Document 1.

A document prepared by Prof. Dr Gert Vermeulen February 2019: draft amendments and Schedule Two to the Arrangement subsequently amended by the author in April 2019 to reflect inputs from FTC, Mexico and Turkey.

Draft amendments & Schedule Two to the Global Cross Border Enforcement Cooperation Arrangement

Gert Vermeulen
Privacy Commissioner, Belgian DPA
Senior Full Professor International and European Criminal Law, Direc
tor Institute for International Research on Criminal Policy (IRCP), Director Knowledge and Research Platform on Privacy, Information Exchange, Law Enforcement and Surveillance (PIXLES), Department Chair Criminology, Criminal Law and Social Law, Faculty of Law, Ghent University

---

1. Draft amendments to the Global Cross Border Enforcement Cooperation Arrangement

[…]

4. NATURE OF THE ARRANGEMENT
(1) This Arrangement sets forth the Participants' commitment with regard to international cross-border privacy enforcement cooperation, particularly on reciprocity, confidentiality, data protection, and coordination.
This Arrangement is NOT intended to:
(i) replace existing national and regional conditions or mechanisms for sharing information, or to interfere with similar arrangements by other networks:
(ii) create legally binding obligations, or affect existing obligations under other arrangements or international or domestic law;
(iii) prevent a Participant from cooperating with other Participants or non-participating PEAs, pursuant to other (binding or non-legally binding) laws, agreements, treaties, or arrangements.
(iv) create obligations or expectations of cooperation that would exceed a Participant's scope of authority and jurisdiction; or
(v) compel Participants to cooperate on enforcement activities including providing nonconfidential or confidential information which may or may not contain personal data.
(2) By derogation of point (1), 2nd paragraph, under (i) and (ii) of this Section, for Participants entering into Schedule Two, the latter shall constitute a legally binding and enforceable commitment.

[…]

7. RESPECTING PRIVACY AND DATA PROTECTION PRINCIPLES
Depending on Participants or the enforcement activity in question, it may be necessary to exchange personal data. However, in accordance with recognised privacy and data protection principles, the exchange of such personal data should be limited to what is necessary for effective privacy and data protection enforcement. All Participants to this Arrangement who either disclose or receive personal data will use their best efforts to respect the data protection safeguards of each other. However, it is recognised that these best efforts alone will not always be sufficient to enable the exchange of personal data.
In that case, if the Participant disclosing the personal data requires specific data protection safeguards, they should either:
- request the other Participants to provide assurance that they will comply with the requirements outlined in Schedule One; or,
- request the other Participants to provide assurance that they will comply with the requirements outlined in Schedule Two; or,
- make other arrangements between those who disclose and receive personal data to ensure that each Participant's privacy and data protection requirements are fully observed.
Participants should notify the Committee if they are committing to the requirements set out in Schedule

One or Schedule Two or notify the Committee of other arrangements as referenced above. In principle, this notification should be done when submitting a notice of intent to participate in accordance with section 13, or, in any case before receiving personal data from another Participant under this Arrangement. A list of Participants, including their initial and updated notifications regarding Schedule One and/or Schedule Two and/or other arrangements as described above, will be made available to all Participants.

[…]

12. ELIGIBILITY CRITERIA
Any PEA may submit a notice of intent to the Committee indicating that they intend to participate in this Arrangement:
(i) As a Member, if they are an accredited member of the International Conference of Data Protection and Privacy Commissioners (the Conference) and, as such, fulfil the membership requirements of Paragraph 5.1 of the Rules and Procedures of the Conference, including the requirement of appropriate autonomy and independence; or
(ii) As a Partner if, although not an accredited member of the Conference, they are:
a. from a Member State signatory to the Convention for the Protection of Individuals with Regard to Automatic Processing (Convention 108); or
b. a member of the Global Privacy Enforcement Network (GPEN); or
c. a Participant in the APEC Cross-border Privacy Enforcement Arrangement (CPEA); or
d. a member of the European Data Protection Board.
The Committee will keep an updated list of all PEAs that have committed to participate in the Arrangement and of all Participants that have committed to respect Schedule One or Schedule Two or that have submitted a notice in accordance with section 5. The list should be easily available to all Participants.

