ICDPPC Group of Experts 2016-2017

Group of Experts on Legal and Practical Solutions for Cooperation

Final documentation accepted at the 39th Conference of the ICDPPC in Hong Kong (abridged reports version)

October 2017

Contents

1

1. Introduction

The Co-chairs (Elizabeth Denham, UK ICO and Wilbert Tomesen, Dutch Data Protection Authority), along with the Office of the Privacy Commissioner of Canada, which provided expert leadership input to Workstream Two of the project of the Group of Experts on Legal and Practical Solutions to Cooperation, are pleased to present the results of the Group's work to the 39TH International Conference of Data Protection and Privacy Commissioners in Hong Kong.

While the main document tabled for the Conference's adoption will be the Draft Resolution on exploring future options for International Enforcement Cooperation (2017) (the "Resolution"), this document package will also include the substantial output of the Group's work in relation to the two workstreams:

(i) key principles in legislation to enhance enforcement cooperation; and

(ii) other measures that can improve enforcement cooperation in the short or long term.

The Co-chairs therefore strongly encourage their counterparts attending the Hong Kong conference in September 2017 to consult the documents which follow, as they provide the background and indeed backbone for the Conference Resolution.

The Co-chairs warmly invite all Members of the Conference to consider co-sponsoring the Resolution.

Moreover, both Co-chair Authorities remain available to any Conference delegation in the run up to, or during the Conference, for questions relating to the project or the Resolution.

Enquiries can be made to the Group of Experts' Administration Team hosted by the UK ICO at: international.team@ico.org.uk

2. Acknowledgements

With special thanks to the Members of the Group of Experts:
By Country (alphabetical order)

Argentina
Eduardo Bertoni
Argentinian Dirección Nacional de Protección de Datos Personales

Belgium
Gert Vermeulen
Belgian Commission for the Protection of Privacy

France
Sophie Bory
CNIL

Germany (Federal)
Stefan Niederer
Office of the Federal Commissioner for Data Protection and Freedom of Information

Germany (Laender Rhineland Palatinate)
Dieter Kugelmann
The Rhineland - Palatinate Commissioner for Data Protection and Freedom of Information

Hungary
Julia Sziklay
NAIH

Hong Kong, China
Sandra Liu
Office of the Privacy Commissioner for Personal Data

Ivory Coast
Cauffi Silvère Assoua
Marie–Grace Konan N'dah
Autorité de Régulation des Télécommunications

Mali
Arouna Keita
Abdou Salam Ag Mohamed
Sow Ahminata Sidbe
APDP

Mexico
Joaquín Jaime González Casanova Fernández
Lilián Irazú Hernández Ojeda
National Institute for Transparency, Access to Information and Personal Data Protection (INAI)

USA
Hugh Stevenson
Guilherme Roschke
Federal Trade Commission (FTC)

Elizabeth Denham, ICO (Co-chair) with Steve Wood and Rob Luke (Deputy Commissioners) in an acting Chair Capacity. Geraldine Dersley (Nominated Legal Expert, ICO). Also contributing from the Co-chair authority: Steve Eckersley, Hannah McCausland, Adam Stevens, Mehreen Perwaiz.

Wilbert Tomesen, Dutch Data Protection Authority (Co-chair) with Udo Oelen (Nominated Legal Expert). Also contributing from the Co-chair Authority: Rosalien Stroot.

Daniel Therrien, OPC-Canada (Workstream Two Lead) with Michael Maguire as Nominated Legal Expert. Also contributing: Brent Homan, Jonathan Bujeau, Regan Morris, Arun Bauri.

WORKSTREAM ONE (member indicated by country)	**WORKSTREAM 2 (member indicated by country)**
UK (Chair for workstream one)	Canada (Chair for workstream two)
Netherlands	Netherlands
Canada	UK
Belgium	Belgium
Hungary	Germany (Federal)
Argentina	Ivory Coast
Hong Kong	Mali
Germany (Laender Rhineland Palatinate)	Mexico
Mexico	USA
Ivory Coast	
Mali	
USA	

3. Report of Activity 2016-2017 (Report to the Conference)

ICDPPC Group of Experts on Legal and Practical Solutions for Cooperation

BACKGROUND

International enforcement cooperation has been a key priority for the International Conference of Data Protection and Privacy Commissioners ("ICDPPC" or "the Conference") for more than a decade. Great strides have been made by the Conference with the development of a set of practical tools and initiatives to improve such cooperation as the pressure has intensified on regulatory agencies to maintain pace with new data protection developments that are increasingly of a global nature and relevance.

In Marrakesh in 2016, the Conference adopted a Resolution on International Enforcement Cooperation (the "Resolution"). The Resolution, as proposed by the lead sponsor, the Information Commissioner's Office, UK, and co-sponsored by eight other authorities from around the globe, set out, the parameters for the work of a new working group (since named the "ICDPPC Group of Experts on Legal and Practical Solutions for Cooperation" or herein "Group"):

'1) To mandate a new Working Group of Experts comprised of interested International Conference members and ideally, representative of the Conference membership from across the different global regions to develop a proposal for key principles in legislation that facilitates greater enforcement cooperation between members. The principles could be adapted by individual members to their national, regional and local needs. The principles would be accompanied by an explanatory memorandum that can be presented to national governments by individual members and where appropriate, observers. In addition, the Working Group is encouraged to suggest other measures that it feels may improve effective cross-border cooperation in the short or long term. The Working Group is encouraged to work in cooperation with other networks of privacy enforcement authorities active in cross-border enforcement cooperation, and to consult with networks of enforcement bodies from other sectors where appropriate, and is directed to report back to the 39th Conference on the product of its work.'

OVERVIEW OF THE GROUP AND ITS WORK

The call for members of the Group was issued in late November 2016. A regionally diverse selection of ICDPPC members expressed an interest in designating an Expert from their Authority to form a part of the Group. The Group's initial teleconference call took place on 21 December. The Information Commissioner's Office (UK) and the Dutch Data Protection Authority were elected as Co-chairs of the Group overall. The Office of the Privacy

Commissioner of Canada (OPC-Canada) volunteered to take a lead role in the Group's work related to other measures that may improve cooperation (see workstream two below). Ultimately, the Group gathered an excellent cross-section of experience and expertise to optimize its work output, with participants ranging from the level of Heads or Deputy Heads of Authority, to senior legal, policy and enforcement experts. Individual members of the Conference from the following countries participated: Argentina, Belgium, France, Germany (Federal), Germany (Laender – Rhineland Palatinate), Hungary, Hong Kong, Ivory Coast, Mali, Mexico and USA.

The ICO, as Sponsor Authority for the 2016 Resolution was designated by the Experts as the Administration Team for the project. In that capacity, the ICO worked with GPEN to set up a dedicated Online Space on the GPEN restricted-access web platform to share information between the Group's members, and convened all meetings on behalf of the Co-chairs. The Group also adopted a dedicated Terms of Reference to help steer the work.

In order to effectively manage the work envisaged in the Resolution, the Co-chairs convened two workstreams, one to develop the key principles, and the other to focus on other measures that may improve effective cross-border cooperation in the short or long term. A survey was conducted among the experts to inform the work in each workstream. The co-chairs collated the survey results, which in turn formed the basis of the first drafts of the documentation in each workstream.

Based on the survey results, workstream two was also split into three sub-streams:

- 2.1 - Draft Alternative Wording to the Global Cross Border Enforcement Cooperation Arrangement (the "Arrangement");
- 2.2 - List of Enforcement Cooperation Tools/Initiatives available within the ICDPPC and other relevant networks, and a list of tools/initiatives for potential future development; and
- 2.3 – Additional Cooperation Frameworks (e.g. international treaties or other bilateral agreements)– conduct a preliminary overview of various frameworks used for, or relevant to, enforcement cooperation, with a view to determining whether further work is warranted to evaluate the feasibility/desirability of implementing a new framework to facilitate more broad-based (both functionally and geographically) privacy and data protection enforcement cooperation.

The workstreams each convened a series of teleconferences which culminated in a face-to-face meeting in Toronto where the Principles and a proposed amendment to the Arrangement were discussed and advanced.

After the meeting in Toronto, an Explanatory Memorandum was developed to accompany the Principles, and two more rounds of Expert consultation took

place on this. Fine-tuning of the texts took place to ensure the consistency and continuity with past work of the ICDPPC and other frameworks such as OECD.

For Workstream 2.1, the twelve current signatories to the Arrangement were approached for their support to the proposed amended wording of the Arrangement. All current signatories supported the amendment and its implementation via a Hong Kong ICDPPC resolution.

Concurrently, during the months of April and May, experts prepared a number of research reports which formed the basis of draft reports in respect of workstreams 2.2 and 2.3, which were amended via several rounds of consultation with the Experts in June and July.

On 23 June, in Manchester, on the margins of the GPEN Enforcement Practitioners Workshop, the Co-chairs and OPC-Canada (as lead for Workstream Two), met to draw up a plan for the final submission of documents to the Hong Kong ICDPPC. A full review of all workstream one and two outputs was also conducted, and subsequently, revised documentation was shared with Experts for final comment. A final Group teleconference was held for both workstreams on 12 July to comment on the latest revisions. The Experts were invited to send final written comments, and the ICO as Administrative Team was tasked with finalizing the text of the Principles and their Explanatory Memorandum.

The Co-chairs also consulted with the Experts on a draft resolution to be sent to the ICDPPC in Hong Kong, and issued a call for co-sponsors.

The Co-chairs finalized the work in August. This included proactive work to ensure the different viewpoints of the Experts were accommodated as far as possible.

DOCUMENTATION PRESENTED TO THE CONFERENCE

In addition to this report, the following Annexes are presented to the Conference as output from this project for future use by Conference members:

1) **Draft Resolution on exploring future options for International Enforcement Cooperation**
   Members of the ICDPPC can see that the Resolution to the Conference recommends follow-up to work in workstream 2.3 on treaties and other legal frameworks.

2) Workstream 1 - **Key Principles** and **Explanatory Memorandum** (explaining the principles)
   To be used, individually or as a full collection, as each Member finds appropriate to encourage their governments to implement legislation that facilitates enforcement cooperation.

3) Workstream 2 – three separate tasks:

a. **Proposed Amendment to the Arrangement** (supported by all current Arrangement signatories) and **Summary Report** (explaining the amendments)
b. **Report on Enforcement Cooperation Tools and Initiatives** (including a list of tools/initiatives: (i) available to Conference members; and (ii) recommended for future consideration)
c. Report on Additional Enforcement Cooperation Frameworks (providing an overview of various potential cooperation frameworks and recommending further evaluation of those via a new working group)

With this report, the Heads of Authority of the Co-chairs/Lead for Workstream Two recommend the Resolution and the Group of Experts documents to the Conference in Hong Kong at its 39th edition in September 2017.

