion.

3.49. The redress mechanism must also be combined with the possibility for the transferring party to suspend or terminate the transfer of personal data where the parties do not succeed in resolving a dispute amicably until it considers that the issue has been satisfactorily addressed by the receiving party. Such a suspension or termination, if carried out, must be accompanied by a commitment from the receiving party to return or delete the personal data.

3.50. The EDPS notes that the current wording of the Article (j) on 'Remedies' foresees the right to lodge a complaint to the F4E-IO Transfer Monitoring Board composed of the data protection representatives of the parties. Individuals considering that the processing of their personal data under the AA infringes the data protection principles or safeguards set forth in the AA have the right to seek remedies in accordance with the applicable data protection law. For F4E the applicable data protection law is the Union data protection legislation and in particular Regulation 2018/1725. However, for ITER the AA refers to 'applicable rules and regulations put in place by the ITER Organization', without further specifying the references or the provisions. The AA foresees an obligation to cooperate in resolving complaints and to suspend the transfer until complaints are addressed satisfactorily by the receiving party.

3.51. The AA should set out clearly all the available redress mechanismshow can data subjects seek remedy under the arrangement and under the applicable data protection laws referred in Article 4(j). It should be set out that in relation to the processing carried out by F4E, individuals may lodge a complaint with F4E as a controller, to the EDPS as supervisory authority and have also the right to effective judicial remedy before the Court of Justice of the European Union. In relation to the processing carried out by IETR, the arrangement should describe how data subjects can submit a complaint to ITER, how it is handled and how effective redress mechanisms are implemented by ITER. In order to ensure effective and enforceable rights, the AA should contain assurances from ITER, as receiving party, that individual rights and administrative and redress mechanisms are fully provided by its regulations and can be exercised by EEA individuals under the same conditions as by other data subjects. Especially, it should be clearly stated that under the internal

regulations of ITER, individuals (i) have an effective route to complain to ITER, (ii) can complain to an independent oversight body, and (iii) in the absence of an effective judicial redress, how the AA provides alternative safeguards or other effective redress mechanisms. The arrangement shall also set out that decisions taken through alternative dispute settlement mechanisms are binding for the receiving party.

3.52. In addition, further specific commitments and procedural mechanisms need to be included in the arrangement. 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. Parties can commit to be liable for compensation of damages in cases of unlawful processing of personal data established by the independent review.

Supervision oversight mechanism

3.53. The supervision oversight mechanism should consist of a combination of periodic reviews conducted externally and internally by each party. The combination of the external and internal oversight as well as the adopted possible consequences following a negative review–which may include a recommendation to suspend participation in the administrative arrangement – provides for a satisfactory level of protection.

3.54. Each party to the agreement should conduct periodic internal checks of the procedures put in place and of the effective application of the safeguards provided in the agreement. The periodic internal checks should also verify any changes in legislation that would prevent the party to comply with the data protection principles and safeguards included in the AA. Moreover, it could be provided that a party to the agreement can also request from the other party to conduct such a review. The AA must require that the parties respond to each other's inquiries concerning the effective implementation of the safeguards in the agreement. Each party conducting a review should communicate the results of the checks to the other party to the AA and to the independent oversight mechanism governing the arrangement. In addition, the AA must include the obligation that the parties inform each other without delay if they are unable to effectively implement the safeguards in the agreement for any reason.

3.55. The arrangement must also provide for independent supervision in charge of ensuring that the parties comply with the provisions set out in the arrangement. If there is no competent data protection supervisory authority monitoring the receiving party and no external independent oversight can be ensured from a structural or institutional point of view, oversight could be guaranteed through functionally autonomous mechanisms. It must be a body that, while not external itself, carries out its functions

independently, freely from instructions, with sufficient human, technical and financial resources. The receiving party shall be bound by the decisions of the oversight body.

