EUROPEAN DATA PROTECTION SUPERVISOR

EDPS DECISION ON THE EDPS MODEL ADMINISTRATIVE ARRANGEMENT FOR TRANSFERS OF PERSONAL DATA UNDER REGULATION (EU) 2018/1725 FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES TO INTERNATIONAL ORGANISATIONS (Case 2020-0809)

1. Transfers of personal data from Union Institutions, agencies, offices and bodies to international organisations

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. European Union Institutions, agencies, offices and bodies ('EUIs') have to comply with specific requirements under Regulation 2018/1725[1] ('the Regulation'): subject to a two-steps test: first, the processing must be lawful and second, there must be a suitable ground for transfer in place in line with Chapter V.
2. The first mechanism foreseen by the Union legislator to ensure an essentially equivalent level of protection to the data transferred to a third country is the adoption of an adequacy decision by the European Commission. Such a decision recognises that a third country or an international organisation[2] ('IO') ensures to personal data a protection which is essentially equivalent to that within the EU. There are no adequacy decisions in force for IOs.

[1] 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 (Text with EEA relevance.) OJ L 295, 21.11.2018, p. 39–98.
[2] Article 3(21) of the Regulation defines international organisation as an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

3. 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. A legally binding and enforceable instrument between public authorities or bodies may provide for such appropriate safeguards without any further authorisation by the European Data Protection Supervisor ('EDPS'). Another mechanism that may be used to ensure continuity of protection, through appropriate data protection safeguards is an administrative arrangement ('AA') concluded between an EUI and a public authority or IO, subject to the authorisation of the EDPS.

4. The European Data Protection Board ('EDPB') has issued 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 clarifying the safeguards to be included in an AA ('the 2/2020 EDPB Guidelines'). The criteria for appropriate safeguards under Article 48(3) (b) of the Regulation are the same as under Article 46(3) (b) of the GDPR. Therefore, the 2/2020 EDPB Guidelines are also relevant for AAs concluded between EUIs and other public authorities and have been carefully considered for the EDPS model AA as well.

5. EUIs embrace the cooperation and often work together with IOs insofar as they regularly need to exchange personal data to fulfil their mandates based on the Treaty on the Functioning of the European Union[3]. IOs have a specific status under international law, because of applicable privileges and immunities intended to ensure their independent and effective functioning. Their status therefore also needs to be taken into account in instruments governing transfers of personal data from EUIs to IOs. To further facilitate data exchanges between EUIs and IOs and considering the relevant specific context into account, a specific model AA has been developed and is attached to the present decision as Annex I.

2. Consultations on transfers from EUIs to IOs

6. In 2020, the International Transfers Working Group of Data Protection Officers of EUIs[4] ('EUI DPO ITR Working Group') requested the opinion of the EDPS on a model AA to transfer data between EUIs and IOs under Article 48(3) (b) of the Regulation to further facilitate such transfers.

7. On 25 June 2020 the Data Protection Officers of certain IOs' contacted the EDPS to contribute to the drafting of the model AA and to present their position as already sent to the European Data Protection Board in the context of the public consultation on the 2/2020 EDPB Guidelines.

8. In October 2020 the EDPS set up an informal task force on international transfers with interested IOs to discuss the question of transfers to IOs. It was then decided to address first the question of transfers from public authorities to IOs and focus the work on the EDPS model AA for transfers from EUIs to IOs. Participants to the task force included

[3] Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012

[4] Informal working group of DPOs of EUIs dedicated to international transfers and represented by the DPOs of the European External Action Service and the European Union Intellectual Property Office.

various IOs, the EDPS, the European Commission, the Data Protection Officers of the European External Action Service ('EEAS') and the European Union Intellectual Property Office ('EUIPO') as representatives of the EUI DPO ITR Working Group, other EUI DPOs, the Italian DPA, and two German Federal DPAs at Federal and Länder levels.

9. Several rounds of oral and written exchanges took place within the task force, taking into account various comments of IOs, leading to a revised draft of the model AA.

10. The EDPS appreciates the constructive attitude and the efforts of IOs participating in the debate and contributing to the draft text. To finalise the draft, extensive consultations took place between the EDPS, the European Commission and the EUI ITR DPOs Working Group with the aim of addressing the observations and requests of IOs and the needs of all stakeholders while ensuring that the requirements under the Regulation are met.

3. Proceedings

11. This Decision lays down the EDPS model administrative arrangement ('AA') for transfers of personal data from an EUI[5] to an IO[6] based on Article 48(3)(b) of the Regulation.

12. The EDPS adopts this Decision and the EDPS model AA in annex 1 in accordance with Article 57(1) (g) of the Regulation.

13. The Decision is addressed to EUIs as defined in Article 3(10) of the Regulation.

14. The EDPS model AA is a tool provided to assist controller in fulfilling the minimum requirements for appropriate safeguards pursuant to Article 48(3) (b) of the Regulation and it is in line with the interpretation set out in the 2/2020 EDPB Guidelines 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. To be used by the parties, it must be **duly completed with information about the transfers** to be covered and **may, where necessary, be adapted** in light of the **specific circumstances of the transfers**. For example, it may be adapted to reflect specific requirements of the IO's legal framework, provided these requirements do not affect the level of protection offered under the AA. The text may also need to be complemented or adapted to address specific circumstances (e.g. humanitarian context) on a case-by-case basis. Text in square brackets marked with grey are instructions or explanations: they should be filled out or deleted from the final text as appropriate.

15. Pursuant to Article 48(3) (b) of the Regulation, AAs are subject to the **authorisation of the EDPS**. While this model provides for a template setting out the minimum requirements, its use does not automatically imply the EDPS authorisation. For all AAs based on this model, an EDPS authorisation must be requested by the relevant EUI in line with the requirements of the Regulation. To facilitate the issuance of an authorisation the EUI should:

[5] As defined in Article 3(10) of the Regulation.
[6] As defined in Article 3(21) of the Regulation.