Elizabeth Denham, ICO (Co-chair of the Group of Experts)

Wilbert Tomesen, Dutch Data Protection Authority (Co-chair of the Group of Experts)

Daniel Therrien, OPC-Canada (Workstream Two Lead of the Group of Experts)

4. Resolution

V1.0
39TH INTERNATIONAL CONFERENCE
OF DATA PROTECTION AND PRIVACY COMMISSIONERS
HONG KONG, 2017

Resolution on exploring future options for International Enforcement Cooperation (2017)

Sponsors:

Information Commissioner's Office, UK

Dutch Data Protection Authority

Office of the Privacy Commissioner of Canada

Co-sponsors:

National Directorate for Personal Data Protection, Argentina

Commission for the Protection of Privacy, Belgium

Office of the Privacy Commissioner for Personal Data, Hong Kong, China

Office of the Federal Commissioner for Data Protection and Freedom of Information, Germany

Office of the Rhineland - Palatinate Commissioner for Data Protection and Freedom of Information, Germany

National Institute for Transparency, Access to Information and Personal Data Protection (INAI), Mexico

Federal Trade Commission, USA

The 39TH International Conference of Data Protection and Privacy Commissioners:

Recognising that international enforcement cooperation has been identified by the Conference as important in addressing the challenges presented by the proliferation of global data flows, which can also be of significant cultural, social and economic benefit in the digital society;

Further recognising that increased enforcement cooperation can improve the level of compliance, which is foundational to safeguarding the rights of the individuals, to building consumer trust, and promoting a robust and thriving digital economy;

Recalling the resolutions from the 29th, 31st, 33rd, 34th, 35th, 36th and 38th Conferences relating to improving cross-border enforcement cooperation;

Noting that the Conference has included in its broader strategic plan 2016-2018 the need to develop common approaches and tools for data protection and privacy;

Noting the continued high levels of relevance and importance of the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy, which recommended that member countries take steps to improve the ability of their privacy enforcement authorities to co-operate;

Noting that the protection of personal information and various forms of cooperation between Conference members have been recognised in many jurisdictions, whether specifically through privacy or data protection legislation or more generally through human rights or other regimes[2];

Recalling that there are a variety of ways in which Members of the Conference can cooperate, to enhance privacy enforcement globally, which have produced many successful examples of cooperation to date that were compatible with applicable laws; and such examples have been shared at the 2016-2017 ICDPPC-recognised events on regional and international enforcement cooperation;

Noting however that some Conference members are still unable, or limited in their ability, to cooperate due to limitations imposed by their national or regional laws;

Further noting that some members remain unable to sign binding cooperation agreements, and that others are limited in their ability to cooperate pursuant to non-binding arrangements;

Recalling the establishment, at the 38th Conference, of the mandate for a new Working Group of Experts comprised of interested International Conference members from across different global regions to:

i. develop a proposal for "key principles" in legislation that facilitates greater enforcement cooperation between members; and

[2] For example, Convention 108 from the Council of Europe or the General Data Protection Regulation (GDPR) from the European Union are legal frameworks promoting certain forms of cooperation/mutual assistance in relevant jurisdictions.

ii. suggest "other measures" that may improve effective cooperation in the short or long term;

Further recalling that a Group was established in December 2016 as the Group of Experts on Legal and Practical Solutions for Cooperation, involving Experts from 14 different Conference members: The Dutch Data Protection Authority (Autoriteit Persoonsgegevens), and the United Kingdom's ICO (Co-chairs), Argentinian Dirección Nacional de Protección de Datos Personales, Belgian Commission for the Protection of Privacy, Canadian Office of the Privacy Commissioner, France's CNIL, Germany (representatives from Federal and Laender authorities: The Federal Commissioner for Data Protection and Freedom of Information and the Rhineland-Palatinate Commissioner for Data Protection and Freedom of Information), Office of the Privacy Commissioner for Personal Data, Hong Kong, China, Hungary's NAIH, Ivory Coast's Autorité de Régulation des Télécommunications, Mali's APDP, Mexico's INAI, and the USA's FTC (the "Group");

Noting that with respect to its work on the key principles, the group identified that:

- its work would focus on facilitation of enforcement cooperation on civil and administrative matters, as criminal law cooperation provisions in this area are not always relevant to every jurisdiction; and

- there are various dimensions of cooperation in law which can facilitate a Member's ability and capacity to cooperate: for example, assessment of the law's provision for basic cooperation powers, forms of cooperation, as well as appropriate arrangements to cooperate, conditions (significantly including confidentiality), and practicalities;

Further noting that with respect to its work on other measures, the Group identified at the outset that:

- while the Global Cross Border Enforcement Cooperation "Arrangement" was adopted at the 36th Conference, there would be value in increasing Members' participation therein;

- while there are a variety of existing tools and initiatives that can facilitate cooperation, awareness of those could be improved amongst Members, and additional tools or initiatives could further enhance cooperation; and

- while much cooperation can and does take place pursuant to MOUs like the Arrangement, without the sharing of personal data, there would be value in exploring potential framework options that may facilitate a broader geographic and functional scope of cooperation;

Noting that the existing Signatories to the Arrangement have already indicated their support for a proposed amendment to the Arrangement, as well as to its implementation via this resolution;

Therefore, the Conference resolves to continue to encourage efforts to bring about even more effective cooperation in cross-border enforcement in appropriate cases, and:

1) Endorses the Key Principles for Cooperation and associated Explanatory Memorandum developed by the Group. It also encourages members and observers to, as they deem appropriate, adapt the key principles and the Explanatory Memorandum to their national, regional and local needs and to present the key principles to their governments, with a view to assisting in development of laws that will facilitate more effective privacy enforcement cooperation.

2) Accepts the amendments to optimize the Global Cross Border Enforcement Cooperation Arrangement (the "Amended Arrangement"), as recommended by the Group so as to promote participation in the Arrangement by other Conference Members, such that the Amended Arrangement (Annex One) will come into effect 1 January 2018.

3) Mandates the Executive Committee of the International Conference of Data Protection and Privacy Commissioners to take the steps necessary to fulfil its role under section 12 and 13 of the Amended Arrangement with respect to notices submitted in accordance with section 5, as soon as possible, and in any event, prior to the effective date of the Amended Arrangement.

4) Takes note of the Group's exploratory work regarding tools and initiatives currently available for privacy enforcement cooperation, as well as those potential additional practical measures suggested by the Group, which may further improve effective cross-border cooperation in the short or long term.

5) Mandates, in accordance with the Group's recommendation, the creation of a new Working Group of the Conference to further explore the feasibility of potential framework options that may facilitate a broader geographic and functional scope of cooperation of privacy enforcement cooperation, and for the Working Group to report back on the progress of their work at the 40th Conference, and report back on the results of the work at the 41st Conference, with the recommendation, if it deems appropriate, of the development of any additional cooperation framework(s).

Annex One to the Resolution:

[Annex One copies section 8 – Task 2.1 of this Document Package – Amended Global Cross-border Enforcement Cooperation Arrangement - see section 8].

WORKSTREAM ONE

The Key Principles

5. Summary of Key Legislative Principles

Principle 1 **- Domestic laws should enable Privacy Enforcement Authorities (hereafter 'PEAs'[3]) to cooperate (including by providing assistance) on international privacy enforcement matters where appropriate.**

Purpose - To ensure that, particularly in light of the increasing flow of data around the world, PEAs have the clear ability to cooperate with those in other jurisdictions, to ensure that there is effective enforcement of privacy rights.

Principle 2 - Domestic laws should provide for cooperation with other entities in addition to PEAs.

Purpose - To recognise that a PEA should be able to cooperate or provide assistance to any appropriate body that can achieve the relevant aim of the protection of the rights of the individual in relation to his or her personal data.

Principle 3 **- Domestic laws should provide for the broad forms of cooperation in which a PEA may engage. These may include:-**
a) general strategic or technical cooperation,

b) cooperation with respect to specific enforcement matters not involving the sharing of personal information,

c) cooperation with respect to specific enforcement matters including the sharing of personal information

1) **data sharing**
2) **other forms of case, investigation or information gathering assistance.**

Purpose - To emphasise that the practical ways in which a PEA can cooperate or provide assistance should be set out in domestic laws. There are a number of forms of cooperation and the greatest

[3] The term 'PEA' means any public body that has as one of its responsibilities the enforcement of a privacy and/or data protection law, and that has powers to conduct investigations or take enforcement action and is intended to include supervisory authorities, data protection authorities and other regulators with statutory responsibility within their jurisdiction for the regulation of privacy or data protection laws.

sensitivities will arise around the disclosure and exchange of confidential or personal information.

Principle 4 **- Where additional arrangements are required in relation to particular enforcement matters (whether or not including the exchange of personal information), domestic laws should specify the form of those arrangements. In any event, domestic laws should, where appropriate, facilitate cooperation arrangements.**

Purpose - Whilst jurisdictions are urged to remove legal restrictions that may represent an unnecessary or disproportionate barrier to cooperation, some applicable laws may still necessitate that particular arrangements be put in place to enable certain forms of cooperation. Where this is the case, cooperation may be enhanced by clear indications of the arrangements (e.g., a non-binding MOU and/or binding agreement, as appropriate) by which such other laws and obligations may be addressed. Further, recognizing that co-operation may be enhanced by appropriate arrangements, even where they are not required, domestic laws that facilitate such arrangements will, in turn, facilitate cooperation.

Principle 5 **- Domestic law should provide for the circumstances in which information, including the fact and substance of the request and any response, can be disclosed.**

Domestic law should enable a PEA to require, prior to disclosing such information to another authority, that the recipient authority comply with any appropriate protections for the information.

Purpose - To recognise that many forms of cooperation will involve the request and disclosure of information including personal data, and to ensure that such information is appropriately protected (for example where obligations of confidentiality or data protection and privacy may apply), whilst still enabling cooperation to take place.

6. Explanatory Memorandum to the Principles

Background

In the last two decades, the growth of the internet and digital means of doing business, and even just of communicating, has resulted in changes to the way everyone - organisations and people - interact with each other. The world is more connected than ever and this increased globalisation is powered by flows of data across borders. These flows of information (including personal information) are of tremendous cultural, social and economic benefit, but at the same time, there is an important public interest of protecting personal information when data moves to, and is accessible in, multiple jurisdictions.

Active, and not just theoretical, cooperation is essential to providing appropriate practical protections to our citizens, which in turn can increase consumer confidence and create a robust and thriving digital economy. Increased coordination would improve the effectiveness of privacy enforcement authorities[4] ("PEAs") in cases involving the processing of personal information in multiple jurisdictions.