3.56. The EDPS observes that Article 5 (1) of the draft AA foresees that internal reviews are carried out by the data protection representatives respectively through regular monitoring of the application of the AA. The text should be complemented with provisions on periodic internal checks of the procedures put in place, of the effective application of the safeguards provided in the arrangement as well as of any changes in legislation. The arrangement should provide that the parties could request each other to conduct a review and should require to respond to each other's inquiries concerning the effective implementation of the safeguards in the arrangement. Each party conducting a review should communicate the results of the checks to the other and also to the independent oversight mechanism governing the arrangement. In addition, the AA must include the obligation that the parties inform each other without delay if they are unable to effectively implement the safeguards in the agreement for any reason.

3.57. Article 5(2) establishes the 'F4E-IO Transfer Monitoring Board' composed of the data protection representatives to assess whether the parties' policies, procedures and practices or the AA need to be amended. Pursuant to Article 5 (3) data subjects should be able to lodge a complaint to the Board, which should resolve it independently and impartially. The AA sets out that 'A complaint to the Board is, without prejudice to a data subject's right, under the applicable data protection law. '

3.58. The EDPS observes that the provisions of Article 5 leave doubts whether the Board composed of the data protection representatives is sufficiently independent to ensure an effective oversight and redress mechanism for data subjects, as they are staff members of the parties. In particular, to ensure a functionally autonomous mechanism, the arrangement should include commitments of the parties that the Board carries out its functions independently, free from instructions, and that it is provided with sufficient human, technical and financial resources. The current provisions do not set requirements for the data protection representatives, to be independent and impartial and can also lead to situations of potential conflict of interest, when staff members exercise oversight of their own activities. For example the parties may consider involving external, independent data protection experts chosen by their data protection representative or similar solutions involving an additional, fifth member chosen by the external experts. In addition, the arrangement shall foresee how the Board handles complaints and that the receiving party is bound by the decisions of the oversight body.

4. AUTHORISATION SUBJECT TO CONDITIONS

4.1. Subject to the changes and conditions laid down in the following paragraphs of this Decision, the EDPS takes note that the AA provides appropriate safeguards in the sense of Article 48(1) of the Regulation and under Article 58(3)(f) of the Regulation, the EDPS, thus **authorises** the use of the AA as a means for adducing appropriate safeguards under Article 48(3)(b), **under** the **conditions** specified hereafter.

4.2. Following **changes** are required in the draft AA:

a) Article 1(1)(f) should be complemented to read as follows: (f) 'onward transfer': transfer' for the purposes of the AA means transfer of personal data by the receiving party to a controller, processor or other recipient in a third country or in an international organisation ("third party");

b) Article 1(1)(f) should be complemented with a definition of 'sharing of personal data' setting out that for the purposes of the AA it means transfer of personal data by the receiving party to other recipients within ITER;

c) Article 2 should be complemented to provide for the specific types of personal data transferred, categories of data subjects affected, the type of processing of the personal data and the specific purposes for which that personal data is processed and transferred in annex. In case the AA covers processing of personal data under different international agreements, there should be a separate annex setting out the details for each agreement;

d) Article 3 should be complemented and any other references to the purpose of the AA should be complemented with all relevant, specific, explicit purposes, replacing in particular general references to rights and obligations of the parties;

e) Article 4(a) should be complemented to read as following: '*a) Purpose limitation: The Parties shall limit transfers of personal data between the Parties and 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 AA. 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 authorized. 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 public body which may oppose for specific reasons.';*

f) Article 4(b) should be complemented to read as following: '*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.'*;

g) Article 4(c) should be complemented to read as following: *'Accuracy: The transferring Party shall ensure that the personal data it transfers are accurate and, where necessary, kept up to date. The receiving Party shall ensure that the personal data transferred are accurate and, where necessary, kept up to date during the processing following the transfer. 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.'* ;

h) Article 4(d) should be complemented to indicate retention periods;

i) Article 4(e) should be complemented to read as following: '*e) 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, 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 by the IT security policy of F4E. 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 subjects shall be informed without delay if a personal data breach results in high risks to their rights and freedoms.*';