- provide a **transfer impact assessment**[7] that covers all transfers of personal data from the EUI to the IO envisaged under the AA, and that covers third countries in which it is envisaged that the IO processes the transferred personal data (from which requests for disclosure by those third countries' public bodies may likely be received). The transfer impact assessment should also verify whether the laws of the third countries referred to above, applicable to the transferred personal data, respect the essence of the fundamental rights and freedoms recognised by the Charter and where those laws provide limitations to the exercise of the fundamental right to data protection, they do not exceed what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in EU or Member State law, such as those listed in Article 25(1) of the Regulation. Should the laws of those third countries not fulfil the above criteria, either the transfer cannot take place, or effective supplementary measures should be implemented by the transferring EUI.
- use and **duly fill out the model AA and its annexes** to provide details on the transfer and list relevant security measures, including the supplementary measures, if necessary. Use of the EDPS model AA is however not a condition to obtain the authorisation by the EDPS.
- indicate if applicable where the parties **deviate** from the provisions of the model, and the reasons for that deviation;
- provide **other relevant documents** (e.g. if the AA is an annex to a wider agreement the text should be provided for information).

16. In all cases EUIs are encouraged to informally consult the EDPS already during the negotiations to accelerate the authorisation procedure.

17. The EDPS model aims at providing an example on how the requirements of the EUDPR and the 2/2020 EDPB Guidelines can be implemented in practice by an EUI in its relations with an IO. **There is no obligation to use the EDPS model** AA, but by following it, EUIs can streamline the negotiations between the parties and help the EDPS to accelerate the authorisation procedure.

18. During the authorisation process the EDPS will verify if, considering the specific circumstances of the transfer, appropriate safeguards are provided and if there as an essentially equivalent level of protection ensured for the data transferred outside of the EEA. The EDPS will focus, indicatively, on the specific circumstances of the transfer, the transfer impact assessment provided by the EUI, the adaptations made to the text and the completeness of the annexes. Therefore, the time necessary for the authorisation process depends, in particular, on the complexity of the transfer at stake, the completeness of the authorisation request, whether the EDPS model has been followed,

[7] The Court of Justice of the European Union (CJEU) clarified in the Schrems II judgment of 16 July 2020 (C-311/18) that before a transfer takes place, data controllers must assess whether, in the context of the specific transfer, the third country of destination affords the transferred data an essentially equivalent level of protection to that in the European Union and determine the need to put in place additional safeguards. Such assessment is known as a Transfer Impact Assessment (TIA).

scope and number of changes made to the text, level of details and supporting documents provided.

19. Pursuant to Article 1(3) of the Regulation, the EDPS monitors processing operations carried out by an EUI. The EDPS has however no competence to assess or authorise transfers from IOs to EUIs. The **scope of the authorisation issued under Article 48(3)(b) is therefore limited to transfers from EUIs to IOs**. However, this **does not prevent the parties** from including **the EDPS model AA as an annex of a wider arrangement**, **governing also transfers from IOs to EUIs, provided that the other provisions do not contradict the AA**.

20. The model provides for a template for appropriate safeguards pursuant to Article 48(3)(b) of the Regulation for **transfers between separate controllers**. The model does not ensure compliance with Article 29 of the Regulation, covering cases where the receiving IO is also a processor for the transferring EUI. Considering the nature of cooperation between IOs and EUIs, the most likely scenarios appear to concern controller to controller transfers. Should the transfer take place in the context of an (EUI) controller - (IO) processor relationship, or where the parties involved are joint controllers -, the specific requirements of the Regulation[8] should be addressed separately.

21. The EDPS highlights that the EDPS model AA is an instrument under the Regulation, aimed at helping controllers in fulfilling their tasks of ensuring an essentially equivalent level of protection as it is guaranteed in the EU when EUIs transfer personal data to IOs. Therefore, the provisions of the EDPS model AA should be interpreted in line with the Regulation.

4. Commentaries on specific provisions

Recitals

22. The recitals recall the importance of ensuring efficient international cooperation between the sides to fulfil their mandates, which may require personal data to be exchanged. It also recognises privileges and immunities of both sides and recalls that transfers of personal data to IOs should not undermine the protection of individuals as guaranteed under EU law.

Article 1 - Subject matter and scope

23. Article 1 sets out the scope of the model AA. As explained above, for reasons related to the competence of the EDPS, **it applies only to transfers from EUIs to IOs**. Since the AA is a non-binding instrument, the sides should confirm that their applicable legal framework provides for enforceable data subjects rights and effective legal remedies as

[8] Article 28 for joint controllership and Article 29 for controller-processor relationships.

well as the necessary safeguards and that these can be effectively implemented in practice.

24. It is also clarified that the description of the specific circumstances[9] of the transfer should be included in Annex I.B, which forms an integral part of the model AA and cannot be amended unilaterally by one of the sides.

Article 2 - Definitions

25. Article 2 provides for **definitions**[10] of the terms used in the model AA, such as personal data, processing of personal data, transferring and receiving sides, applicable data protection frameworks, onward transfers, personal data breaches and special categories of personal data. It should be underlined that the list is not exhaustive and the parties may therefore agree, considering the specific circumstances of their transfers, to complete it with other relevant definitions in line with the Regulation.

Article 3 - Personal data protection safeguards

26. Article 3 provides for key data protection safeguards, including to ensure respect of basic data protection principles.

Purpose limitation

27. Article 3(1) provides that personal data can only be **processed for the specific purposes**[11] **included in the AA**. These purposes should be listed in **Annex I.B**, which has to contain information on each specific transfer, and must be described in details. For example, it is not sufficient to simply refer to the official mandate or the legal framework of the sides, or to an alleged unspecified public interest, without providing further details. The specific purposes for processing agreed by the sides should always be listed in Annex I.B.