The protection of personal information[5] has been recognised in many jurisdictions, whether specifically through privacy or data protection legislation, or through human rights or other regimes. The challenges associated with protecting personal information and ensuring that an individual may exercise his or her associated rights in a multi-jurisdictional context has placed a greater burden on PEAs to investigate and, where necessary, enforce against violations. PEAs often face limitations with respect to enforcement tools, viability and leverage in investigating complaints or conduct occurring outside their borders without the assistance of relevant authorities in other jurisdictions. There can also be a sub-optimal duplication of investigative work when multiple PEAs investigate the same multi-jurisdictional matter.

[4] The term 'privacy enforcement authority' ("PEA") is intended to include supervisory authorities, data protection authorities and other regulators with statutory responsibility within their jurisdiction for the regulation of privacy or data protection laws.
[5] In the context of enforcement cooperation, personal information could, depending on the jurisdiction and interpretation of relevant laws, relate to a number of different individuals including (but not limited to) the complainant, consumer, those being investigated and their staff, PEA staff (e.g. investigators) and secondees.

This need to take a more international approach to regulation and enforcement of data protection and privacy laws has been universally accepted. The OECD Guidelines in 1980 recognised that its member countries have a common interest in protecting individuals and should establish procedures to facilitate "mutual assistance in the procedural and investigative matters involved".[6]

Significant work has been done by PEAs, both bilaterally and multilaterally, to improve cooperation, particularly in the areas of enforcement and investigation, by concentrating in the first instance on practical measures that the authorities can take. Those PEAs whose legislation already enables cooperation are, in fact, cooperating more and more, in different ways, which has yielded great successes.
However, legal barriers still exist for some authorities, either with respect to their ability, or breadth of that ability, to cooperate. As was recognised by the OECD in its 2007 Recommendation, there is a specific need for member countries to "improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities".[7] One of the purposes of this document is to break down legal barriers, and to legally enable more authorities to engage in enhanced cooperation.

The ICDPPC has long been an active proponent of international cooperation (as evidenced by numerous resolutions adopted over recent years[8]) and, as a next step, agreed to develop "key principles" in domestic legislation that will further reduce cooperation barriers and facilitate even greater enforcement cooperation between ICDPPC members.

It is not a "one size fits all" proposition or challenge. The legislative starting point for each member may be different, with some only having limited provision for enforcement activities within their own jurisdictions, with others having more extensive enforcement powers and obligations that already provide for some ability to cooperate with counterparts in other jurisdictions.

[6] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Part Five, Guideline 21, 1980.
[7] OECD Recommendation on cross-border co-operation in the enforcement of laws protecting privacy, 2007.
[8] There are resolutions from the 29th, 31st, 33rd, 34th, 35th, 36th and 38th ICDPPC Conferences which relate to improving cross-border enforcement cooperation. Website page: https://icdppc.org/document-archive/adopted-resolutions/ (last accessed 20170817)

It is therefore the aspiration of this project that: (i) the key principles be adapted by individual members, as they deem appropriate according to their national, regional and local needs[9], with a view to assisting their governments in developing legislation that will enable and facilitate their own engagement in enforcement cooperation; and (ii) national governments around the world implement legislation that reflects the key principles, thus promoting increased enforcement cooperation globally, to best face the challenges, and leverage the opportunities, associated with the global digital economy.

Principles

The purpose of this work is to develop key legislative principles that can be adapted to national, regional and local needs to reduce uncertainty and facilitate cooperation (and thereby enable) PEAs to protect privacy more effectively.

In order to achieve this goal, it must be recognized that:

- enforcement cooperation is a wide concept that covers many activities, such as general knowledge-sharing, sharing of investigative information and provision of various other forms of mutual assistance, all of which can be valuable to the enforcement of cross-border privacy matters;
- a PEA, in considering cooperation, may need to be assured of certain levels of protection and other obligations required by its own regime, where appropriate;
- while reciprocity is key to effective cooperation, PEAs should have the discretion to decide whether, and if so, how to respond to a request for cooperation or assistance; and
- an authority is more likely to engage in enforcement cooperation with counterparts when there is clarity and certainty with respect to its legal ability to do so, provided that enabling provisions are sufficiently flexible, and not unnecessarily narrow or prescriptive.

Given that many PEAs do not have criminal enforcement powers, and that criminal enforcement cooperation is already the subject of various other international agreements, it was decided that the Key Principles would only relate to cooperation on civil and administrative enforcement matters.

[9] By way of example, the term 'local' would include sub-national level or relate to autonomous regions.

Although the key principles refer to domestic laws, it does recognise that the laws in some countries are actually derived from a supranational law or result from international agreements, which may have the effect of creating harmonized enforcement cooperation approaches at the domestic level, and any amendments or additions to domestic laws would have to take into account this supranational framework[10].

***Principle 1* - Domestic laws should enable PEAs to cooperate (including by providing assistance) on international privacy enforcement matters where appropriate.**

Purpose
To ensure that, particularly in light of the increasing flow of data around the world, PEAs have the clear ability to cooperate with those in other jurisdictions, to ensure that there is effective enforcement of privacy rights.

Most PEAs derive their powers entirely from their domestic law, whether set out in legislation or arising out of common law, and this law defines the authority's functions, powers and obligations. Where such powers derive from legislation, it should clearly set out the powers of the PEA to cooperate, as uncertainty in this regard may prove a paralyzing hindrance to cooperation.

The power to cooperate should include the ability to provide assistance where the conduct in question is substantially similar to conduct prohibited in its jurisdiction, even where no harm has occurred in its jurisdiction.

While cooperation and reciprocity should be encouraged in appropriate circumstances, it should not be mandatory but within the discretion of the authority. This is to prevent a PEA being obliged to provide assistance or cooperate even if it does not deem it appropriate.

It should also be noted that a PEA can only act, when cooperating, within its own powers and in compliance with its domestic law. Consideration may need to be given as to whether data obtained from the disclosing

[10] For example, Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108)

authority can be used by the recipient authority in pursuit of actions in its own jurisdiction.

Principle 2 - Domestic laws should provide for cooperation with other entities in addition to PEAs.

Purpose
To recognise that a PEA should be able to cooperate or provide assistance to any appropriate body that can achieve the relevant aim of the protection of the rights of the individual in relation to his or her personal data.

Domestic laws should identify (for example, by category, description or name) those other regulators and authorities, in addition to PEAs, which may be effective in achieving the aims of protecting privacy and enforcing against privacy violations. It could be of relevance to consider the type and range of powers of these authorities and their effect in protecting privacy or enforcing laws similar to, or overlapping with, those regulated by the PEA. Such bodies could include foreign, regional, international and other domestic authorities[11]. They could also include specialised regulators in other relevant regulatory sectors such as consumer protection, where issues of intersection appear to be increasing, or spam/electronic threats (e.g., telecommunications). More widely, the OECD recommended in 2007 that member states should foster the establishment of informal networks of PEAs and other appropriate stakeholders[12] to achieve many of the aims being taken forward by this work[13].

***Principle 3* - Domestic laws should provide for the broad forms of cooperation in which a Privacy Enforcement Authority may engage. These may include:-**
a) general strategic or technical cooperation,

b) cooperation with respect to specific enforcement matters not involving the sharing of personal information,

[11] Although domestic laws could also enable a domestic PEA to cooperate with authorities responsible for handling criminal matters, this is outside the scope of this project.
[12] Such stakeholders could include non-public authorities e.g. businesses and civil society. It is for the jurisdiction to determine the entities with whom a PEA may cooperate and (in line with Principle 1) any cooperation would be at the discretion of the PEA.
[13] OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007), paragraph 21

c) cooperation with respect to specific enforcement matters including the sharing of personal information

1) data sharing

2) other forms of case, investigation or information gathering assistance.

Purpose
To emphasise that the practical ways in which a PEA can cooperate or provide assistance should be set out in domestic laws. There are a number of forms of cooperation and the greatest sensitivities will arise around the disclosure and exchange of confidential or personal information.

Having defined the power to cooperate or provide assistance and identified those that could benefit from it, consideration should also be given to the forms of cooperation in which a PEA can engage. These broad forms of cooperation have been set out at various levels, from the least to the most sensitive, and are intended to be an illustrative, rather than prescriptive or exhaustive, list of collaborative options.

(a) At its widest, there should be general strategic or technical cooperation, which does not involve the exchange or disclosure of confidential or personal information[14]. This could include:-

- the ability to join networks of other similar authorities,
- sharing best practices, research, general policy relating to enforcement,
- sharing of information on technical expertise, investigative methods, and
- information exchange on complaint numbers and statistics.

It should be recognised that much effective cooperation already takes place along these lines. This enables authorities to learn from each other, not just about general issues of concern, but also about effective ways of dealing with violations of privacy and data protection laws.

(b) Situations will arise where cooperation is required on specific enforcement matters, but these will not necessarily require the sharing of personal information. Assistance in these circumstances could include:-

- the notification of anonymised complaints, and

[14] Recognizing that cooperation between authorities that does not relate to specific enforcement activity will generally still involve the sharing of personal data of PEA staff.

- the provision of evidence which does not including personal data, for example, technological analysis, practices, procedures, and primary evidence with all personal data redacted.

This information may, however, still be confidential, and will need to be treated as such in the hands of the receiving authority. Further consideration of this point is set out in Principle 5.

Again, much cooperation on specific enforcement matters already takes place in this form, without the need to share personal data, or to compromise the integrity or strength of any enforcement action.

(c) Cooperation on specific enforcement matters which includes the sharing of personal information may require special consideration. At the same time, as recognized by the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy,[15] there can be great value in enabling PEAs to provide investigative assistance to authorities outside their jurisdiction, via the gathering of primary evidence located within its jurisdiction.

Such cooperation can, broadly, be put into two categories:

i. data sharing, which can include:-

   - the notification of specific complaints including the disclosure of personal data of complainants and/or the identity of data controllers or processors allegedly involved, and
   - the sharing of evidence including personal data – e.g., forensic reports, witness statements, corporate records, third party records, etc.

ii. other case, investigation or information gathering assistance, which can include the following examples, with a fuller list set out in annex 1. :-

   - investigation-relevant proactive exchange of information
   - search (including access to premises),

[15] OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007), paragraph 12(b).

- freezing and/or seizure (and transfer) of documents, objects or other data (including on hardware or storage devices or in information systems),
- the hearing of a witness, expert, victim, suspected or accused person or third party in the territory of another state, and
- interception of telecommunications or electronic communications.

When considering any data sharing or providing other forms of assistance, a PEA will have to take into account all relevant/enabling laws and obligations, including procedural safeguards under its relevant laws. These may include seeking, in advance, judicial authorisation or warrant for certain activities or disclosures. These requirements should not necessarily prevent the gathering and/or disclosure of such information, but rather enable the PEA to consider the most appropriate cases for assistance or cooperation, and the most appropriate ways in which it can respond to any such request.