j) Article 4(f) should be complemented to read as following:

f) 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 ITER. 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 the 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 text of the arrangement or the relevant provisions providing for appropriate safeguards, considering also the need to protect sensitive or confidential information. Where necessary that data subjects know the content of the AA, at least a summary will be provided to them.';

k) Article 4(h)(i) should be complemented to read as following: '*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 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 and redress possibilities as well as access and to the appropriate safeguards relating to the transfer.';*

l) Article 4(h)(ii) should be complemented to read as following:

ii. ***"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, or where the data have been unlawfully collected or processed;*

iii. "***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;*

iv. "***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;*

v. ***"right of rectification"*** *means a data subject's right to have the data subject's inaccurate personal data corrected or completed without undue delay;*

vi. ***"right of 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;

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.';*

m) Article 4(h) should be further complemented to provide for the modalities on how data subjects can exercise their rights and how the parties will respond to such requests in a timely manner. The AA shall set out an obligation for the transferring party to provide information without delay, but at the latest within one month on the action taken on the request of the data subject exercising his/her rights. The AA shall equally foresee an obligation for the transferring party to inform the data subject without delay and at the latest within one month about not taking action on his /her request either. Such decisions should provide the reason for not taking action and refer to the possibility to lodge a complaint or seek remedies. Finally, the draft AA should either prohibit taking decisions based solely on automated individual decision making or provide for the necessary safeguards in the text;

n) Article 4 (i)(i) should be complemented to read as following: '*i. to competent French authorities subject to the GDPR listed in Annex X, where required by the ITER Agreement or the Agreement between the Government of the French Republic and IO, upon prior written authorization, 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 AA, in case of, but not limited to background checks; or';*

o) *Article 4(i)(ii) should be complemented to read as following: 'ii. to authorized third parties, 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 AA, on condition that , the principle of purpose limitation is respected and such contractors are subject to the GDPR and commit to respect the data protection principles and safeguards of this AA; or';*

p) Article 4(i)(iii) should be complemented to read as following: *'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. The receiving Party shall notify the transferring Party prior to the sharing of personal data. Should prior notification would impinge 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 public 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.';

q) Article 4(i)(iv) should be deleted;

r) the draft AA should be complemented with an annex listing third parties authorized by F4E to access the data transferred, setting out also the types of personal data and the purpose for which it is necessary to share or transfer the data. Article 6 of the draft AA may set out that the annex may be up-dated without a formal amendment (only the list or respective annex will be modified by common agreement and signed by the parties) provided that including the new recipient does not have a substantial impact on the effectiveness of the safeguards, technical and organisational measures set out in the AA;

s) Article 4(j) should be complemented to set out that in relation to the processing carried out by F4E, individuals may lodge a complaint with F4E as a controller, to the EDPS a supervisory authority and have also the right to effective judicial remedy before the Court of Justice of the European Union. In relation to the processing carried out by IETR, the arrangement shall also describe how data subjects can submit a complaint to ITER, how it is handled and how effective redress mechanisms are implemented by ITER.

The AA shall contain assurances from ITER receiving the EEA personal data that individual rights and administrative and redress mechanisms are fully provided by its regulations and can be exercised by EEA individuals under the same conditions as by other data subjects. It should be clearly stated that under the internal regulations of ITER individuals, (i) have an effective route to complain to ITER, (ii) can complain to an independent oversight body and (iii) in the absence of an effective judicial redress, how the AA provides alternative safeguards or other effective redress mechanisms. The arrangement shall also set out that decisions taken through alternative dispute settlement mechanisms are binding for the receiving party.