28. The AA provides for the possibility of **further compatible processing** and provides an explanation of the factors that need to be taken into account to determine whether a purpose is compatible[12]. The link with the original purpose(s), the circumstances of the data collection, the reasonable expectations of data subjects on further use of the data, the nature of the personal data, as well as the impact of the further processing on individuals should equally be considered. In addition, the AA lists some examples of compatible purposes in Article 3(1) and in the annex (e.g. processing for archiving, scientific research, historical purposes or for internal audits and internal investigations).

---

[9] See also point 2.1 of the 2/2020 EDPB Guidelines.
[10] See also point 2.2 of the 2/2020 EDPB Guidelines.
[11] See also point 2.3.1 of the 2/2020 EDPB Guidelines.
[12] For further information controllers may consult Point III.2 of the 03/2013 Article 29 Data Protection Working Party's guidelines on purpose limitation.

If relevant in the context of a specific AA, the compatible purposes for which data may be processed should be **included in Annex I.B.**

Data accuracy and minimisation

29. Article 3(2) provides that the personal data exchanged and processed by the parties must be **accurate**[13] **and up to date**; inaccurate data should be corrected or erased and the sides need to keep each other informed. The text recalls the receiving side, considering also the specific circumstances of the processing (e.g. humanitarian context), has an obligation to take every reasonable step to ensure the accuracy of the data received.

Data retention

30. Article 3(3) provides that personal data cannot be kept longer than necessary for the purposes for which the data is processed[14]. In this respect, the model AA also refers to compatible purposes for which data may be processed. For example, if personal data received from an EUI is further processed by the IO for archiving or internal purposes, the data may be kept by the IO for as long as need for those purposes. In addition**, the applicable retention periods** or, if that is not possible, the criteria to determine such periods should be set out in the annex.

Integrity and confidentiality

31. Article 3(4) provides that the IO should have in place **appropriate technical and organisational measures to ensure the security of the personal data** received[15], including to prevent data breaches[16]. It is further specified that when assessing the appropriate level of security, due account should be taken of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved for individuals. In this context, the specific measures applied should be described in **Annex III**, which contains a list of examples of possible **technical and organisational security measures** that could be put in place including measures to ensure protection as regards unlawful requests for access from national authorities.

32. In case of a **data breach** concerning the personal data transferred under the AA, the IO should inform without delay the EUI on the nature of the breach, its likely consequences, and the measures taken or proposed to mitigate it. It has also to provide a contact point. All this is essential so that EUIs can comply with their obligations under the Regulation and inform the EDPS as necessary.

[13] See also point 2.3.2 of the 2/2020 EDPB Guidelines.
[14] See also point 2.3.3 of the 2/2020 EDPB Guidelines.
[15] See also point 2.3.4 of the 2/2020 EDPB Guidelines.
[16] As defined in Article 2(7) of the AA.

Article 4 - Data subject rights

Transparency

33. Article 4(1) recalls that the EUI is required to give individual information to the data subject in line with the Regulation. **EUIs need to make sure that the annexes of the AA are precisely filled out also with a view to be able to provide individual information to the data subjects**.

34. For the receiving IO, the AA provides that, at least, general information should be publicly available[17]. This includes, as a minimum, the categories of personal data transferred and further processed, how the data is processed by the IO, the relevant ground used for the transfer under the Regulation, the purpose of the processing, third parties or categories of third parties to whom the information may be onward transferred, individual rights and available mechanisms to exercise their rights and obtain redress as well as the contact details for submitting a request or complaint. The model AA intends to set out the minimum requirements to inform data subjects. This is however **without prejudice to stricter obligations IOs may have in place**, which can always be added to the AA.

35. Article 3(2) also provides that upon request, the sides should make available to data subjects a **copy or at least a meaningful summary of the AA**. Depending on the circumstances, the parties may redact the text prior to sharing a copy, as long as data subject can still understand the content of the AA and exercise their rights.

Data Subject Rights

36. Article 4(2) concerns data subject rights[18], namely the **right to access** (including information on and a copy of personal data processed), **rectification** of inaccurate or outdated data, **erasure** of unlawfully processed personal data and, under certain conditions, the **right to object to the processing** of personal data. It is important to underline, that if data protection rights and redress for EEA individuals are not provided for in internal rules/regulatory framework of the IO, preference should be given to concluding a legally binding agreement[19]. The AA, not having a binding nature, it cannot itself establish data subject rights.

37. The AA specifies when these rights can be invoked and includes the **modalities** on how the data subjects can exercise these rights including that the parties will respond to such requests within one month. In case of abusive or unfounded requests the data subject should be informed in a month if no action is taken on the request, including the reasons and the possibility of lodging a complaint and of seeking remedy.

[17] See also point 2.4.1 of the 2/2020 EDPB Guidelines.
[18] See also paragraphs 27 and 28 and point 2.4.2 of the 2/2020 EDPB Guidelines.
[19] See 2/2020 EDPB Guidelines, paragraph 72.

38. The parties may rely on **exceptions**[20] restricting the exercise of data subject rights where necessary to protect important objectives of public interest or essential functions under the mandate of the IO or the rights and freedoms of others, subject to the principle of proportionality. Any restriction has to be a necessary and proportionate measure in a democratic society to safeguard important objectives of public interest, in line with the ones listed in Article 25(1) of the Regulation. **These restrictions should be provided by law or in case of an IO by their regulatory framework**, in line with the restrictions envisaged by Article 25 of the Regulation and should be applied only for as long as the reason for the restriction exists.

Automated decision - making

39. If relevant to the agreement in question, the AA should contain a clause stating that the IO will **not take a decision based solely on automated individual decision-making**[21], including profiling, producing legal effects concerning the data subject in question or similarly affecting this data subject. The EDPS recalls that in case of an AA involving automated decision-making, specific safeguards should be in place in the regulatory framework, in order to ensure that the protection provided by Article 24(1) of the Regulation is afforded to personal data transferred to EUIs. The EUI should inform the data subject about the envisaged automated decision, its consequences, the logic involved and it should implement suitable safeguards, at least by enabling the data subject to contest the decision, express their point of view and obtain human review.