While not clearly falling under one of the three forms of cooperation outlined above, it should also be noted that an exchange of staff or secondments can be very effective in building relationships as well as exchanging knowledge and experience[16].

Principle 4 - Where additional arrangements are required in relation to particular enforcement matters (whether or not including the exchange of personal information), domestic laws should specify the form of those arrangements. In any event, domestic laws should, where appropriate, facilitate cooperation arrangements.

Purpose
Whilst jurisdictions are urged to remove legal restrictions that may represent an unnecessary or disproportionate barrier to cooperation, some applicable laws may still necessitate that particular arrangements be put in place to enable certain forms of cooperation. Where this is the case, cooperation may be enhanced by clear indications of the arrangements (e.g., a non-binding MOU and/or binding agreement, as appropriate) by which such other laws and obligations may be addressed.

[16] Consideration should be given to the fact that secondments can often involve the sharing of confidential or personal data related to investigations.

Further, recognizing that co-operation may be enhanced by appropriate arrangements, even where they are not required, domestic laws that facilitate such arrangements will, in turn, facilitate cooperation.

It is important to consider the impact that specific arrangement requirements may have on the practical ability of the PEA to cooperate[17]. It appears that most PEAs do not currently have the power to enter into binding agreements, with such authority resting with their governments (and that some may not be able to enter into even non-binding arrangements). Consideration should therefore be given to whether a binding agreement or non-binding MOU would be appropriate in the circumstances, including by balancing the following two objectives: (i) ensuring that the PEA obtains adequate commitments or assurances from cooperating authorities; and (ii) avoiding undue barriers for the authority to engage in enforcement cooperation. Domestic laws should also consider how best to provide for the PEA to enter into any specific arrangements that need to be in place. Consideration should be given to the fact that a PEA will be more likely to cooperate where it is enabled to enter into any required arrangements.

***Principle 5* - Domestic law should provide for the circumstances in which information, including the fact and substance of the request and any response, can be disclosed.**

Domestic law should enable a PEA to require, prior to disclosing such information to another authority, that the recipient authority comply with any appropriate protections for the information.

Purpose
To recognise that many forms of cooperation will involve the request and disclosure of information including personal data, and to ensure that such information is appropriately protected (for example where obligations of confidentiality or data protection and privacy may apply), whilst still enabling cooperation to take place.

The allowable use or disclosure of the information that is to be provided by a PEA to another authority should be addressed and enabled, whether in general or specific form, within domestic law. Treatment requirements may apply not just to information (including personal data) disclosed in

[17] An example would be arrangements required to satisfy any obligations in domestic law regarding the transfer of personal information to another country.

response to a request, but also to the substance of a request for information itself, as well as the fact that a request was made. This is to ensure that the disclosing authority's investigation and possible enforcement action are not prejudiced.

This principle recognises that by setting out reasonable and proportionate confidentiality requirements, as well as providing for any other conditions which apply under the PEA's relevant laws, domestic law can provide the PEA with necessary clarity and consistency with respect to the parameters within which it can cooperate. This could, in turn, avoid uncertainty that may serve as a barrier to cooperation.

Existing legal requirements may include those in relation to processing and disclosure of personal information, and may arise in domestic and/or international law, such as pursuant to international agreements or treaties.[18] Such laws could provide, for example:

- for disclosure to be made only where certain specified circumstances arise (e.g., for criminal or civil proceedings, when is in the public interest, or where the rights and interests of relevant parties have been balanced against each other); or
- for obtaining consent of the data subject prior to disclosure, unless this would prejudice the investigation or enforcement activity.

Domestic law may already provide for confidentiality generally (e.g. not limited to privacy breach investigations or enforcement cooperation), but the jurisdiction should consider requiring only such restrictions as reasonably necessary. It would usually be expected that where information is provided to a recipient authority in relation to particular enforcement activities, the recipient authority should be able to use that information in the context of those enforcement proceedings.

Where the recipient authority wishes to use or disclose information for a purpose other than that for which the information was disclosed to it, the recipient authority may be required to obtain prior express authorization from the disclosing authority.

A recipient authority may also be required by law to disclose information it holds (including that obtained pursuant to enforcement cooperation) to another person or organisation, in certain circumstances (e.g., via lawful

[18] For example, Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108)

access, or Freedom of Information). The potential for such disclosures could serve as a barrier to other authorities' willingness to share information with that PEA. To address this, the relevant domestic laws (such as Freedom of Information) could include appropriate exemptions for the disclosure of any information provided by another authority (for example, only with the disclosing authority's consent). Such laws may also provide for a balancing exercise, to consider the benefits of disclosure against the harm that could be caused to international relations, for example. In any event, where such disclosure may be required, the providing authority should be promptly notified of the request.

Domestic laws may also instil greater confidence, for other authorities wishing to cooperate with a domestic PEA, by providing for sanctions for the PEA's staff who breach an obligation, for example, of confidentiality or non-disclosure without lawful authority.

Practical matters

There may be other aspects of cooperation (including practical matters) that a jurisdiction may want to consider. These do not necessarily need to be set out in domestic law, but could be left to the discretion of the relevant PEA, so that it can determine its own processes and requirements.

Such practical matters could include:

- the form (e.g., written) and substance (i.e., details) required for the PEA's consideration of any request for cooperation or specific information;
- whether secure communication channels should be used; or
- which authority will bear the costs associated with any assistance to be provided[19].

Next steps

Enforcement cooperation is a critical element in ensuring appropriate practical protections for citizens, particularly in the digital world. Much has been done previously in this area, all with the aim of focussing on facilitating greater enforcement cooperation between members, in the manner determined by each individual jurisdiction. It is the aim of this

[19] Further examples and ways of managing and ensuring efficient and effective cooperation between PEAs can be found in the ICDPPC Enforcement Cooperation Handbook.

work on key principles in legislation to build on the great progress that has been made in this area. Individual members are strongly encouraged to use these key principles, as they deem appropriate, to engage with and assist their own governments in developing legislation that will enable and facilitate their own engagement in enforcement cooperation. In so doing, this will urge national governments around the world to implement legislation that reflects the key principles, thus promoting increased enforcement cooperation globally, to best face the challenges, and leverage the opportunities, associated with the global digital economy.

Annex to the Key Principles

Non-exhaustive list of types of investigation or information gathering assistance[20]:

- investigation-relevant proactive exchange of information
- exchange or posting of staff (involved in case- or investigation-related work)
- sending and service of procedural documents (addressed to addressees in another state, through the local DPA)
- search (including access to premises)
- freezing and/or seizure (and transfer) of documents, objects or other data (including on hardware or storage devices or in information systems)
- the hearing of a witness, expert, victim, suspected or accused person or third party in the territory of another state
- hearing by videoconference of data controllers, data processors, witnesses or experts
- hearing by teleconference of witnesses or experts
- cooperation in joint investigation teams (JITs)
- identification of persons holding a subscription of a specified phone number or IP address
- interception of telecommunications or electronic communications (traffic and other metadata, geolocation data, communication content)
- access to ICT hardware and storage devices, networks, etc.
- access to information on servers abroad
- identification of financial accounts (banks, numbers, of holders or proxies)
- information on financial transactions
- bank account monitoring (as a covert measure).

[20] See Principle 3. It is for the jurisdiction to determine the extent and range of the powers of the PEA and provide for any safeguards it considers appropriate on the exercise of those powers.

WORKSTREAM TWO

Other measures to improve cooperation

7. Task 2.1: Alternative Language to the Arrangement

Introduction

This document is intended to accompany the **Report of Activity 2016-2017 of the Group of Experts on Legal and Practical Solutions for Cooperation**.

In their responses to the survey administered by the Co-Chairs of the Group of Experts (the "Group"), the Group members (the "Experts") identified that there would be value in exploring potential alternative wording to the Global Cross Border Enforcement Cooperation Arrangement (the "Arrangement") to encourage increased participation.

The survey results highlighted that many authorities (at least the 12 current participants from North America, Europe and the Asia Pacific region – the "Participants") are currently able to cooperate pursuant to the Arrangement in its current form. At the same time, it was identified that a greater number of authorities may be able to participate in the Arrangement if they were able to expressly limit their participation in the Arrangement, such that they would not share personal data and/or cooperate in respect of criminal matters.

The Experts recognized that much cooperation can be, and has been, accomplished in respect of administrative or civil matters, without sharing personal data.

Process

The Group therefore undertook to draft proposed alternative wording for the Arrangement (the "Proposed Amendment") to give each new and existing Arrangement participant the option to expressly limit the scope of their participation.

The Group prepared a first draft which would allow any new or existing participant in the Arrangement to elect that, pursuant to the Arrangement: (a) it would not share personal data; and/or (b) it would not cooperate in respect of criminal matters. Based on comments received in response to that draft, a third more general option, that would allow participants to limit cooperation in other circumstances that they may specify, was added to the Proposed Amendment. This version received consensus support from the Group.

The Experts recognized that the Amendment should be acceptable, at the very least, to all existing Participants. The draft Proposed Amendment, as well as the plan for its implementation via resolution at the Hong Kong Conference (without further specific ratification by existing Participants), was therefore shared with all existing Participants, including those who were not represented in the Group

of Experts, with a view to ensuring that the proposal would be broadly acceptable.

We are pleased to report that **each existing participant to the Arrangement has confirmed its support for the Proposed Amendment and its implementation via resolution in Hong Kong**.

Proposed Amendment

The final Proposed Amendment, which is recommended for adoption via the resolution flowing from the Experts' work (the "Resolution"), is appended to this Report (in a proposed "Amendment Summary" and "Amended Arrangement").

Role of the ICDPPC Executive Committee and Effective Date

We note that the Proposed Amendment would, in a limited manner, expand the ICDPPC Executive Committee's role in administering the Arrangement, by mandating it to accept and communicate any elections for which it is notified by new or existing participants (as it does currently with respect to "Schedule 1" or "Other Arrangements" related to the handling of personal data). The Group conferred with the Executive Secretariat and has received preliminary indications that the changes to the ICDPPC website that would be required to fulfil this expanded mandate would be minor, and not resource-intensive to implement.

We are therefore recommending that, to give the Executive Secretariat sufficient time to implement necessary changes to the website, the Proposed Amendment come into effect 1 January 2018, approximately three months after adoption of the Resolution in Hong Kong.