[…]

13 ROLE OF THE INTERNATIONAL CONFERENCE EXECUTIVE COMMITTEE
The Committee will:
a. Receive notices of intent to participate in or withdraw participation in this Arrangement;
b. Receive notices of commitment to Schedule One or Schedule Two or such other arrangements as referenced in clause seven above and notices submitted in accordance with section 5;
c. Review such notices in order to verify that a PEA is eligible to sign this Arrangement;
d. Review the operation of the Arrangement three years after its commencement and submit its findings to the International Conference;
e. Publicise this Arrangement;
f. Recommend to the International Conference, upon due consideration of evidence, that a Participant to this Arrangement should have their participation suspended. Or, in the most serious cases of breach of the requirements set out in this Arrangement or in Schedule One or Schedule Two, where the Participant concerned has entered into either one of the latter, and thus breaching the trust that this Arrangement establishes between Participants, recommend to the International Conference that the Participant should be excluded from the Arrangement.

2. Draft SCHEDULE TWO

Article 1 - Legally binding and enforceable safeguards securing an appropriate level of data protection

1. For Participants entering into this Schedule, the latter shall constitute a legally binding and enforceable commitment, in derogation of point (1), 2nd paragraph, under (i) and (ii) of Section 4 of this Arrangement.

2. For ~~recipient~~ Participants ~~which are subject to the jurisdiction of a non-EU Member State or of a State or international organisation which is not Party to the Modernised Convention for the protection of individuals with regard to Automatic Processing of Personal Data (ETS No. 108)~~ which have entered into this Schedule, the latter shall be deemed to provide appropriate data protection safeguards and to secure an appropriate level of data protection~~n~~.

3. Even for Participants which have not entered into Schedule One, the safeguards in the latter form an integral part of this Schedule. In case of inconsistency between their respective provisions, the provision of either one of both Schedules offering the widest protection to data subjects shall prevail.

4. None of the provisions of this Schedule shall be interpreted as limiting or otherwise affecting the possibility or obligation for a Participant to grant data subjects a wider measure of protection than that stipulated in this Schedule.

5. Onward transfers of personal data by a Participant which is the initial recipient of the original data transfer shall be permitted only where the further recipient ~~is either subject to the jurisdiction of an EU Member State or of a State or international organisation which is Party to the Modernised Convention for the protection of individuals with regard to Automatic Processing of Personal Data (ETS No. 108) or~~ has entered into this Schedule, or can otherwise provide similar safeguards.

6. Participants entering into this Schedule shall constitute data controllers, and make sure that, where applicable, provide that their processors also comply with the relevant provisions of this Schedule.

Article 2 – Definitions

For the purposes of this Schedule:

a. ~~a.~~ "personal data" means any information relating to an identified or identifiable individual ("data subject"), including data from which it is practicable that the identity of the individual can be directly or indirectly ascertained;

b. "genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

c. "biometric data" means personal data resulting from specific technical processing relating to the physical, physio- logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

~~a.~~ ~~b.~~ "data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, use, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;

d.

~~b.~~ ~~c.~~ Where automated processing is not used, “data processing” means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

e.

~~c.~~ ~~d.~~ “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;

f.

~~d.~~ ~~e.~~ “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

g.

h. ~~f.~~ “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

Article 3 – Legitimacy of data processing and quality of data

1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.

2. Personal data undergoing processing shall be processed lawfully.

3. Personal data undergoing processing shall be:

a. processed fairly and in a transparent manner;
b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

Article 4 – Sensitive data~~pecial categories of data~~

~~1.~~ The processing of sensitive data, including~~:~~

- genetic data;
- personal data relating to offences, criminal proceedings and convictions, and related security measures;
- biometric data ~~uniquely identifying a person~~;
- personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life,

shall only be allowed where appropriate safeguards, ~~are enshrined in law,~~ complementing those of this Schedule, ~~.~~

~~2. Such safeguards shall~~ guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

Article 5 – Data security

Each Participant takes~~, or~~ appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.

Article 6 – Transparency of processing

1. Each Participant shall inform the data subjects of:

a. its identity and habitual residence or establishment;
b. the legal basis and the purposes of the intended processing;
c. the categories of personal data processed;

d. the recipients or categories of recipients of the personal data, if any; and
e. the means of exercising the rights set out in Article 7,

as well as any necessary additional information in order to ensure fair and transparent processing of the personal data.