t) In addition, further specific commitments and procedural mechanisms need to be included in the arrangement. 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. Parties can commit to be liable for

compensation of damages through unlawful processing of the personal data if that is established by the independent review;

u) Article 5(1) should be complemented to provide for periodic internal checks of the procedures put in place, of the effective application of the safeguards provided in the arrangement as well as of any changes in legislation. The arrangement should provide that the parties could request each other to conduct a review and should require to respond to each other's inquiries concerning the effective implementation of the safeguards in the arrangement. Each party conducting a review should communicate the results of the checks to the other and also to the independent oversight mechanism governing the arrangement. In addition, the AA must include the obligation that the parties inform each other without delay if they are unable to effectively implement the safeguards in the agreement for any reason;

v) Article 5 (2) and (3) of the draft AA should be complemented to provide for commitments of the parties to ensure a functionally autonomous mechanism for supervision. In particular the Board shall carry out its functions independently, free from instructions, and it shall be provided with sufficient human, technical and financial resources. The arrangement shall foresee how the Board handles complaints and that the receiving party is bound by the decisions of the oversight body. The arrangement shall also set out, that when it comes to complaints under 'the applicable data protection law', concerning the processing of personal data by F4E, the data subjects have the right to lodge a complaint to the EDPS and they have the right to an effective judicial remedy before the Court of Justice of the EU;

w) In case sensitive personal data is processed under the draft AA, the wording of the AA should be modified and enhanced by adding a specific point regarding the transfer and processing of sensitive data and providing for suitable and specific measures to safeguard and enhance the rights and freedoms of data subjects as required by the principle of lawfulness under Article 10 of the Regulation. In particular, in such cases the draft AA should foresee that the level of protection required by the IT security policy of F4E is not diminished. It should also provide for additional minimum safeguards: (a) encryption of the data in transit, including the context of personal data breaches, using state of art encryption algorithms and standards (b) marking of data by ITER as personal data transferred; and (c) specialized training for ITER staff processing data transferred from F4E.

4.4. The EDPS **urges** F4E to inform the EDPS without undue delay of any suspensions of transfers of personal data, on the redress (Section 5), on the oversight of the AA and any revision or discontinuation.

4.5. The EDPS **asks** F4E to report on the implementation of this Decision by sending a revised copy of the AA within 6 months after the date of this Decision.

4.6. The EDPS may exercise the existing powers conferred under Article 58 of the Regulation, and in particular the power to order the suspension of data flows to ITER under the AA. The EDPS may in particular do so when:

a) the EDPS or another competent supervisory authority or court has determined that F4E or a recipient party is in breach of the applicable standards of protection; or
b) there is a substantial likelihood that the standards of protection are being infringed; or
c) there are reasonable grounds to believe that any of the conditions set out in this Decision are not complied with.

5. JUDICIAL REMEDY

5.1. Pursuant to Article 64 of the Regulation, any action against a decision of the EDPS shall be brought before the Court of Justice of the European Union within two months from the adoption of the present Decision and according to the conditions laid down in Article 263 TFEU.

Done at Brussels, 5 July 2021

(e-signed)

Wojciech Rafał WIEWIÓROWSKI

Annex: 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

Annex

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
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 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 processed and transferred and otherwise processed in the framework of their mutual cooperation by means of the appropriate safeguards specified in this Administrative Arrangement (hereinafter "AA");

HAVE AGREED AS FOLLOWS:

ARTICLE 1 – DEFINITIONS

1. For the purposes of this AA 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 AA; 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) **'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;
c) **'transferring Party (data exporter)'** means the Party who transfers the personal data;
d) **'receiving Party (data importer)'** means the Party who agrees to receive personal data from the data exporter for further processing in accordance with this AA;
e) **'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;
f) **'onward transfer'** for the purposes of the AA means transfer of personal data by the receiving Party to a controller, processor or other recipient in a third country ("third party");
g) **'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;
h) **'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;

i) **'processor'** means the natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller;
j) **'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 AA 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 before the entry into force of the present Administrative Arrangement. The Parties agree to interpret data protection provisions of existing agreements and arrangements in light of the AA as regards data transfers and processing between the Parties. The AA shall be without prejudice to applicable data protection law.