Article 5 - Onward transfers

40. Article 1(6) defines **onward transfers**[22] "*as a transfer of personal data by a receiving Side to any entity that is not a Side signatory to the AA (´third party´)*". A third party can be another IO (even if they are part of the same global organisation), a private or public entity. The provisions of Article 5 apply by analogy also in case of date transmitted back by the IO or one of its processors to a recipient in the EEA.

41. Onward transfers by a receiving IO, to recipients not bound by the agreement should, as a rule, be specifically excluded by the AA[23]. Depending on the subject matter and the particular circumstances at hand, the parties may find it necessary to allow onward transfers. Article 5(1) provides a **general rule** that any onward transfer is possible only if necessary for the fulfilment of the mandate of the IO, for the purposes described in Annex I.B. and if the other requirements of the AA are also respected, including to put in place the technical and organisational measures listed in Annex III.

42. Conditions apply regarding onward transfers to entities outside the European Economic Area[24] or to other international organisations. In particular, pursuant to Article 5(2), in

[20] See also point 2.4.5 of the 2/2020 EDPB Guidelines.
[21] See also point 2.4.3 of the 2/2020 EDPB Guidelines.
[22] See also point 2.5 of the 2/2020 EDPB Guidelines.
[23] Paragraph 41 of the 2/2020 EDPB Guidelines.
[24] The 27 EU Member States and Norway, Iceland and Liechtenstein.

case the general conditions of Article 5(1) are fulfilled, such onward transfers may take place if the country where the recipient is located or the IO benefit from an **adequacy decision** adopted by the European Commission and the transfer is covered by that adequacy decision.

43. In case the general conditions of Article 5(1) are fulfilled, such onward transfers may also take place if the transfer is authorised by the EUI. The model AA provides two different options for the authorisation. It may be provided by **including the transfers in Annex IV** of the AA if the sides know in advance about onward transfers that are necessary, or can be granted after the signature of the AA, once an onward transfer is envisaged. In case the onward transfer is not listed in Annex IV, the IO needs to provide the details listed in therein, so that the EUI can authorise the onward transfer in writing before it takes place. In both cases, the recipient third party should enter into a binding commitment with the IO to ensure the same level of data protection as provided by the AA, including to put in place the technical and organisational measures listed in Annex III, before the onward transfer takes place. The assessment of whether or not to authorise an onward transfer should be carried out by the transferring EUI, considering the specific circumstances and the information provided.

44. In addition, pursuant to Article 5(3), in case the general conditions of Article 5(1) are fulfilled, an onward transfer to a non-EEA country or an international organisation may also take place **without the authorisation of the EUI** if the data subject gave their informed consent[25]; or it is necessary in order to protect the vital interests of the data subject or of another natural person; or for the establishment, exercise or defence of legal claims. Onward transfers may also be possible for an important objective of public interest as also recognised by EU law if the third party commits to process the data only for the specific purpose(s) as described in Annex I.B and to delete the data once the processing is no longer necessary for that purpose.

45. In case the onward transfer takes place under the exceptional circumstances listed in Article 6(3), the IO should **notify the EUI** before they take place by providing the information required under Annex IV, or, if that is not possible, immediately thereafter.

Article 6 - Request for access from national authorities

46. Article 6 provides specific commitments to handle requests for access from national authorities[26] to personal data transferred by EUIs. The commitments set out in Article 6 apply in addition to the other requirements of the AA, in particular Article 5. The general rule is that the **EUI needs to be notified** of such access requests by the IO. Article 6(1) takes into account that in some cases the IO may be prohibited from informing the EUI by laws applicable to the requesting authority. Such laws must respect the essence of the fundamental rights and freedoms recognised by the Charter and must not exceed what is necessary and proportionate in a democratic society to safeguard one of the important

[25] After having informed the data subject of the purpose(s) of the onward transfer, the identity of the recipient and the possible risks of such transfer in terms of applicable data protection safeguards.
[26] See also paragraph 47 of the 2/2020 EDPB Guidelines.

objectives as also recognised in EU or Member State law, such as those listed in Article 25(1) of the Regulation. In all cases it should try to waive the prohibition on a best efforts basis, document such efforts and provide as much information as possible to the EUI without undue delay.

47. When it comes to the handling of requests for disclosure, Article 6(2) first of all refers to the IOs assessment of the **application of its own privileges and immunities**. In addition, it refers to an assessment by the IO about the lawfulness of the request under the laws applicable to the requesting authority. The model AA aims at setting minimum common standards to make sure that the legality of the request is reviewed and that the IO challenges the request or asks for a review if appropriate. This assessment and a possible appeal is done according to the IO's procedural rules and the applicable legal framework, but it has to be duly documented and made available to the transferring side upon request.

48. In case the IO concludes that personal data can be disclosed in line with its applicable legal framework, the sides should cooperate in view of seeking the best protections available. In such cases the EUI should endeavour to disclose the minimum amount of information permissible, based on a reasonable interpretation of the request.

Article 7 - Special categories of personal data

49. Should **special categories of personal data**[27] need to be transferred to the IO, this should be clearly indicated in Annex I. In this case, the IO should apply specific restrictions and/or additional safeguards adapted to the specific nature of special categories of personal data and the risks involved in the processing of such data. These could be for example restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation or encryption of the data in transit) and/or additional restrictions with respect to further disclosure[28].

Article 8 - Redress mechanism

50. Article 8 provides individuals with a right to lodge a complaint before the IO and obtain its effective and timely handling and resolution[29]. EUIs should be informed about all received complaints and their resolution by the IO.