2. Paragraph 1 shall not apply where the data subject already has the relevant information.

3. Where the personal data are not collected from the data subjects, the Participant shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

Article 7 – Rights of the data subject

1. Every individual shall have a right:

a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;
b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the Participant is required to provide in order to ensure the transparency of processing in accordance with Article 6, paragraph 1;
c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;
d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the Participant demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;
e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Schedule;
f. to have a remedy under Article 11 where his or her rights under this Schedule have been violated;

2. Paragraph 1.a shall not apply if the decision is authorised by a law to which the Participant is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

Article 8 – Additional obligations

1. Each Paricipant shall take all appropriate measures to comply with the obligations of this Schedule and be able to demonstrate that the data processing under its control is in compliance with the provisions of this Schedule.
2. Each Paricipant shall examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.
3. Each Paricipant shall implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

Article 9 – Exceptions and restrictions

1. No exception to the provisions set out in Articles 3-8 shall be allowed except to the provisions of Article 3 paragraph 34, Article 6 paragraph 1 and Article 7, when such an exception is provided for by the laws to which the Participant is subject, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;
b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

2. Restrictions on the exercise of the provisions specified in Articles 6 and 7 may be provided for by the laws to which the Participant is subject with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.

Article 10 – Safeguards in co-operation between Participants

1. The Participants shall not exchange or share personal data undergoing processing unless such data are essential for co-operation, or where the data subject concerned has given explicit, specific, free and informed consent to its provision.

2. A Participant which has received information from another Participant, either accompanying a request or in reply to its own request, shall not use that information for purposes other than those specified in the request.

3. In no case will a Participant be allowed to make a request on behalf of a data subject of its own accord and without the express approval of the data subject concerned.

Article 11 – Sanctions and remedies

Violations of the provisions of this Schedule may give rise to all judicial and non-judicial sanctions and remedies available under the laws to which the violating Participants are subject.

Document 2.

An explanatory table prepared by Prof. Dr Gert Vermeulen February 2019 to accompany Document 1. subsequently amended by the author in April 2019 to reflect inputs from FTC, Mexico and Turkey.

Column 1: correspondence to the remarks of the CoE T-PD

Column 2: draft amendments and Schedule Two

Council of Europe T-PD	Draft amendments to the Global Cross Border Enforcement Cooperation Arrangement (Gert Vermeulen)
[...] the committee stresses the importance of ensuring that the conditions set out in Section 7 and Schedule I of the Arrangement fully meet the requirements of the modernised Convention 108, in particular with regard to Chapter II and Chapter III, and in particular article 14.3, of the Convention which contain the general provisions and establish the basic principles of data protection.	
Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data	
Chapter III – Transborder flows of personal data	
Article 14 – Transborder flows of personal data 1. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation. 2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured. 3. An appropriate level of protection can be secured by: a. the law of that State or international organisation, including the applicable international treaties or agreements; or b. ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing. 4. Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data a. the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or b. the specific interests of the data subject require it in the particular case; or c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or d. it constitutes a necessary and proportionate measure in a democratic society for freedom of expression. 5. Each Party shall provide that the competent supervisory authority within the meaning of Article 15 of this Convention is provided with all relevant information concerning the transfers of data referred to in paragraph 3.b and, upon request, paragraphs 4.b and 4.c. 6. Each Party shall also provide that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.	4. NATURE OF THE ARRANGEMENT (1) This Arrangement sets forth the Participants' commitment with regard to international cross-border privacy enforcement cooperation, particularly on reciprocity, confidentiality, data protection, and coordination. This Arrangement is NOT intended to: (i) replace existing national and regional conditions or mechanisms for sharing information, or to interfere with similar arrangements by other networks: (ii) create legally binding obligations, or affect existing obligations under other arrangements or international or domestic law; (iii) prevent a Participant from cooperating with other Participants or non-participating PEAs, pursuant to other (binding or non-legally binding) laws, agreements, treaties, or arrangements. (iv) create obligations or expectations of cooperation that would exceed a Participant's scope of authority and jurisdiction; or (v) compel Participants to cooperate on enforcement activities including providing nonconfidential or confidential information which may or may not contain personal data. (2) By derogation of point (1), 2nd paragraph, under (i) and (ii) of this Section, for Participants entering into Schedule Two, the latter shall constitute a legally binding and enforceable commitment.