APPENDIX TO THE 2.1 REPORT

DRAFT AMENDMENT TO THE GLOBAL CROSS BORDER ENFORCEMENT COOPERATION ARRANGEMENT ("THE ARRANGEMENT")

The Arrangement is hereby amended by:

(1) Inserting the following text at the end of section 5:

A Participant may notify the Committee, either in its notice of intent to participate submitted in accordance with section 12 or in a separate notice that it will not:

(a) disclose personal data to other Participants pursuant to this Arrangement;

(b) provide assistance under this Arrangement in respect of matters that would be considered criminal or penal under its laws; and/or

(c) provide assistance under this Arrangement in other circumstances that it may specify.

Failure to provide a notice pursuant to this section does not affect a Participant's discretion to limit its cooperation in respect of particular requests for assistance pursuant to this section.

(2) Replacing the last paragraph of section 12 with the following text:

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 that have submitted a notice in accordance with section 5. The list should be easily available to all Participants.

(3) Replacing section 13 with the following text:

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 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 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.

8. Task 2.1 - Updated Global Cross Border Enforcement Cooperation Arrangement (with amendment shown in task 2.1 report)

Version 17

Global Cross Border Enforcement Cooperation Arrangement

PREAMBLE

Recalling that the resolution of the Warsaw Conference mandated an extension to the work of the International Enforcement Coordination Working Group to develop a common approach to crossborder case handling and enforcement coordination, to be expressed in a multilateral framework document addressing the sharing of enforcement-related information, including how such information is to be treated by recipients thereof.

Acknowledging that a global phenomenon needs a global response and that it is in the interests of privacy enforcement authorities,[21] individuals, governments and businesses that effective strategies and tools be developed to avoid duplication, use scarce resources more efficiently, and enhance effectiveness in relation to enforcement in circumstances where the privacy and data protection effects transcend jurisdictional boundaries.

Mindful that cases are increasingly demonstrating how increased transborder data flows and the practices of private and public sector organisations relating to these transborder flows can quickly and adversely affect the privacy and the protection of the personal data of vast numbers of individuals across the world and that therefore increased transborder data flows should be accompanied by increased cross-border information sharing and enforcement cooperation between privacy enforcement authorities with such information sharing and enforcement cooperation being essential elements to ensure privacy and data protection compliance, serving an important public interest.

Reflecting on the fact that a number of privacy enforcement authorities have concurrently investigated several of the same practices or breaches.

Recalling the provisions of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), specifically those under Chapter IV on mutual assistance.

Recalling the 2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy which recommends Member Countries cooperate across borders in the enforcement of laws protecting privacy and data protection, and taking the appropriate steps to:

- improve their domestic frameworks for privacy law enforcement to better enable cross-border cooperation, in a way consistent with national laws;

- provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards; and

- engage relevant stakeholders in discussions and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.

[21] For the avoidance of doubt and for the purposes of this document, the term 'privacy enforcement authorities' also includes data protection authorities.

Recalling the Resolutions of previous International Conferences of Data Protection and Privacy Commissioners (ICDPPC) and the Montreux Declaration which encouraged privacy enforcement authorities to further develop, amongst other things, their efforts to support international enforcement cooperation and to work with international organisations to strengthen data protection worldwide.

Building on significant progress which has been made in recent years at a global and regional level to enhance arrangements for, inter alia, cross-border enforcement cooperation.

Recognising that cross border enforcement cooperation can manifest itself in various ways. It can happen at different levels (national, regional, international), be of different types (coordinated or uncoordinated), and cover several activities (sharing best practice, internet sweeps, co-ordinated investigations, or joint enforcement actions leading to penalties/sanctions). However it manifests itself, key to its success is creating a culture of proactive and appropriate information sharing which may include information which is non-confidential or confidential and may or may not include personal data; and coordinating enforcement activities appropriately.

Encouraging all privacy enforcement authorities to use and develop further existing enforcement related mechanisms and cooperation platforms and help maximise the effectiveness of cross border enforcement cooperation.

Concluding that to effectively respond to data protection and privacy violations that affect multiple jurisdictions a multi-lateral approach is required and therefore appropriate mechanisms to facilitate the information sharing of confidential enforcement related material, and coordination of enforcement amongst privacy enforcement authorities to tackle said violations is much needed.

Therefore, privacy enforcement authorities are strongly encouraged to become Participants to this Arrangement and commit to following its provisions, particularly on confidentiality and data protection, when engaging in cross border enforcement activities.

1. DEFINITIONS

The following definitions will apply in this Arrangement:

'**enforcement cooperation**' – is a general term referring to privacy enforcement authorities working together to enforce privacy and data protection law.

'**enforcement coordination**' – refers to a specific type of enforcement cooperation in which two or more data protection or privacy enforcement authorities link their enforcement activities in relation to the enforcement of violations of privacy or data protection law in their respective jurisdictions.

'**Privacy and Data Protection Law**' means the laws of a jurisdiction, the enforcement of which has the effect of protecting personal data.

'**Privacy Enforcement Authority**' (hereafter 'PEA')[22] means any public body that has as one of its responsibilities the enforcement of a privacy and/or data protection law, and that has powers to conduct investigations or take enforcement action.

'**Request for assistance**' is a request from a Participant to one or more other Participants to cooperate/coordinate enforcing a privacy and data protection law and may include:

i. A referral of a matter related to the enforcement of a privacy and data protection law;
ii. A request for cooperation on the enforcement of a privacy and data protection law;
iii. A request for cooperation on the investigation of an alleged breach of a privacy and data protection law; and
iv. A transfer of a complaint alleging a breach of a privacy and data protection law.

'**Participant**' means a PEA that signs this Arrangement.

'**Committee**' means the Executive Committee of the International Conference of Data Protection and Privacy Commissioners.

'**Complainant**' – means any individual that has lodged, with the PEA, a complaint about an alleged violation of privacy and/or data protection law.

2. PURPOSE

The purpose of this Arrangement is to foster data protection compliance by organisations processing personal data across borders. It encourages and facilitates all PEAs' cooperation with each other by sharing information, particularly confidential enforcement-related information about potential or

[22] For the avoidance of doubt and for the purposes of this document, the term 'privacy enforcement authorities' also includes data protection authorities.

ongoing investigations, and where appropriate, the Arrangement also coordinates PEAs' enforcement activities to ensure that their scarce resources can be used as efficiently and effectively as possible.

3. AIMS

This Arrangement aims to achieve its objective by:

(i) Setting out key provisions to address the sharing of enforcement-related information, including how such information is to be treated by recipients thereof.

(ii) Promoting a common understanding and approach to cross-border enforcement cooperation at a global level;

(iii) Encouraging Participants to engage in cross-border cooperation by sharing enforcement related material and, where appropriate, coordinating their knowledge, expertise and experience that may assist other Participants to address matters of mutual interest;

(iv) Encouraging Participants to use and assist in the development of secure electronic information sharing platforms to exchange enforcement related information, particularly confidential information about on-going or potential enforcement activities.

4. NATURE OF THE ARRANGEMENT

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 non-confidential or confidential information which may or may not contain personal data.

5. RECIPROCITY PRINCIPLE

All Participants will use their best efforts to cooperate with and provide assistance to other Participants in relation to cross border enforcement activity. This includes responding to requests for assistance as soon as practicable.

Participants should indicate in writing, when providing enforcement related material and data pursuant to this Arrangement, that such material is being provided pursuant to the terms of this Arrangement.

Participants receiving requests for assistance should acknowledge receipt of such requests as soon as possible, and preferably within two weeks of receipt.

Prior to requesting assistance from another Participant, the sending Participant should perform an internal preliminary check to ensure that the request is consistent with the scope and purpose of this Arrangement and does not impose an excessive burden on the request participants.

A Participant may limit its cooperation in relation to cross border enforcement at its sole discretion. The following is a non-exhaustive list of such circumstances:

(i) The matter is not within the Participant's scope of authority or their jurisdiction.
(ii) The matter is not an act or practice of a kind that the Participant is authorized to investigate or
(i) enforce against in its domestic legislation.
(ii) There are resource constraints.
(iii) The matter is inconsistent with other priorities or legal obligations.
(iv) There is an absence of mutual interest in the matter in question.
(v) The matter is outside the scope of this Arrangement.
(vi) Another body is a more appropriate body to handle the matter.
(vii) Any other circumstances that renders a Participant unable to cooperate

If a Participant refuses or limits its cooperation then it should notify the reasons for refusal or limitation in writing to the Participant(s) requesting assistance where feasible four weeks of receiving the request for assistance.

A Participant may notify the Committee, either in its notice of intent to participate submitted in accordance with section 12 or in a separate notice that it will not

(a) disclose personal data to other Participants pursuant to this Arrangement;
(b) provide assistance under this Arrangement in respect of matters that would be considered criminal or penal under its laws; and/or
(c) provide assistance under this Arrangement in other circumstances that it may specify.

Failure to provide a notice pursuant to this section does not affect a Participant's discretion to limit its cooperation in respect of particular requests for assistance pursuant to this section.

6. CONFIDENTIALITY PRINCIPLE

6.1 Participants will, without prejudice to section 6.2, treat all information received from other Participants pursuant to this Arrangement as confidential by:

(i) treating any information received or requests for assistance pursuant to this Arrangement - which includes that another Participant is considering, has launched, or is engaged in, an enforcement investigation - as confidential , and, where necessary, making additional arrangements to comply with the domestic legal requirements of the sending Participants ;

(ii) not further disclosing information obtained from other Participants to any third parties, including other domestic authorities or other Participants, without the prior written consent of the Participant that has shared the information pursuant to this Arrangement;

(iii) limiting the use of this information to those purposes for which it was originally shared;

(iv) ensuring that, where a Participant receives an application from a third party (such as an individual, judicial body or other law enforcement agency) for the disclosure of confidential information received from another Participant pursuant to this Arrangement, the Participant that has received the application should:

a. oppose, or strive to minimise, to the fullest extent possible any such application;
b. maintain the confidentiality of any such information;
c. notify the Participant that supplied the information forthwith and seek to obtain that
d. Participant's consent for the disclosure of the information in question;
e. inform the Participant who shared the information and has refused consent for its disclosure, if there are domestic laws that nevertheless oblige the disclosure of the information.

(v) upon withdrawal from this Arrangement, maintaining the confidentiality of any confidential information shared with it by another Participant pursuant to this Arrangement, or with mutual agreement with other Participants, return, destroy or delete the information.

(vi) ensuring that all appropriate technical and organizational measures are taken so that any information provided to it under this Arrangement is kept secure . This includes returning or handling the information, (as far as possible to be consistent with national law) in accordance with the consent of the Participant that provided it.

6.2 Where domestic legal obligations may prevent a Participant from respecting any of the points in 6.1(i) – (vi), this Participant will inform the sending Participant(s) prior to the exchange of information.

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,

- 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 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 other arrangements as described above, will be made available to all Participants.