51. In addition, the AA has to refer to a specific redress mechanism[30] that may be used in case a complaint cannot be resolved amicably by the IO to ensure effective redress for the individual. . In case it is available, the sides should agree on the use of judicial redress (e.g. international courts). However, considering the specific status of IOs, judicial redress may not be available. Therefore, the model AA provides the **minimum requirements** that alternative redress mechanisms have to meet offering essentially equivalent

[27] As defined under Article 2(8) of the AA.
[28] See also point 2.6 of the 2/2020 EDPB Guidelines.
[29] See also paragraph 50 of the 2/2020 EDPB Guidelines.
[30] See also points 2.4.4.and 2.7 as well as paragraph 75 of the 2/2020 EDPB Guidelines.

guarantees to individuals to those required by Article 47 of the Charter of Fundamental Rights of the European Union[31] In particular, such a mechanism should be a pre-established (i.e. agreed and available throughout the duration of the AA) mechanism that ensures independent and impartial adjudication, in accordance with principles of due process, binds the IO and should include also the possibility to obtain compensation for damages.

52. Considering the comments received during the consultation process the EDPS clarifies, that the criterion **pre-established** does not aim at restricting the redress mechanism to courts, it specifies that the redress mechanism cannot be developed just when a data subject submits a complaint under the AA. It has to be established or agreed before the sides sign the AA and it needs to be available throughout the duration of the AA. Depending on the specific circumstances, it could be binding arbitration, administrative tribunal/mechanism within the IO or established at international level as well.

53. When issuing a concrete authorisation, the EDPS will assess each redress mechanism, including the possibility to obtain compensation for damages, on a case-by-case basis, considering also the specific circumstances of the transfer.

Article 9 - Independent oversight

54. In Article 9, the parties identify an **independent oversight mechanism**[32] that will oversee compliance with the AA. For the EUI, such oversight will be exercised by the EDPS. The model AA describes the minimum requirements for an independent oversight mechanism as an external or internal body including a functionally autonomous body that is independent and impartial and has binding investigatory and remedial powers. It should be free from any influence or instructions; appointed for a fixed term on the basis of specific criteria through a transparent procedure; can only be dismissed for cause; has sufficient human, technical and financial resources, can access to all relevant information, can order the suspension or change of processing, or deletion of unlawfully processed data.

55. When issuing a concrete authorisation, the EDPS will assess the specified oversight mechanism on a case-by-case basis, considering also the specific circumstances of the transfer.

Article 10 - Implementation, revisions and termination

56. Article 10 requires the sides to jointly review the effective implementation of the AA. They should inform each other if there are substantial changes in their respective legal frameworks and may adapt the AA as necessary.[33]

[31] Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407.
[32] See also paragraphs 56 and 59 of the 2/2020 EDPB Guidelines.
[33] See also paragraphs 56, 57 and 58 of the 2/2020 EDPB Guidelines.

57. In case the IO is **not able to implement effectively** the AA the EUI should be promptly informed to allow the sides adapting the text as necessary.

58. If the IO is **unable to comply with the AA,** the EUI should suspend the transfers until compliance is ensured. Transfers may also be suspended or **terminated until a dispute is resolved** if the sides cannot do it amicably[34].

59. The EUI may terminate the transfer in case the IO is **in substantial or persistent breach of the AA**. The IO should either delete or send back the data to the EUI unless its legal framework prevents from doing so. In case a side wishes to **terminate the AA for other reasons**, they may agree to continue processing the already transferred data in line with the AA after termination.

60. As a general rule, in case of termination, **personal data transferred that must be kept because of** a legal obligation, **should continue to be processed in line with safeguards of the AA** until the data is deleted or returned.

Annexes

61. The **four annexes** form integral part of the AA and provide for specific details on the transfers. **They must be filled in by the parties with information specific to the transfers covered by the AA.**

Annex I

62. **Annex I, includes the description of the sides and the transfers,** including categories of personal data and of data subjects whose personal data is transferred, the special categories of data transferred and respective restrictions and safeguards, as well as the purpose(s) of the data transfer and of further processing, including how they relate to the mandate of the sides.

63. It must be possible to clearly distinguish the information applicable to each transfer or set of transfers and, in this regard, to determine the respective role(s) of the sides. This does not necessarily require completing and signing separate sets of annexes for each transfer or set of transfers, where this transparency can be achieved through one set of annexes. However, where necessary to ensure sufficient clarity, separate sets of annexes should be used.

Annex II

64. **In Annex II, the sides should** describe the **data protection framework that applies to them**. For the IOs there should be a description or summary or reference to the applicable data protection framework, including substantive rules (e.g. data protection

[34] See also paragraph 58 of the 2/2020 EDPB Guidelines.

principles, individual rights) and procedural safeguards (oversight and redress mechanisms), as well as the privileges and immunities.

Annex III

65. **In Annex III, the sides should** list the **technical organisational and security measures** that the IO will apply, including measures to ensure protection as regards unlawful requests for access from national authorities. The measures need to be described in specific (and not generic) terms. In particular, it is necessary to clearly indicate which measures apply to each transfer or set of transfers. The annex should describe technical and organisational measures implemented by the IO or in case of sub-processors by those entities (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. The annex provides for some examples of measures.

Annex IV

66. **In Annex IV, the sides should** provide information on **onward transfers**. It must be possible to clearly distinguish the information applicable to each onward transfer or set of onward transfers and, in this regard, to determine the respective recipient(s) and the IO's role, the categories of personal data involved, the reasons and purposes of onward transfers, the third countries or IOs involved and the applicable technical and organisational measures implemented by the IO and the third party recipient.

67. The EDPS **recommends** that EUIs use the model AA adapted and filled out as necessary when requesting an authorisation from the EDPS under Article 48(2)(b) of the Regulation for transfers to IOs.