	7. RESPECTING PRIVACY AND DATA PROTECTION PRINCIPLES Depending on Participants or the enforcement activity in question, it may be necessary to exchange personal data. However, in accordance with recognised privacy and data protection principles, the exchange of such personal data should be limited to what is necessary for effective privacy and data protection enforcement. All Participants to this Arrangement who either disclose or receive personal data will use their best efforts to respect the data protection safeguards of each other. However, it is recognised that these best efforts alone will not always be sufficient to enable the exchange of personal data. In that case, if the Participant disclosing the personal data requires specific data protection safeguards, they should either: - request the other Participants to provide assurance that they will comply with the requirements outlined in Schedule One; or, - request the other Participants to provide assurance that they will comply with the requirements outlined in Schedule Two; or, - make other arrangements between those who disclose and receive personal data to ensure that each Participant's privacy and data protection requirements are fully observed. Participants should notify the Committee if they are committing to the requirements set out in Schedule One or Schedule Two or notify the Committee of other arrangements as referenced above. In principle, this notification should be done when submitting a notice of intent to participate in accordance with section 13, or, in any case before receiving personal data from another Participant under this Arrangement. A list of Participants, including their initial and updated notifications regarding Schedule One and/or Schedule Two and/or other arrangements as described above, will be made available to all Participants.
	12. ELIGIBILITY CRITERIA Any PEA may submit a notice of intent to the Committee indicating that they intend to participate in this Arrangement: (i) As a Member, if they are an accredited member of the International Conference of Data Protection and Privacy Commissioners (the Conference) and, as such, fulfil the membership requirements of Paragraph 5.1 of the Rules and Procedures of the Conference, including the requirement of appropriate autonomy and independence; or (ii) As a Partner if, although not an accredited member of the Conference, they are: a. from a Member State signatory to the Convention for the Protection of Individuals with Regard to Automatic Processing (Convention 108); or b. a member of the Global Privacy Enforcement Network (GPEN); or c. a Participant in the APEC Cross-border Privacy Enforcement Arrangement (CPEA); or d. a member of the European Data Protection Board. The Committee will keep an updated list of all PEAs that have committed to participate in the Arrangement and of all Participants that have committed to respect Schedule One or Schedule Two or that have submitted a notice in accordance with section 5. The list should be easily available to all Participants.
Chapter IV – Supervisory authorities	
Article 15 – Supervisory authorities 1 Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of 2 To this end, such authorities: a. shall have powers of investigation and intervention; b. shall perform the functions relating to transfers of data provided for under Article 14, notably the approval of standardised safeguards; c. shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions; d. shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention; e. shall promote: i. public awareness of their functions and powers as well as their activities;	13 ROLE OF THE INTERNATIONAL CONFERENCE EXECUTIVE COMMITTEE The Committee will: a. Receive notices of intent to participate in or withdraw participation in this Arrangement; b. Receive notices of commitment to Schedule One or Schedule Two or such other arrangements as referenced in clause seven above and notices submitted in accordance with section 5; c. Review such notices in order to verify that a PEA is eligible to sign this Arrangement; d. Review the operation of the Arrangement three years after its commencement and submit its findings to the International Conference; e. Publicise this Arrangement; f. Recommend to the International Conference, upon due consideration of evidence, that a Participant to this Arrangement should have their participation suspended. Or, in the most serious cases of breach of the requirements set out in this Arrangement or in Schedule One or Schedule Two, where the Participant concerned has entered into either one of the latter, and thus breaching the trust that this Arrangement establishes between Participants, recommend to the International

ii. public awareness of the rights of data subjects and the exercise of such rights; iii. awareness of controllers and processors of their responsibilities under this Convention; specific attention shall be given to the data protection rights of children and other vulnerable individuals. 3. The competent supervisory authorities shall be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data. 4. Each competent supervisory authority shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of progress. 5. The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions. 6. Each Party shall ensure that the supervisory authorities are provided with the resources necessary for the effective performance of their functions and exercise of their powers. 7. Each supervisory authority shall prepare and publish a periodical report outlining its activities. 8. Members and staff of the supervisory authorities shall be bound by obligations of confidentiality with regard to confidential information to which they have access, or have had access to, in the performance of their duties and exercise of their powers. 9. Decisions of the supervisory authorities may be subject to appeal through the courts. 10. The supervisory authorities shall not be competent with respect to processing carried out by bodies when acting in their judicial capacity.	Conference that the Participant should be excluded from the Arrangement.