8. COORDINATION PRINCIPLES

All Participants will use their best efforts to coordinate their cross border enforcement activities. The following principles have been established to help achieve the coordination of cross-border enforcement of privacy and data protection laws.

(i) Identifying Possible Coordinated Activities

a. PEAs should identify possible issues or incidents for coordinated action and actively seek opportunities to coordinate cross-border actions where feasible and beneficial.

(ii) Assessing Possible Participation

a. PEAs should carefully assess participation in coordinated enforcement on a case-by-case basis and clearly communicate their decision to other authorities.

(iii) Participating in Coordinated Actions

a. PEAs participating in a coordinated enforcement action should act in a manner that positively contributes to a constructive outcome and keep other authorities properly informed.

(iv) Facilitating Coordination

a. PEAs should prepare in advance to participate in coordinated actions.

(v) Leading Coordinated Action

a. PEAs leading a coordinated action should make practical arrangements that simplify cooperation and support these principles.

For further explanation of these principles, Participants can refer to the International Enforcement Coordination Framework

9. RESOLVING PROBLEMS

Any dispute between Participants in relation to this Arrangement should ideally be resolved by discussions between their designated contacts and, failing resolution in a reasonable time, by discussion between the heads of the Participants.

10. ALLOCATION OF COSTS

Each Participant bears their own costs of cooperation in accordance with this Arrangement.

Participants may agree to share or transfer costs of particular cooperation.

11. RETURN OF EVIDENCE

The Participants will return any materials that are no longer required if, at the time they are shared, the Requested Participant makes a written request that such materials be returned. If no request for return of the materials is made, then the Requesting Participant may dispose of the materials using methods prescribed by the Requested Participant, or if no such methods have been prescribed, by other secure methods, as soon as practicable after the materials are no longer required.

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 Article 29 Working Party.

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 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
b. Arrangement;
c. Receive notices of commitment to Schedule One or such other arrangements as referenced in clause seven above and notices submitted in accordance with section 5;
d. Review such notices in order to verify that a PEA is eligible to sign this Arrangement;
e. Review the operation of the Arrangement three years after its commencement and submit its findings to the International Conference;
f. Publicise this Arrangement;
g. 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 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.

14. WITHDRAWAL FROM THE ARRANGEMENT

A Participant may withdraw participation in this Arrangement by giving one month's written notice to the Committee.

A Participant shall, as soon as reasonably practicable after notifying the Committee of its intention to withdraw participation in this Arrangement, take all reasonable steps to make its withdrawal from participation known to other Participants. This should include posting such information on the Participant's website whilst still participating in the Arrangement and for a reasonable period after ceasing to participate.

A Participant that is actively involved in a cross-border enforcement activity pursuant to this Arrangement should endeavour to satisfy its obligations in relation to such an activity before withdrawing from participation.

Regardless of withdrawal from the Arrangement, any information received pursuant to this Arrangement remains subject to the confidentiality principle under clause six and data protection principles referred to under clause seven and Schedule One of this Arrangement where relevant.

15. COMMENCEMENT

The Committee will accept notices of intent from the date of the 37th Conference and the Arrangement will commence once there are at least two Participants.

PEAs will become Participants once notified by the Committee of their acceptance.

SCHEDULE ONE

(1) Pursuant to clause seven of this Arrangement, the commitments in this Schedule may be appropriate to enable the exchange of personal data.

This Schedule does not, however, preclude circumstances where privacy and data protection laws of a Participant require further safeguards to be agreed between Participants in advance of any sharing of personal data.

As a minimum, provided both the Participants are in a position to enter into them, Participants exchanging personal data and committed to this Schedule will:

(i) restrict the sharing of personal data to only those circumstances where it is strictly necessary, and in any event, only share personal data that is relevant and not excessive in relation to the specific purposes for which it is shared; in any case personal data should not be exchanged in a massive, structural or repetitive way;

(ii) ensure that that personal data shared between Participants will not be subsequently used for purposes which are incompatible with the original purpose for which the data were shared;

(iii) ensure that personal data shared between Participants is accurate and, where necessary, kept up to date;

(iv) not make a request for assistance to another Participant on behalf of a complainant without the complainant's express consent;

(v) inform data subjects about (a) the purpose of the sharing (b) the possible storage or further processing of their personal data by the receiving Participant, (c) the identity of the receiving Participant, (d) the categories of data concerned, (e) the existence of the right of access and rectification and (f) any other information insofar as this is necessary to ensure a fair processing. This right can be limited if necessary for the protection of the data subject or of the rights and freedoms of others;

(vi) ensure that, data subjects have the right to access their personal data, to rectify them where they are shown to be inaccurate and to object to the exchange, storage or further processing of personal data relating to them. These rights can be limited if necessary for the protection of the data subject or of the rights and freedoms of others; the right to object can be further limited either where exercising this right would endanger the integrity of the enforcement action between Participants or where such a right interferes with other domestic legal obligations; ensure that where sensitive personal data are being shared and further

processed, additional safeguards are put in place, such as the requirement that the data subjects give their explicit consent.

(vii) adopt, when receiving personal data, all technical and organizational security measures that are appropriate to the risks presented by the exchange, further use or storage of such data. Participants must also ensure that security measures are also adopted by an organization acting as data processor on their behalf and such processors must not use or store personal data except on instructions from that receiving Participant;

(viii) ensure that any entity to which the receiving participant makes an onward transfer of personal data is also subject to the above safeguards.

(ix) ensure that, where a Participant receives an application from a third party (such as an individual, judicial body or other law enforcement agency) for the disclosure of personal data received from another Participant pursuant to this Arrangement, the Participant that has received the application should:

a. oppose, or strive to minimise, to the fullest extent possible any such application.
b. notify the Participant that supplied the information forthwith and seek to obtain that
c. Participant's consent for the disclosure of the information in question.
d. inform the Participant who shared the information and has refused consent for its disclosure, if there are domestic laws that nevertheless oblige the disclosure of the information.

(x) ensure mechanisms for supervising compliance with these safeguards and providing appropriate redress to data subjects in case of non-compliance;

(2) In this Schedule, 'sensitive personal data' means:

a. Data which affect the complainant's most intimate sphere; or
b. Data likely to give rise, in case of misuse, to:
   (i) Unlawful or arbitrary discrimination; or
   (ii) A serious risk to the data subject.

In particular, those personal information which can reveal aspects such as racial or ethnic origin, political opinions, or religious or philosophical beliefs as well as those data relating to health or sex life, will be considered sensitive data. The applicable national legislation may lay down other categories of sensitive data where the conditions referred to in the previous paragraph are met.

9. Task 2.2 – Summary Report on Enforcement Cooperation Tools and Initiatives

INTRODUCTION

This document is intended to accompany the **Report of Activity 2016-2017 of the Group of Experts on Legal and Practical Solutions for Cooperation**.

In the Experts' responses to the Co-chairs' survey at the outset of this project, they identified the need: (i) for more and better enforcement cooperation tools; and (ii) to explore what tools are available to privacy enforcement authorities via other networks.

The Experts therefore conducted a cursory review of the resources made available by the following networks, which respective experts suggested as being relevant for consideration:

NETWORK
ICDPPC (International Conference)
GPEN (Global Privacy Enforcement Network)
APPA (Asia Pacific Privacy Authorities)
RIPD (Ibero-American Data Protection Network)
CTN (Common Thread Network)
AFAPDP (Assn. francophone des autorités de protection des données personnelles)
WP29 (Article 29 Working Party) and EDPB (European Data Protection Board)[23]
CEEDPA (Central and Eastern European Data Protection Authorities)
OECD Working Party Security and Privacy in the Digital Economy (WP SPDE)
ICPEN (International Consumer Protection Enforcement Network)
UCENet (Unsolicited Communications Enforcement Network)
APEC (Asia-Pacific Economic Cooperation)
COE (Council of Europe) – Convention 108 – T-PD-Committee
PHAEDRA project
IAPP (International Association of Privacy Professionals)
International Coordinating Committee of National Human Rights Institutions (GANHRI)
UNODC (UN Office on Drugs and Crime)

The tools and initiatives identified in this Annex represent a summary of the results of that research, and are organized into two groups:

[23] The Group did not receive a research report for European Commission WP29/EDPB but were provided with information by two Experts in relation to tools and initiatives associated therewith, and these are included below. It should further be taken into account that WP29 will be replaced by the European Data Protection Board (EDPB) in May 2018, potentially having broad effects on nature and availability of cooperation tools.

1. The first list is intended to serve as a non-comprehensive representation of the various types of privacy enforcement cooperation tools and initiatives that are currently available to privacy enforcement authorities.

2. The second list represents potential future enforcement cooperation resources that flow from either Experts' survey responses, or their research into resources currently available via networks outside of privacy and data protection.

The research reports of the individual experts are appended to this Annex, and reference various other resources that, while not necessarily directly related to enforcement cooperation, may be of interest to ICDPPC members.

1. EXISTING PRIVACY ENFORCEMENT COOPERATION TOOLS AND INITIATIVES

The below list of enforcement cooperation tools currently available to privacy enforcement authorities has been categorized broadly into two types: (A) those relevant to enforcement cooperation on specific investigations; and (B) those that may facilitate enforcement cooperation more generally.

Recommendation: The Experts' survey responses suggested certain tools that our research revealed are, in reality, currently available to many (or all) ICDPPC members via various networks. This evidences a challenge that is two-fold: (i) enhancing broad awareness of the existence of such tools, and (ii) rendering them easily and intuitively accessible by relevant authorities.

The Group would, therefore, suggest the creation of an easily accessible repository, on the ICDPPC website, where members could find a comprehensive list and description of available enforcement cooperation resources, as well as links thereto (with authorization from the respective networks for links to non-ICDPPC resources). This could be a living repository, updated to include further resources as they are developed. Once created, there would be a broad communications launch to ICDPPC members (including through ICDPPC social media channels), sensitizing the membership to the various tools, as well as their source and potential utility.

A. Specific Enforcement Cooperation Tools and Initiatives

We have identified four broad categories of enforcement cooperation resources: (i) the identification, evaluation and contact of potential partners; (ii) the sharing of confidential information or personal data; and (iii) enforcement cooperation guidance; and (iv) coordinated compliance initiatives.

i. Authority Lists and Registries

The following resources may provide information that would assist in the identification, evaluation and contact of potential enforcement cooperation partners.

ICDPPC: Member List (incl. links to websites and social media, contacts list maintained by Executive Secretariat):

- https://icdppc.org/participation-in-the-conference/members-online/

APPA: Member List (incl. agency head, link to website)

- http://www.appaforum.org/members/

CTN: Members and Observers List (incl. contacts, website link, jurisdictional information):

- https://commonthreadnetwork.org/home/membership/

WP29: Composition and Structure and a Member List.