Done in Brussels

Annex 1: EDPS Model administrative arrangement for a transfer of personal data under Regulation (EU) 2018/1725 from European Union Institutions, bodies, offices and agencies to international organisation

Annex 1

EDPS model template arrangement for data transfers from an Union institution, body, office or agency to an International Organisation

Administrative Arrangement

for the transfer of personal data from

Name of EU institution/body/office/agency

(_____)

to

Name of International Organisation

(_____)

Hereinafter individually referred to as 'the Side' or collectively as 'the Sides',

(1) having regard to the need to ensure efficient international cooperation between the Sides acting in accordance with their public mandates, including mandates as established under international law;

(2) having regard to the need to process personal data to carry out the public mandate and exercise the official authority vested in the Sides;

(3) recognising the importance of the right to privacy under international human rights law and the right to personal data protection as a fundamental right under European Union law;

(4) recognising that the transfer of personal data by EU institutions and bodies to international organisations should not undermine the protection of natural persons that is ensured in the European Union;

(5) recognising the privileges and immunities granted to [name of international organisation] under [add reference] as well as to [the EUI] under Protocol VII of the Treaties on the Functioning of the European Union[35];

have reached the following understanding:

ARTICLE 1 SUBJECT MATTER AND SCOPE

1.1 The Sides should apply this administrative arrangement ('AA') to personal data transferred by the transferring Side to the receiving Side. The annexes form an integral part of the AA and may be amended only with the agreement of both Sides.

1.2 The receiving Side confirms that it guarantees the safeguards set out in this AA, including enforceable and effective data subject rights, under its legal framework. Nothing in the arrangement establishes a binding legal obligation for either Side.

1.3 The details of the transfer(s), including the categories of personal data to be transferred and the purpose of processing, are specified in Annex I.B.

ARTICLE 2 DEFINITIONS

For the purpose of this AA the following definitions apply:

2.1 '**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); 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;

2.2 '**processing of personal data**' means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

2.3 '**applicable data protection framework**' means:

For the EU institution, body, office or agency: Regulation (EU) 2018/1725[36].

[35] Consolidated version of the Treaty on the Functioning of the European Union, Protocol (No 7) on the privileges and immunities of the European Union, OJ C 326, 26.10.2012, p. 266–272.
[36] 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.

For the IO: [*applicable (internal) legal framework governing the protection of personal data*].

2.4 '**transferring Side**' means [EU institution or body], transfers the personal data under this AA;

2.5 '**receiving Side**' means [international organisation], which receives personal data from the transferring Side under this AA;

2.6 '**onward transfer**' means transfer of personal data by a receiving Side to any entity that is not a Side signatory of this AA (´third party´);

2.7 '**personal data breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

[If other/additional terms are used in the AA (e.g. in light of the purpose of the transfer, type of data transferred, etc.), the Sides should agree on the applicable definitions. For example:

*2.8 '**special categories of personal data**' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation or personal data relating to criminal convictions and offences.*

ARTICLE 3 PERSONAL DATA PROTECTION SAFEGUARDS

3.1 Purpose limitation

The receiving Side should only process the personal data for the purposes as set out in Annex I.B. or for archiving purposes in the public interest scientific or historical research purposes or statistical purposes. In the latter cases, the receiving Side should put specific appropriate technical and organisational measures in place to ensure the security of the data to safeguard the rights and freedoms of the data subjects.

[The AA could also allow the processing of personal data for other compatible purposes. In order to ascertain whether such additional purposes are compatible with the initial purpose(s) of collection, the Sides should take account of, inter alia, the link between the initial purpose(s) and such additional purposes, the situation in which the personal data were collected, including the reasonable expectations of the data subjects as to the further use, the nature of personal data and the impact of the further data processing on data subjects and the applicable safeguards to ensure fair processing and to prevent any undue impact on the data subjects. In that case, the Sides should agree on those compatible purposes and list them in Annex I.B). Where appropriate, a requirement for additional safeguards (or the specific safeguards themselves) should be agreed (similar to the processing of personal data for archiving, statistics or scientific research).]

3.2 **Data accuracy and minimisation**

3.2.1 The transferring Side should only transfer personal data that are adequate, relevant and limited to what is necessary for the purposes for which they are transferred and further processed.

3.2.2 Each Side should ensure that the personal data is accurate and, where necessary, kept up to date. Where a Side becomes aware that personal data it has transferred to, or received from, another Side is incorrect or outdated, it should without delay notify the other Side about the incorrect or outdated data. The Sides should take every reasonable step, having regard to the purposes for which the personal data have been transferred and are further processed, to correct, supplement, or erase inaccurate personal data.

3.3 **Storage limitation**

The receiving Side should retain personal data for no longer than is necessary for the purpose for which the data are transferred and subsequently processed, including for compatible purposes, as specified in Annex I. *[The Sides should indicate the period for which the data will be retained in the annex, or, if that is not possible, the criteria to determine that period.*]

3.4 **Integrity and confidentiality**

3.4.1 The receiving Side should have in place appropriate technical and organisational measures to ensure the security of the personal data that are transferred to it, including to protect them against accidental or unlawful access, destruction, loss, alteration, or unauthorised disclosure. Such measures should include appropriate administrative, technical and physical security measures. In assessing the appropriate level of security, account should be taken of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject.

3.4.2 If the receiving Side becomes aware of a personal data breach concerning personal data received under this AA, it should inform the transferring Side without undue delay and take appropriate measures to address the personal data breach and mitigate its potential adverse effects. The information should include i) a description of the nature of the breach, ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible to provide all the information at the same time, it may be provided in phases without undue further delay.

ARTICLE 4 DATA SUBJECT RIGHTS

4.1 **Transparency**

4.1.1 The transferring Side should provide individual information to data subjects about the transfer of their personal data to the receiving Side, as well as of any additional information that may be required in compliance with Regulation 2018/1725.

4.1.2 The receiving Side should make available to the concerned data subjects a public privacy statement on its website and if necessary also by other means. This general notice should include information at least on the categories of data transferred and processed, how the data is processed, the relevant tool used for the transfer, the purpose of the processing, third parties or categories of third parties to whom the information may be onward transferred, individual rights and available mechanisms to exercise their rights and obtain redress as well as the contact details for submitting a request or complaint.

