Annex I

Instructions to use the model administrative arrangement:

Articles 3(3), 8(3), 9(3) and the annexes shall be filled out and adapted by including the requested information on the specific circumstances of the transfer. Indicating the requested information for these sections is a pre-condition to assess an authorisation request.

Optional clauses may be used to adapt the model administrative arrangement to the specific circumstances of the transfers. In case the optional clauses are not included in the text, they should be deleted.

Instructions in blue and **explanatory notes** in the annexes should be deleted, once the requested information is included in the text.

Administrative Arrangement

for the transfer of personal data from

Name of EU

institution/body/office/agency ()

to

Name of public authority in the

third country (_____)

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

(1) having regard to the need to ensure efficient international cooperation between the Parties acting in accordance with their tasks carried out in the public interest

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

(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 public authorities in third countries should not undermine the protection of natural persons that is ensured in the European Union;

OPTIONAL CLAUSE 1

Text to be added together with optional clauses 6 and 7 and adapted in case the third country of destination made international commitments to accord privileges and immunities to the transferring EUI (in accordance with the customary privileges, immunities and facilities accorded to international organisations by international public law) and enacted in its national legislation:

(5) [recognising customary privileges, immunities and facilities accorded to European Union institutions, bodies, offices and agencies by international public law and in particular the privileges and immunities granted to [the EUI] by [the third country of destination] under its laws,]

have reached the following understanding:

ARTICLE 1 SUBJECT MATTER AND SCOPE

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

1.2 The receiving Party 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 Party.

I.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[1].

For the authority in the third country: [*applicable (internal) legal framework governing the protection of personal data*].

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

2.5 '**receiving Party**' means [third country authority], which receives personal data from the transferring Party under this AA;

2.6 '**onward transfer**' means transfer of personal data by a receiving Party to any entity that is not a Party 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;

OPTIONAL CLAUSE 2

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 Parties should agree on the applicable definitions. For example, in case special categories of data are transferred under the arrangement, the definition below should be included together with optional clause 8:

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.

[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.

ARTICLE 3 PERSONAL DATA PROTECTION SAFEGUARDS

3.1 Purpose limitation

The receiving Party 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 Party 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.

OPTIONAL CLAUSE 3

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 Parties 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 Parties 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 Party 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 Party should ensure that the personal data are accurate and, where necessary, kept up to date. Where a Party becomes aware that personal data it has transferred to, or received from, another Party is incorrect or outdated, it should without delay notify the other Party about the incorrect or outdated data. The Parties 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 Party 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 Parties 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 Party 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 Party becomes aware of a personal data breach concerning personal data received under this AA, it should inform the transferring Party 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 Party should provide individual information to data subjects about the transfer of their personal data to the receiving Party, as well as of any additional information that may be required in compliance with Regulation 2018/1725.

4.1.2 The receiving Party 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 are 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 Parties 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 Parties 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 Party 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 Party 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 Party 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 Party 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.

OPTIONAL CLAUSE 4

Clause to be inserted in case the transfer involves pseudonymized personal data

[4.2.4] If the receiving Party receives a request from a data subject, but it is not able to confirm their identity due to pseudonymization by the transferring Party, the receiving Party should contact the transferring Party without delay to provide support and cooperation to handle the request.

OPTIONAL CLAUSE 5

If applicable under the data protection framework of the receiving Party, the Parties 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 Party (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 Party 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 Party may only onward transfer the personal data, if this is necessary for the fulfilment of its tasks carried out in the public interest or in the exercise of official authority vested in it and the purposes as described in Annex I. and if the other requirements of the AA are fulfilled, provided that the conditions set out in 5.2 or in 5.3 are also met.

5.2 In addition to the requirements of 5.1, the receiving Party 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 Party 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 Party should provide the information required under Annex IV. The transferring Party 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 Party may only onward transfer

the personal data in exceptional cases, if the requirements of 5.1 are met and:

a) the receiving Party 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 Party should notify the transferring Party of transfers referred to in paragraph 5.3 before they take place by providing the information required under Annex IV, or, if that is not possible, immediately thereafter. The transferring Party 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 Party agrees to notify the transferring Party, and, where possible, the data subject promptly if it receives a request from a public authority under the laws of the country of destination or from a public authority of another third country 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. Such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided for requests and, for direct access, all information available to the receiving Party.

6.2 If the receiving Party is prohibited from notifying the transferring Party or the data subject under the laws of the country of destination or under the laws of the requesting third country, the receiving Party 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 to document the procedure. The receiving Party agrees to document its best efforts in order to be able to demonstrate them on request of the transferring Party.

6.3 Where permissible under the laws of the country of destination or under the laws of the requesting third country, the receiving Party agrees to provide the transferring Party, at regular intervals for the duration of this AA, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

6.4 The receiving Party agrees to preserve the information pursuant to paragraphs 6.1 to 6.3 for the duration of this AA and make it available to the competent supervisory authority on request.

6.5 Paragraphs 6.1 to 6.3 are without prejudice to the obligation of the receiving Party pursuant to Article 10.2 and Article 10.6 to inform the transferring Party promptly where it is unable to comply with this administrative arrangement.