ARTICLE 3 – PURPOSE OF THE PROCESSING

The purpose of the processing is to implement the rights and obligations pursuant to the agreements and arrangements referenced in Article 2 of this AA. This processing includes the transfer of personal data between the Parties, the collection, recording, organisation, structuring, storage, adaptation, alteration or use of such data.

ARTICLE 4 – DATA PROTECTION PRINCIPLES AND SAFEGUARDS

With respect to the personal data subject to transfers covered by this AA, 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 and further processing of such personal data to what is strictly necessary for the purpose of implementation of the agreements and arrangements referenced under Art. 2 of the AA. Further processing which is not incompatible with the principle of purpose limitation, 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 host country laws, and which is subject to appropriate safeguards is authorized.

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 subparagraph a.

c) Accuracy: The transferring Party shall ensure that the personal data it transfers are accurate and, where necessary, kept up to date. 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.

e) 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. marking received personal data, restricting access, secure storage and transmission). The level of security of the measures shall be determined taking into consideration the risks, the state of the art and the related cost. 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.

f) 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. This privacy statement shall be published on the external websites of F4E. 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.

g) Accountability: A Party may request the other Party to demonstrate its compliance with this AA, 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 AA, respecting any conditions, which the other Party may have attached to such provision of information, notably as regards confidentiality.

h) 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 AA and are being processed, and, where that is the case, access to the personal data and the appropriate safeguards relating to the transfer.
ii. *Rectification, erasure, etc.*: The data subject shall have the right to obtain the rectification, erasure, restriction of processing, or blocking of personal data concerning him or her in accordance with applicable data protection law, unless this proves impossible or involves disproportionate effort.

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.

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

i. to competent French authorities subject to the GDPR[24]where required by the ITER Agreement or the Agreement between the Government of the French Republic and IO, upon prior written consent. Prior written consent shall not be required in case of informed consent of the concerned individual, and in case of routine or foreseeable transfers in *direct* implementation of the agreements and arrangements referenced in Article 2 of the AA, such as but not limited to background checks; or
ii. to Contractors of the receiving Party where necessary for carrying out tasks on behalf of the receiving Party for purpose of implementing the agreements and arrangements referenced in Article 2 of the AA, on condition that such contractors are either subject to the GDPR or commit to respect the data protection principles and safeguards of this AA; 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; or

[24] *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.*

iv. where the prior informed consent of a data subject has been obtained, after having been informed of the possible risks of such transfers.

j) Remedies: The Parties recognise that, notwithstanding the right to lodge a complaint to the Board under Article 5(3) of the AA, a data subject who considers that the processing under this AA of personal data related to him or her infringes the data protection principles or safeguards set forth in this AA has the right to seek remedies in accordance with the applicable data protection law. 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 AA, 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 5 – OVERSIGHT MECHANISM

1. Each Party shall nominate a data protection representative who shall regularly monitor the application of the AA.

2. The data protection representatives of the Parties form the F4E-IO Transfer Monitoring Board (hereinafter the "Board") which shall periodically assess whether the Parties' policies, procedures and practices or the AA need to be amended to give full effect to the latter.

3. A data subject who considers that the processing under this AA of personal data related to him or her infringes the data protection principles or safeguards set forth in this AA may lodge a complaint with the Board addressed to one of the data protection representatives. The Board shall seek to resolve the complaint independently and impartially. A complaint to the Board is, without prejudice to a data subject's right, under the applicable data protection law.

ARTICLE 6 – AMENDMENTS AND TERMINATION

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

2. A Party shall be entitled to terminate this AA 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 AA for a period set in advance. In this case, the receiving Party shall destroy the personal data by the date the period expires.

ARTICLE 7 – PRIVILEGES AND IMMUNITIES

This AA 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 8 – SETTLEMENT OF DISPUTE

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

ARTICLE 9 – ENTRY INTO FORCE

This AA shall enter into force on (...).

30