4.1.3 Upon request, the Sides should make a copy of this AA available to a data subject, free of charge. To the extent necessary to protect confidential information, including personal data, the Sides may redact parts of the text of the Annexes prior to sharing a copy, but should provide a meaningful summary if the data subject would otherwise not be able to understand its content or exercise their rights.

4.2 Data subject rights

4.2.1 Upon request from a data subject, the receiving Side should, without undue delay:

4.2.1.1 Confirm to the data subject whether or not personal data concerning them is being processed (right to access), and provide:

(a) information on the categories of data, purpose of processing, recipients or categories of recipients to whom the data has been or will be disclosed, the envisaged retention period (or, if that is not possible, the criteria used to determine that period), the existence of other data subject rights and how to obtain redress; the source of the personal data if it was not collected from the data subject, the appropriate safeguards in place to transfer the personal data, and

(b) a copy of the personal data without adversely affecting the rights and freedoms of others individuals.

4.2.1.2 Rectify their personal data that is incomplete, inaccurate or outdated.

4.2.1.3 Erase personal data concerning them that has been processed in violation of the safeguards in this AA or that is no longer necessary in relation to the purposes for which it has been lawfully processed.

4.2.1.4 Stop processing personal data if the data subject objects to it on grounds relating to their particular situation, unless there are compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject.

4.2.2 The receiving Side should inform the data subject on the action taken on their request without undue delay, and in any event within one month of the request.

4.2.3 The receiving Side may take appropriate steps, such as declining to act on a request, where requests from the data subject are manifestly unfounded or excessive, in particular because of their repetitive character. If the receiving Side does not take action on the request

of the data subject, it should also inform the data subject of the reasons thereof and of the possibility to file a complaint with an oversight body or seek redress.

4.2.4 If applicable under the data protection framework of the receiving Side, the Sides should include in the AA specific exceptions where necessary to protect important objectives of public interest or essential functions under the mandate of the receiving Side (including internal investigations or audits connected thereto) or the rights and freedoms of others, subject to respect for the principle of proportionality This may for instance include an exception to the right of erasure, to the extent that the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the exercise of the right is likely to render impossible or seriously impair the achievement of the objectives of that processing and appropriate safeguards are put in place.]

4.3 Automated decision making

The receiving Side should not take a decision which produces legal effects concerning a data subject or similarly significantly affects them based solely on automated processing of personal data, including profiling, without human involvement.]

ARTICLE 5 ONWARD TRANSFERS OF PERSONAL DATA

5.1 The receiving Side may only onward transfer the personal data, if this is necessary for the fulfilment of its mandate and the purposes as described in Annex I. and if the other requirements of the AA are fulfilled, provided that the conditions set out it 5.2 or in 5.3 are also met.

5.2 In addition to the requirements of 5.1, the receiving Side may only onward transfer the personal data to a third party located outside of the EEA or to an international organisation if:

a) the country where the third party is located or the international organisation benefits from an adequacy decision adopted by the European Commission pursuant to Article 45 of Regulation (EU) 2016/679 (adequacy decision) that covers the onward transfer; or
b) the third party is listed in Annex IV and enters into a binding commitment to ensure the same level of data protection as provided by this AA, including with respect to the rights of data subjects; or
c) the transferring Side expressly authorises an onward transfer to a third party not listed in Annex IV that enters into a binding commitment to ensure the same level of data protection as provided by this AA, including with respect to the rights of data subjects. Before requesting the authorisation, the receiving Side should provide the information required under Annex IV. The transferring Side should keep a record of such notifications and provide its supervisory authority with this information upon request.

5.3 Where none of the conditions of 5.2 apply, the receiving Side may only onward transfer the personal data in exceptional cases, if the requirements of 5.1 are met and:

a) the receiving Side has obtained the explicit consent of the data subject for the onward transfer, after having informed them of its purpose(s), the identity of the recipient and the possible risks of such transfer in terms of applicable data protection safeguards; or
b) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person; or
c) the onward transfer is necessary for the establishment, exercise or defence of legal claims; or
d) for an important objective of public interest as also recognised by EU law and the third party commits to process the data only for the specific purpose(s) as described in Annex I.B for which it is onward transferred and to immediately delete it once the processing is no longer necessary for that purpose.

5.4 The receiving Side should notify the transferring Side of transfers referred to in paragraph

5.5 Before they take place by providing the information required under Annex IV, or, if that is not possible, immediately thereafter. The transferring Side should keep a record of such notifications and provide its oversight body with this information upon request.

ARTICLE 6 REQUESTS FOR ACCESS FROM NATIONAL AUTHORITIES

6.1 The receiving Side agrees to notify the transferring Side if it receives a request from a public authority for the disclosure of personal data transferred pursuant to this AA, or if it becomes aware of direct access by a public authority to such data. If the receiving Side is prohibited from notifying the transferring Side, the receiving Side agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible and document the procedure.

6.2 The receiving Side agrees to review the legality of the request for disclosure, including in light of its own privileges and immunities and whether it remains within the powers granted to the requesting public authority, and to challenge or appeal the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country requesting disclosure, applicable obligations under international law and principles of international comity. The receiving Side agrees to document its legal assessment and any challenge to the request for disclosure and make it available to transferring Side upon request.

6.3 If the receiving Side decides in accordance with its applicable legal framework that it will disclose personal data transferred pursuant to this AA in response to a request from a public authority, including by waiving applicable privileges and immunities, the Sides should cooperate in view of seeking the best protections available.

[Additional clauses, if relevant in the context of the AA:

[ARTICLE 7] SPECIAL CATEGORIES OF PERSONAL DATA

The receiving Side should apply specific restrictions and/or additional safeguards adapted to the specific nature of special categories of personal data and the risks involved in the processing of such data. This may include for example restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation or encryption of the data in transit) and/or additional restrictions with respect to further disclosure.]