	Draft SCHEDULE TWO
Chapter III – Transborder flows of personal data (REPEATED)	
Article 14 – Transborder flows of personal data 1. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation. 2. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the 3. An appropriate level of protection can be secured by: a. the law of that State or international organisation, including the applicable international treaties or agreements; or b. ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing. 4. Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data a. the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or b. the specific interests of the data subject require it in the particular case; or c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or d. it constitutes a necessary and proportionate measure in a democratic society for freedom of expression. 5. Each Party shall provide that the competent supervisory authority within the meaning of Article 15 of this Convention is provided with all relevant information concerning the transfers of data referred to in paragraph 3.b and, upon request, paragraphs 4.b and 4.c. 6. Each Party shall also provide that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.	**Article 1 - Legally binding and enforceable safeguards securing an appropriate level of data protection** 1. For Participants entering into this Schedule, the latter shall constitute a legally binding and enforceable commitment, in derogation of point (1), 2nd paragrapgh, under (i) and (ii) of Section 4 of this Arrangement. 2. For Participants which have entered into this Schedule, the latter shall be deemed to provide appropriate data protection safeguards and to secure an appropriate level of data protection. 3. Even for Participants which have not entered into Schedule One, the safeguards in the latter form an integral part of this Schedule. In case of inconsistency between their respective provisions, the provision of either one of both Schedules offering the widest protection to data subjects shall prevail. 4. None of the provisions of this Schedule shall be interpreted as limiting or otherwise affecting the possibility or obligation for a Participant to grant data subjects a wider measure of protection than that stipulated in this Schedule. 5. Onward transfers of personal data by a Participant which is the initial recipient of the original data transfer shall be permitted only where the further recipient has entered into this Schedule, or can otherwise provide similar safeguards. 6. Participants entering into this Schedule shall constitute data controllers, and make sure that, where applicable, provide that their processors also comply with the relevant provisions of this Schedule.
Chapter I – General provisions	
Article 1 – Object and purpose The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.	
Article 2 – Definitions For the purposes of this Convention: a. "personal data" means any information relating to an identified or identifiable individual ("data subject");	**Article 2 – Definitions** For the purposes of this Schedule: a. "personal data" means any information relating to an identified or identifiable individual ("data subject"), including data from which it is practicable that the identity of the individual can be directly or indirectly ascertained; b. "genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

	c. "biometric data" means personal data resulting from specific technical processing relating to the physical, physio-logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
b. "data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data; c. Where automated processing is not used, "data processing" means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;	d. "data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, use, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data; e. Where automated processing is not used, "data processing" means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;
d. "controller" means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing; e. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available; f. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.	f. "controller" means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing; g. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available; h. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

Article 3 – Scope 1. Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's right to protection of his or her personal data. 2. This Convention shall not apply to data processing carried out by an individual in the course of purely personal or household activities.	[note: not be taken over, since addressed to the Parties] [note: not applicable]
Chapter II – Basic principles for the protection of personal data	
Article 4 – Duties of the Parties 1. Each Party shall take the necessary measures in its law to give effect to the provisions of this Convention and secure their effective application. 2. These measures shall be taken by each Party and shall have come into force by the time of ratification or of accession to this Convention. 3. Each Party undertakes: a. to allow the Convention Committee provided for in Chapter VI to evaluate the effectiveness of the measures it has taken in its law to give effect to the provisions of this Convention; and b. to contribute actively to this evaluation process.	[note: irrelevant, since addressed to the Parties]
Article 5 – Legitimacy of data processing and quality of data 1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake. 2. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law. 3. Personal data undergoing processing shall be processed lawfully. 4. Personal data undergoing processing shall be: a. processed fairly and in a transparent manner; b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes; c. adequate, relevant and not excessive in relation to the purposes for which they are processed; d. accurate and, where necessary, kept up to date; e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.	**Article 3 – Legitimacy of data processing and quality of data** 1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake. [note: not be taken over, since addressed to the Parties] 2. Personal data undergoing processing shall be processed lawfully. 3. Personal data undergoing processing shall be: a. processed fairly and in a transparent manner; b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes; c. adequate, relevant and not excessive in relation to the purposes for which they are processed; d. accurate and, where necessary, kept up to date; e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.
Article 6 – Special categories of data 1. The processing of: - genetic data; - personal data relating to offences, criminal proceedings and convictions, and related security measures; - biometric data uniquely identifying a person; - personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.	**Article 4 – Sensitive data** The processing of sensitive data, including - genetic data; - personal data relating to offences, criminal proceedings and convictions, and related security measures; - biometric data; - personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards, complementing those **of this Schedule,** guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.
Article 7 – Data security	**Article 5 – Data security**

1. Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.	Each **Participant** takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.
2. Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.	[note: irrelevant to take over, since PEAs will in most cases be the competent supervisory authority]

Article 8 – Transparency of processing 1. Each Party shall provide that the controller informs the data subjects of: a. his or her identity and habitual residence or establishment; b. the legal basis and the purposes of the intended processing; c. the categories of personal data processed; d. the recipients or categories of recipients of the personal data, if any; and e. the means of exercising the rights set out in Article 9, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data. 2. Paragraph 1 shall not apply where the data subject already has the relevant information. 3. Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.	**Article 6 – Transparency of processing** 1. Each **Participant** shall inform the data subjects of: a. **its** identity and habitual residence or establishment; b. the legal basis and the purposes of the intended processing; c. the categories of personal data processed; d. the recipients or categories of recipients of the personal data, if any; and e. the means of exercising the rights set out in **Article 7,** as well as any necessary additional information in order to ensure fair and transparent processing of the personal data. 2. Paragraph 1 shall not apply where the data subject already has the relevant information. 3. Where the personal data are not collected from the data subjects, the **Participant** shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.
Article 9 – Rights of the data subject 1. Every individual shall have a right: a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration; b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1; c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her; d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention; f. to have a remedy under Article 12 where his or her rights under this Convention have been violated; g. to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention. 2. Paragraph 1.a shall not apply if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.	**Article 7 – Rights of the data subject** 1. Every individual shall have a right: a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration; b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the **Participant** is required to provide in order to ensure the transparency of processing in accordance with **Article 6**, paragraph 1; c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her; d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the **Participant** demonstrates legitimate grounds for the processing which override his or her interests or rights e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this **Schedule**; f. to have a remedy under **Article 11** where his or her rights under this **Schedule** have been violated; [note: irrelevant to take over, since PEAs will in most cases be the supervisory authority] 2. Paragraph 1.a shall not apply if the decision is authorised by a law to which the **Participant** is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.
Article 10 – Additional obligations 1. Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention. 2. Each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms. 3. Each Party shall provide that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.	**Article 8 – Additional obligations** 1. Each **Paricipant** shall take all appropriate measures to comply with the obligations of this **Schedule** and be able to demonstrate that the data processing under **its** control is in compliance with the provisions of this **Schedule.** [note: shortened, since the reference to domestic implementing legislation is irrelevant and PEAs will in most cases be the supervisory authority] 2. Each **Paricipant** shall examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms. 3. Each **Paricipant** shall implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

4. Each Party may, having regard to the risks arising for the interests, rights and fundamental freedoms of the data subjects, adapt the application of the provisions of paragraphs 1, 2 and 3 in the law giving effect to the provisions of this Convention, according to the nature and volume of the data, the nature, scope and purpose of the processing and, where	[note: irrelevant, since referring to transposition law of the convention, which most PEAs from non-CoE countries will not have]