- http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

GPEN: Several relevant tools for members (www.privacyenforcement.net):

- Members List (authority name only)
- Privacy Authorities Page (general contact, jurisdiction, legislation, etc.)
- Enforcement Contacts List (consolidated for GPEN / OECD / APEC)

RIPD: Member List (authority name and website links)

- http://www.redipd.es/la_red/Miembros/index-iden-idphp.php

CEEDPA: Various lists (incl. members, website links, and an online contact tool)

- http://www.ceecprivacy.org/main.php

AFAPDP: Member list (authority name and website links), a list of French-speaking countries with data protection laws and links to those laws.

- https://www.afapdp.org/

UCENet: Developing Inventory of Experts within each member authority, to be available on members-only section of the site, and serve as contacts for specific forms of engagement.

ii. Sharing Confidential Information (including, potentially, personal data)[24]

ICDPPC: **Global Cross Border Enforcement Cooperation Arrangement** – (12 participants) global arrangement that allows bi-lateral and multilateral cooperation on enforcement cooperation matters amongst participants

- https://icdppc.org/wp-content/uploads/2015/02/Global-Cross-Border-Enforcement-Cooperation-Arrangement.pdf

APEC: **Cross-border Privacy Enforcement Arrangement** – (10 participants) regional arrangement that allows the request for and provision of enforcement cooperation assistance by Asia-Pacific participants

- http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

UCENet: **Memorandum of Understanding** – (11 participants) facilitates cooperation and information sharing amongst member participants.

GPEN: **GPEN Alert Tool** – (10 participants) Secure online platform for sharing confidential information relating to potential or ongoing investigations. It is accessible, via a link on the GPEN website, to GPEN members who have signed an MOU and committed to certain security requirements.

Council of Europe**: Convention 108** (50 participants, 47 COE Members States plus 3 others) – While this treaty provides that Member States will take the necessary steps in their domestic legislation to apply the data protection principles set out in the Convention, it also provides for enforcement cooperation, and in particular, confidential information sharing between parties.

iii. Enforcement Cooperation Guidance

ICPPDC: **Enforcement Cooperation Handbook** - a practical guide that provides a continuum of enforcement cooperation models, suggested strategies and tactics, and factors to consider in determining the appropriate approach in specific circumstances. Also includes various template arrangements/tools.

[24] Experts noted that EU Data Protection Directive 95/46/EC (applicable to 28 EU member states, as well as Liechtenstein, Norway and Iceland) foresees that member authorities shall cooperate with one another, in particular by exchanging all useful information (which may include personal or confidential information).

- https://icdppc.org/wp-content/uploads/2015/03/Enforcement_cooperation_handbook_2016_-_en.pdf

iv. Enforcement Cooperation Compliance Initiatives

GPEN: Each year since 2013, GPEN has organized the **Global Privacy Sweep**, whereby during a specified week, privacy enforcement authorities from around the world (generally 25-30 per year) conduct a review of organizations' privacy practices related to an important or emerging privacy theme (e.g., mobile, children, Internet of Things), with a view to identifying potential contraventions or trends for individual or collaborative follow-up. This highly impactful non-formal enforcement initiative builds on inspiration from the ICPEN Annual Sweep and we note that UCENet held its first Sweep in 2017. The Sweep kits, which have been produced for each issue-specific GPEN sweep, also contain useful principles and approaches for non-formal enforcement initiatives (available in the Documents library on the GPEN website).

B. Sharing Best Practices & Lessons Learned, and Networking

The resources outlined below are available to support cooperation and knowledge transfer for general enforcement and compliance matters.

i. Information Sharing Tools and Initiatives[25]

CEEDPA: Password protected **Forum** allows information exchange amongst members:

- http://www.ceecprivacy.org/main.php?s=4

GPEN:

- Website (https://www.privacyenforcement.net/) includes a members-only platform housing various information sharing tools:
  - **Discussion Forum** - allows members to engage in online discussions regarding non-confidential privacy enforcement matters
  - **Document Library** - allows authorities to share non-confidential documents related to enforcement cooperation, including published findings, positions, practices

[25] Experts noted various reference tools available that provide searchable access to substantive privacy and data protection information (e.g., juris prudence, investigative decision, guidance, and other resources) – e.g., the Wordlii database available via the GPEN and ICDPPC websites, the RIPD's new Corpus Iuiris platform, as well as the WP29's CIRCA BC platform (soon to be replaced by a EPDB platform under the GDPR).

- **Network of Networks** – creates linkages between networks for sharing of information, and seeks to find collaboration opportunities between Networks

ii. Enforcement Cooperation Meetings and Teleconferences

The networks examined, including the ICDPPC, generally hold regular in-person meetings, often with enforcement matters as a focal point of the agenda (e.g., scheduled on an annual or semi-annual basis).

ICDPPC:

- The ICDPPC has initiated a program whereby it will endorse events organized by individual member authorities and/or other networks as **ICDPPC-recognized enforcement cooperation events**.
  - https://icdppc.org/news-events/enforcement-cooperation-meetings/

- The ICDPPC website (www.icdppc.org) has a **calendar of relevant privacy and data-protection related events**:
  - https://icdppc.org/news-events/events-calendar/

GPEN:

- **Pacific and Atlantic teleconferences** (approx. monthly for each) – allow member participants to discuss various subjects related to privacy enforcement cooperation.

WP29: Sub-groups meet regularly to advance enforcement cooperation:

- **Cooperation Subgroup** – preparing tools for future cooperation mechanisms according to the GDPR (e.g., "One-Stop", "Mutual Assistance" and "Joint Operations") as well as for current cooperation needs (e.g. common complaint form for referral between DPAs).

- **Enforcement Subgroup** - coordinating ongoing enforcement by member authorities with regard to international companies, as well as observing emerging trends in markets and technology, evaluating possible needs for new coordinated enforcement activities of EU DPAs.

iii. Enforcement Cooperation Training and Capacity Development

GPEN:

- **Enforcement Practitioners Workshop** (Pilot June 2017 - potentially annual or bi-annual) provides an opportunity for

operational level staff from within and outside privacy to share and learn practical investigative skills and strategies.

- **Opportunities Board** - allows authorities to publicize training, secondment or job opportunities available to GPEN member staff.

AFAPDP: Regular training, or ad hoc assistance, provided to members and their employees, face-to-face and online, taking into account the cultural and legal diversity of those members. Training materials made available via a members-only section of the website.

- https://www.afapdp.org/a-propos/espace-membres

CoE – T-PD: **European Case Handling Workshop** (generally open to DPAs of Convention 108 Parties), covers a broad spectrum of topics that might be relevant for DPAs current or future work, with the purpose being to exchange experience/expertise/information, and networking.

APPA: **Secondment Framework** – provides guidance and templates to authorities wishing to implement a secondment from one data protection authority to another.

- http://www.appaforum.org/resources/secondments/

Note: The US-FTC and EDPS (for staff from DPAs within the EU), as well as the Canadian OPC / UK-ICO (jointly), have established practical models that have served to facilitate staff interchanges or exchanges.

UCENet: Working to develop a **training programme**. Sessions will be recorded where possible and included in a restricted area on the UCENet website.

2. POTENTIAL FUTURE ENFORCEMENT COOPERATION PROJECTS

Recommended Initiatives

The Marrakesh Resolution on International Enforcement Cooperation (2016) (the "Marrakesh Resolution") mandated the ICDPPC Executive Committee to "further discuss with GPEN and other relevant networks with a view to creating practical projects that better coordinate the efforts towards global enforcement cooperation". The following potential initiatives could serve as such "practical projects" for consideration in the short term, in carrying out that mandate.

A. Comprehensive Authorities Database

We note that there are various resources available listing member authorities, within and outside the privacy and data protection sectors.

Each of these provides different, but generally limited, information – e.g.: authority name; general contact information; specific enforcement contacts; and/or operational and jurisdictional details. All of this information may be relevant to the identification, evaluation and contact of potential enforcement cooperation partners, but no one available resource currently provides access to all this information for privacy enforcement authorities, or authorities in other relevant sectors (e.g., consumer protection). The challenge faced mirrors that outlined above – ensuring awareness and readily available access to information on ICDPPC members and key stakeholders. Authorities and networks must also maintain such information in various locations.

The Experts see value in the development and population of a comprehensive database, like that specifically referenced in Item 3 of the Marrakesh Resolution on International Enforcement Cooperation (2016). Based on examples viewed in other sectors, such a database could list, for all ICDPPC members as well as other privacy networks (and perhaps other authorities relevant to privacy enforcement): (i) general information and website hyperlink; (ii) office size and structure; (iii) enforcement contact details; (iv) legal authority to cooperate (including mechanisms pursuant to which they can cooperate, and requirements for information or assistance requests); and (v) links to domestic legislation and case law (including evidence-gathering requirements, definitions of personal data and confidential data).

In particular, we would draw your attention to the UNODC's SHERLOC (sharing electronic resources and laws on crime) website (https://www.unodc.org/cld/v3/sherloc/). While this website requires an account to log-in, the home page references a registry of information reflective of that which might be useful for purposes of privacy enforcement cooperation. Further information could likely be obtained on this database, and various other relevant tools, by reaching out to the UNODC directly.

Consideration can also be given to the most efficient method of populating such a data-base and keeping it current, and whether a wiki-format may be preferable to the standard data-base caretaker approach.

B. Dedicated Repository for Sharing Enforcement Cooperation Accomplishments, Lessons Learned and Best Practices

The Experts' indicated the need for improved communication with respect to enforcement cooperation experience, successes and lessons learned, on specific cases.

One interesting model is from the UNODC. It developed the Digest of Organized Crime, which provides guidance on implementing the *Organized Crime Convention* ("OCC") through case studies as well as examples of best practices and international cooperation: https://www.unodc.org/unodc/en/organized-crime/digest-of-organized-crime-cases.html

Another option for sharing such experience is to create a central repository where privacy enforcement authorities could share such lessons learned in the form of individual case studies or presentations. Given the nature of the information that would be included in such a repository, it would likely be most appropriately situated in a restricted access website.

Such a repository could also facilitate annual updates to the ICDPPC Enforcement Cooperation Handbook, with key lessons and examples being showcased in that document.

Other Potential Initiatives

The following represent other potential initiatives for future consideration:

C. Cross-Sectoral Information Sharing Platform

While not included in the Experts' research reports, we note that the newly formed EDPS-led Digital Clearing House, an informal network of authorities in the privacy, consumer protection and competition law sectors (where issues are increasingly intersecting) are exploring the potential of creating an online platform for authorities to share non-confidential information in support of greater cross-sector cooperation and awareness– see: https://edps.europa.eu/data-protection/our-work/subjects/big-data-data-mining_en. This initiative is deemed by the Experts to merit ongoing monitoring of its evolution.