ARTICLE 8 REDRESS

8.1 The receiving Side confirms that it will effectively and timely handle and resolve complaints from data subjects relating to the processing of their personal data.

8.2 In case a complaint cannot be resolved amicably by the receiving Side, a data subject has the right to obtain effective redress and effective remedy before a pre-established mechanism that ensures independent and impartial adjudication, in accordance with principles of due process and binds the receiving Side. Where the applicable conditions are fulfilled, this should include the possibility to obtain compensation for damages.

8.3 For the purpose of this AA, such redress will be ensured by [*insert reference, e.g. to binding arbitration, administrative tribunal/mechanism within the international organisation or established at international level without prejudice to the possibility to use judicial or quasi-judicial mechanisms in case the Sides wish to do so. Whatever the mechanism is, it should meet the requirements set out in the previous paragraph and it must be established /agreed before the signature of the AA and available throughout the duration of the AA.*].

8.4 The receiving Side should inform the transferring Side about complaints it receives concerning the processing of personal data under this AA and their resolution without undue delay.

ARTICLE 9 INDEPENDENT OVERSIGHT

9.1 Compliance of the processing of personal data with this AA should be subject to oversight by an external or internal body including a functionally autonomous body that is independent and impartial (in particular, free from any influence or instructions; appointed for a fixed term on the basis of specific criteria through a transparent procedure; can only be dismissed for cause; has sufficient human, technical and financial resources) and has binding investigatory (e.g. to access to all relevant information) and remedial powers (e.g. to order the suspension of processing, order a change in processing, or order deletion of unlawfully processed data.

9.2 For the EU institution or body, such oversight will be ensured by the European Data Protection Supervisor.

9.3 For the international organisation, such oversight will be ensured by [*insert reference*].

ARTICLE 10 IMPLEMENTATION, REVISION AND TERMINATION

10.1 The Parties should jointly review the implementation of the AA on a regular basis.

10.2 In the event of substantial change in their legal frameworks affecting the operation of this AA, the Sides should enter into consultations with a view to adapt the AA where necessary.

10.3 The Sides should respond to inquiries from the other side concerning the effective implementation of the safeguards in the AA without undue delay.

10.4 In the event that the receiving Side is unable to effectively implement this AA for any reason, it should promptly inform the transferring Side, in which case both parties should enter into consultations with a view to adapt the AA where necessary.

10.5 In situations where the receiving Side is in breach of or unable to comply with the safeguards set out in this AA, the transferring Side should suspend the transfer of personal data under this AA until compliance is again ensured. The transferring Side may also suspend or terminate the transfer of personal data where the parties do not succeed in resolving disputes amicably until it considers that the issue has been addressed by the receiving Side satisfactorily.

10.6 The transferring Side may terminate the AA where the receiving Side is in substantial or persistent breach of the arrangements set out in this AA. In this case, the receiving Side should, at the choice of the transferring Side, return without undue delay all the personal data transferred and the copies thereof, or destroy all the personal data and certify to the transferring Side that it has done so. Until the data is deleted or returned, the receiving Side should continue to ensure compliance with this AA. If its internal legal framework prevents the receiving Side from returning or destroying all or part of the personal data transferred, the receiving Side warrants that it should continue to ensure compliance with this AA and should only process the data to the extent and for as long as required under its legal framework.

10.7 If a Side wishes to terminate this AA for other reasons than the ones laid down in paragraph.

10.8 The Sides may agree that the receiving Side should continue to process personal data already transferred pursuant to this AA. In this case the personal data should be processed in compliance with the safeguards provided in this AA.

[Possible additional clauses, if relevant in the context of the AA, e.g. regulating a possible termination of the AA, on dispute resolution between the Sides on the application of this arrangement (e.g. final and binding arbitration in accordance with the Permanent Court of Arbitration Optional Rules for Arbitration Involving International Organisations and States), etc.]

ANNEX I

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or set of transfers and, in this regard, to determine the respective role(s) of the Sides as transferring side(s) and/or receiving side(s). This does not necessarily require completing and signing separate sets of annexes for each transfer/set of transfers, where this transparency can be achieved through one set of annexes. However, where necessary to ensure sufficient clarity, separate sets of annexes should be used.

A. LIST OF SIDES

I.	**TRANSFERRING SIDE**	
	Name:	
	Address:	
	Contact person's name, position and contact details:	
	Signature and date:	
II.	**RECEIVING SIDE**	
	Name:	
	Address:	
	Contact person's name, position and contact details:	
	Signature and date:	

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred	
Categories of personal data transferred	
Special categories of personal data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including	

access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	
Purpose(s) of the data transfer and further processing, including how they relate to the mandate of the Sides for the processing. [Processing for further compatible purposes may for example include processing for internal audits or internal investigations or where necessary to protect the vital interests of an individual or for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes.]	
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	

ANNEX II

APPLICABLE DATA PROTECTION FRAMEWORK

Description/summary/reference to the data protection framework applicable to the IO, including substantive rules (e.g. data protection principles, individual rights) and procedural safeguards (oversight and redress mechanisms), as well as the IO's Privileges and Immunities.

ANNEX III

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms; in particular, it is necessary to clearly indicate which measures apply to each transfer/set of transfers. See in this respect also the explanatory note to Annex I.

Description of the technical and organisational measures implemented by the receiving side(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure

ANNEX IV

ONWARD TRANSFERS

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each onward transfer or set of onward transfers and, in this regard, to determine the respective the recipient(s) and their role, the categories of personal data involved, the reasons and purposes of onward transfer, the third countries or international organisations involved and the applicable technical and organisational measures implemented by the receiving Side and the recipient.

Categories of data to be onward transferred

Purposes of the onward transfers

Recipients or categories of recipients to which personal data will be onward transferred, including the country where they are located or the international organisation of which they are part.

Ground for the onward transfer pursuant to Article 5 of the present AA.