Article 11 – Exceptions and restrictions 1. No exception to the provisions set out in this Chapter shall be allowed except to the provisions of Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9, when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for: a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; b. the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression. 2. Restrictions on the exercise of the provisions specified in Articles 8 and 9 may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.	**Article 9 – Exceptions and restrictions** 1. No exception to the provisions set out in **Articles 3-8** shall be allowed except to the provisions of **Article 3** paragraph 3, **Article 6** paragraph 1 and **Article 7**, when such an exception is provided for by **the laws to which the Participant is subject**, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for: a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; b. the protection of the data subject or the rights and fundamental freedoms of others, including freedom of expression. 2. Restrictions on the exercise of the provisions specified in **Articles 6 and 7** may be provided for **by the laws to which the Participant is subject** with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.
3. In addition to the exceptions allowed for in paragraph 1 of this article, with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d. This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.	[note: irrelevant, since PEAs do not conduct processing activities for national security and defense purposes] [note: not applicable]
Article 12 - inserted at the end **Article 13** - inserted at the end **Chapter III – Transborder flows of personal data (INSERTED AT THE BEGINNING)** **Article 14 –** inserted at the beginning **Chapter IV – Supervisory authorities (INSERTED AT THE BEGINNING)** **Article 15 –** inserted at the beginning **Chapter V – Co-operation and mutual assistance**	
Article 16 – Designation of supervisory authorities 1. The Parties agree to co-operate and render each other mutual assistance in order to implement this Convention. 2. For that purpose: a. each Party shall designate one or more supervisory authorities within the meaning of Article 15 of this Convention, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe; b. each Party which has designated more than one supervisory authority shall specify the competence of each authority in its communication referred to in the previous littera.	[note: irrelevant, since PEAs are the supervisory authorities]

Article 17 – Forms of co-operation 1. The supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties and exercise of their powers, in particular by: a. providing mutual assistance by exchanging relevant and useful information and co-operating with each other under the condition that, as regards the protection of personal data, all the rules and safeguards of this Convention are complied with; b. co-ordinating their investigations or interventions, or conducting joint actions; c. providing information and documentation on their law and administrative practice relating to data protection. 2. The information referred to in paragraph 1 shall not include personal data undergoing processing unless such data are essential for co-operation, or where the data subject concerned has given explicit, specific, free and informed consent to its provision. 3. In order to organise their co-operation and to perform the duties set out in the preceding paragraphs, the supervisory authorities of the Parties shall form a network.	**Article 10 – Safeguards in co-operation between Participants** [note: covered in the Arrangement] 1. **The Participants shall not exchange or share** personal data undergoing processing unless such data are essential for co-operation, or where the data subject concerned has given explicit, specific, free and informed consent to its provision.
Article 18 – Assistance to data subjects 1. Each Party shall assist any data subject, whatever his or her nationality or residence, to exercise his or her rights under Article 9 of this Convention. 2. Where a data subject resides on the territory of another Party, he or she shall be given the option of submitting the request through the intermediary of the supervisory authority designated by that Party. 3. The request for assistance shall contain all the necessary particulars, relating inter alia to: a. the name, address and any other relevant particulars identifying the data subject making the request; b. the processing to which the request pertains, or its controller; c. the purpose of the request.	
Article 19 – Safeguards 1. A supervisory authority which has received information from another supervisory authority, either accompanying a request or in reply to its own request, shall not use that information for purposes other than those specified in the request. 2. In no case may a supervisory authority be allowed to make a request on behalf of a data subject of its own accord and without the express approval of the data subject concerned.	2. A **Participant** which has received information from another **Participant,** either accompanying a request or in reply to its own request, shall not use that information for purposes other than those specified in the request. 3. In no case **will a Participant** be allowed to make a request on behalf of a data subject of its own accord and without the express approval of the data subject concerned.
Article 20 – Refusal of requests A supervisory authority to which a request is addressed under Article 17 of this Convention may not refuse to comply with it unless: a. the request is not compatible with its powers; b. the request does not comply with the provisions of this Convention; c. compliance with the request would be incompatible with the sovereignty, national security or public order of the Party by which it was designated, or with the rights and fundamental freedoms of individuals under the jurisdiction of that Party.	[note: since cooperation under the Arrangement is not mandatary anayway, there is no poin in stipulating when refusal is not allowed]
Article 21 – Costs and procedures 1. Co-operation and mutual assistance which the Parties render each other under Article 17 and assistance they render to data subjects under Articles 9 and 18 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party making the request. 2. The data subject may not be charged costs or fees in connection with the steps taken on his or her behalf in the territory of another Party other than those lawfully payable by residents of that Party.	[note: cost dimension already covered in Arrangement itself]

3. Other details concerning the co-operation and assistance, relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.	
Chapter II – Basic principles for the protection of personal data (CONTINUED)	
Article 12 – Sanctions and remedies Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this Convention.	**Article 11 – Sanctions and remedies** Violations of the provisions of this **Schedule may give rise to all** judicial and non-judicial sanctions and remedies **available under the laws to which the violating Participants are subject.**
Article 13 – Extended protection None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.	[note: inserted in Article 1, paragrapgh 4]