6.6 The receiving Party agrees to review the legality of the request for disclosure, 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 of destination or under the laws of the requesting third country, applicable obligations under international law and principles of international comity. When challenging a request, the receiving Party shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the receiving Party under Article 10.3 and Article 10.7.

OPTIONAL CLAUSE 6

This clause shall replace Article 6.6 in case the third country of destination made international commitments to accord privileges and immunities to the transferring EUI (in accordance with the customary privileges, immunities and facilities accorded to international organisations by international public law) and enacted in its national legislation. This clause should be inserted together with optional clauses 1 and 7.

6.6 The receiving Party agrees to review the legality of the request for disclosure, including in light of any privileges and immunities accorded to the transferring Party by the laws of the country of destination or by the laws of the requesting third country 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 of destination or under the laws of the requesting third country, applicable obligations under international law and principles of international comity. When challenging a request, the receiving Party shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the receiving Party under Article 10.3 and Article 10.7.

6.7 The receiving Party agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination or under the laws of the requesting third country, make it available to transferring Party and the competent supervisory authority upon request.

6.8 The receiving Party agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

OPTIONAL CLAUSE 7

Clause to be inserted together with Clause 1 and 6 in case the third country of destination made international commitments to accord privileges and immunities to the transferring EUI (in accordance with the customary privileges, immunities and facilities accorded to international organisations by international public law) and enacted in its national legislation.

6.9 Where the request received by the receiving Party concerns information falling under the privileges and immunities of the transferring Party accorded to it by the country of destination or by the requesting third country, the receiving Party shall promptly inform the requesting public authority and promptly notify the transferring Party, so that the transferring Party may decide to waive or not its privileges and immunities in the context of that request.

ARTICLE 7 SPECIAL CATEGORIES OF PERSONAL DATA

7.1 The transfer will not involve 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 ('special categories of data').

OPTIONAL CLAUSE 8

The receiving Party 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) prohibition to attempt re-identification of data subjects, adequate training of and information to personnel that has access to special categories of personal data transferred and/or additional restrictions with respect to further disclosure. The specific measures need to be listed in Annex I.B, but measures listed in Annex III also apply.

This clause shall replace Article 7.1 in case special categories of personal data is transferred under the arrangement:

7.1 Where the transfer involves special categories of personal data as defined in Article 2.8, the receiving Party should apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. The receiving Party should put in place the specific measures listed in Annex I.B for the transfer of special categories of personal data as well as the technical and organizational measures foreseen in Annex III with the purpose of adequately protecting such personal data that the receiving Party might be processing pursuant to this Administrative Arrangement.

ARTICLE 8 REDRESS

8.1 The receiving Party 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 Party, 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 Party. 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, to available judicial redress or in the absence thereof, to quasi judicial mechanisms, binding arbitration, administrative tribunal/mechanism within the third country of destination or established at international level . 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 Party should inform the transferring Party 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 transferring Party, such oversight will be ensured by the European Data Protection Supervisor.

9.3 For the receiving Party, such oversight will be ensured by [*insert reference, e.g. the data protection authority competent for the receiving Party*].

ARTICLE 10 IMPLEMENTATION, REVISION AND TERMINATION

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

10.2 The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 25(1) of Regulation (EU) 2018/1725, are not in contradiction with this administrative arrangement.

10.3 The receiving Party agrees to notify the transferring Party promptly if, after having agreed to this administrative arrangement and for its duration, it has reason to believe that it is or has become subject to laws or practices that prevent the receiving Party from fulfilling its obligations under this administrative arrangement, including following a change in the laws of the third country or a measure (such as a disclosure request).

10.4 Following a notification pursuant to paragraph 10.3, or if the transferring Party otherwise has reason to believe that the receiving Party can no longer fulfil its obligations under this administrative arrangement, the transferring Party shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the transferring Party and/or receiving Party to address the situation. The transferring Party shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the transferring Party shall be entitled to terminate the administrative arrangement. Where the administrative arrangement is terminated pursuant to this Article, paragraph 10.9 shall apply.

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

10.6 The Parties should respond to inquiries from the other Party concerning the effective implementation of the safeguards in the AA without undue delay.

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

10.8 In situations where the receiving Party is in breach of or unable to comply with the safeguards set out in this AA, the transferring Party should suspend the transfer of personal data under this AA until compliance is again ensured. The transferring Party 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 Party satisfactorily.

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

10.10 If a Party wishes to terminate this AA for other reasons than the ones laid down in paragraph 10.4 the Parties may agree that the receiving Party 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.

OPTIONAL CLAUSE 9

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 Parties 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 Parties as transferring Party(ies) and/or receiving Party(ies). 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 PARTIES

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

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data are 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 Parties for the processing.	
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

[EXPLANATORY NOTE:

Description/summary/reference to the data protection framework applicable to the public authority in the third country (the requesting Party), including substantive rules (e.g. data protection principles, individual rights) and procedural safeguards (oversight and redress mechanisms), as well as any privileges and immunities accorded to the EUI (the transferring Party) by the third country of destination under that country's laws]

ANNEX III

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The receiving Party should implement the following technical and organisational measures (or equivalent):

[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 Party(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]

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 Party 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.