D. Cross-border Multi-jurisdictional Online Complaint Tool

The group noted with interest, the ICPEN Econsumer.gov initiative, a joint effort to gather and share cross-border e-commerce complaints of consumer protection agencies from 36 countries. The project has two components: a multilingual public website, where consumers can lodge cross-border complaints, and try to resolve their complaints through means other than formal legal action; and a password-protected website through which the incoming complaints are shared with the participating consumer protection law enforcers. The website is currently available in English, French, German, Korean, Japanese, Polish, Spanish, and Turkish.

E. Teams of Case Handlers/Practitioners

The Experts noted that there may be value in further exploring the possibility of developing a mechanism for creating teams of Case Handlers and Practitioners to address matters of multi-jurisdictional significance (like we see in some MLA instruments). Such teams could bring together selected staff members who have acquired or proven specific expertise or skills that are deemed to be relevant to the conduct of a joint investigation envisaged by two or more Supervisory Authorities. Each team member would provide his/her own skills and expertise as input to the joint investigation. Each individual team member would directly benefit from others´ experience, and the team as a whole would benefit from each other's complementary expertise, thus enhancing the level of the joint team´s achievements. Such a strategy could leverage the relative strengths of partner authorities, and avoid duplication of effort to achieve more impactful outcomes more efficiently.

F. Model Bilateral or Multilateral Cooperation Treaties/Agreements/Clauses

Survey responses indicated that some authorities are unable to engage in cooperation via a non-binding MOU like the ICDPPC Arrangement. The Group of Experts agreed to explore, on a preliminary basis, potential solutions to this issue via task 2.3, which is covered separately in the Report.

10. Task 2.3 - Summary Report on Additional Frameworks

Introduction

This document is intended to accompany **Section 2.3 of the Report of the Group of Experts on Legal and Practical Solutions for Cooperation**.

The Group of Experts (the "Experts") acknowledge that there is much investigative enforcement cooperation that can be achieved via existing instruments, including the ICDPPC Arrangement, the APEC Cross-border Privacy Enforcement Arrangement and various bilateral MOUs. Many authorities, like the current participants in those arrangements, are able to cooperate pursuant to a non-binding instrument. Furthermore, with respect to authorities that are unable to share personal data via such arrangements, the Experts acknowledge that certain forms of cooperation on specific enforcement matters, like those identified in Principle 3(b) of Workstream 1, can be highly productive absent the need to share any personal data (e.g., for the sharing of technical analysis or confidential representations from an organization regarding its policies and practices). That said, it may not always be possible to sever all personal data from source documents, depositions, and other evidence (e.g., relating to the individuals who created these sources, where addressees in correspondence, or are otherwise named in them).

Certain Experts also identified in their responses to the Co-chairs' initial survey, that their respective authorities would be unable, legally or practically, to use such non-binding arrangements to: (i) cooperate on specific enforcement matters at all; or (ii) engage in certain forms of enforcement cooperation, like those involving the exercise of formal powers in the gathering of evidence for another authority. Those authorities may require a formal legal instrument be it in the form of an international treaty or agreement, to engage in such cooperation.

Recognizing that privacy and data protection are becoming an increasingly global issue, with individuals' data flowing seamlessly across borders within and amongst both large multinational organizations and small businesses, the Experts identified the desirability of exploring, on a preliminary basis, as a further step in addition to the development of the Key Principles for legislation (Workstream 1), additional framework options that might allow for a broader geographic and/or functional scope of enforcement cooperation.

Workstream 2.3 was therefore created to review a sample of existing cooperation frameworks in various sectors, with a view to determining: (i) if further evaluation of additional framework options appears to be warranted; and if deemed appropriate, (ii) the recommended scope for a subsequent working

group to conduct such further evaluation. **For clarity, the Group's agreed objective for this task was to better understand these frameworks via a cursory review of the texts thereof; it was <u>not</u> to evaluate the appropriateness of any of these options for privacy enforcement cooperation. It was agreed that such an evaluation would be, if deemed appropriate, subject to terms of reference established for a subsequent working group.**

The Experts identified the following frameworks for examination, and then drafted a brief research report for each (these reports are appended to this Annex).

This list contains frameworks providing for cooperation on specific enforcement matters:

Enforcement Cooperation Framework
1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108")
1988 Convention on Mutual Administrative Assistance in Tax Matters (as amended by the Protocol of 2010) (herein after the "Tax Convention")
Convention on Cybercrime ("CoC")
2000 UN Convention against Transnational Organized Crime (UNTOC)
2003 Agreement on mutual legal assistance between the European Union and the United States of America ("EU-US MLA")
Agreement Between the United States of America and Canada Regarding the Application of Their Competition and Deceptive Marketing Practices Laws ("US-Canada Agreement")
Ibero-American Data Protection Standards ("RIPD Standards")
International Organization of Securities Commissions (IOSCO) Multilateral MOU and Enhanced Multilateral MOU ("IOSCO E-MMOU")
Unsolicited Communications Enforcement Network MOU ("UCENet MOU")

The Experts also opted to review the following frameworks, which they felt, while not directly related to enforcement cooperation, might provide broader relevant inspiration:

Other Frameworks
International human rights law Optional Protocol to the Convention against Torture (OPCAT)
UN Commission on International Trade Law (UNCITRAL)
The International Covenant on Civil and Political Rights (ICCPR)

Summary Conclusion and Recommendation

The Group identified three broad types of enforcement cooperation frameworks (in addition to a fourth, whereby an authority can cooperate pursuant to its domestic legal framework without the need for a specific cooperation instrument): (i) non-binding arrangements; (ii) bi-lateral or multi-lateral agreements; and (iii) international treaties.

Ultimately, the Group noted that each of the three types of frameworks outlined above has relative benefits and challenges, and each has been implemented to facilitate a broad range of cooperation and assistance in respect of specific administrative and criminal enforcement matters.

It was not within the scope of the Experts' work to evaluate the potential appropriateness of those frameworks as additional mechanisms for cooperation on specific privacy and data protection enforcement matters. We believe, however, that such work would be valuable. We therefore recommend the establishment of a subsequent working group to evaluate whether any of these options may be feasible and effective in broadening the geographic and functional scope of cooperation on specific privacy enforcement matters.

The summary below represents a synthesis of those research reports reviewed in conjunction with some further review of the underlying instruments.

General Observations

At the outset, it should be noted that, except for Convention 108, none of the existing legally binding frameworks that the Experts examined provides for cooperation on specific privacy or data protection enforcement matters. Frameworks were suggested by the respective Experts based on their perceived potential to offer insights into the structure, scope and/or implementation of an additional framework for privacy enforcement cooperation.

A Brief Note regarding the RIPD Standards

In June 2017, the RIPD Network members adopted the RIPD Standards. These standards, a set of detailed data protection legislative principles, represent non-binding recommendations for member states. The aim is that they will be adopted via new or updated national legislation, where such legislation is not yet consistent with the RIPD Standards, thus creating a more harmonized regulatory data protection framework in the region.

The standards themselves do not provide the legal basis for enforcement cooperation. They do, however, allow for the adoption of international cooperation mechanisms to facilitate the application/ implementation/

enforcement of national legislation, which may provide for, among other forms of cooperation, assistance among States through: (i) notifications and submission of complaints; (ii) assistance in investigations; and (iii) exchange of information.

A Continuum of Enforcement Cooperation Frameworks

Based on the various frameworks examined, we can see that international enforcement cooperation generally occurs via a continuum of mechanisms - from an ability to cooperate that is rooted in domestic or regional law, through to that which is fully defined and legally required (subject to certain limited caveats) pursuant to a bilateral or multilateral agreement or treaty. Specifically, we have identified four types of frameworks:

1. A domestic legal framework that allows for enforcement cooperation (information sharing and/or assistance) without the need for any additional instrument, binding or otherwise;

2. A non-binding enforcement cooperation arrangement or MOU between authorities; and

3. Two forms of legally binding instruments allowing for (or potentially requiring, subject to limited caveats), the sharing of information and the provision of assistance:

    a. A bi-lateral or multi-lateral agreement between states in respect of cooperation between authorities; or

    b. An international mutual legal assistance (MLA) treaty.

    Such instruments could be, in turn, based on a model agreement or treaty.

This document will provide, based on the Experts' research reports and a cursory review of the underlying instruments, an overview of our observations in respect of: (i) non-binding arrangements, like those that are currently most prevalent in privacy enforcement cooperation; and (ii) legally binding agreements or treaties, which we often see in other sectors, and which have been suggested for further consideration by certain of the Experts.

We reviewed these frameworks with a view to assessing the following aspects: (i) level of participation; (ii) the scope of investigative measures provided for; (iii) the scope of legal proceedings in respect of which participants can cooperate; (iv) any special provisions with respect to personal data protection; (v) applicable law provisions; and (vi) the manner of implementation.

We did not endeavour to evaluate the relative merits of the frameworks, which would be the task of a subsequent working group, should the ICDPPC opt to accept the Group's recommendation as outlined at the end of this Annex. Further, we will not provide a full account of each framework reviewed - the Experts' research reports are included at the end of this report's Annex[26]. Finally, we will speak only in general terms about the UCENet MOU, which has not been made public.

i) Participation

Binding enforcement cooperation instruments can range from bi-lateral agreements (e.g., US-Canada Agreement) to global treaties (like several of those the Experts reviewed). We saw similar potential for non-binding enforcement cooperation MOUs, which can also involve broad global participation (e.g., the IOSCO E-MMOU, with over 100 participants). We note as well that the IOSCO E-MMOU generates over 3,000 requests for information each year.

ii) Scope of Investigative Measures

Several of the treaties reviewed (Convention 108, UNTOC, COC, EU-US MLA and Tax Convention) provided for a broad range of specific investigative measures in providing assistance – for example (in one or more of the five conventions):

- exchange of information spontaneously or upon request, for unilateral or parallel investigations,
- compelling the provision of digital, physical and oral evidence,
- search and seizure,
- videoconference testimonies or investigative statements,
- cooperation in joint investigative teams,
- recovery of amounts owing and conserving assets,
- service of documents, and
- any other type of assistance that is not contrary to the domestic law of the requested State Party.

The US-Canada Agreement, a binding international agreement, also specifies a similarly broad range of investigative measures including information sharing, territorial visits, locating/securing witnesses and evidence, the initiation of enforcement action on behalf of the other party, and the joint examination of relevant issues.

With respect to the MOUs, the scope of investigative measures provided for ranged widely, from:

i. under the UCENet MOU, principally sharing of confidential information; to

[26] This applies to the full unabridged version of the Document Package of the Group of Experts which includes all Annexes.

ii. under the IOSCO E-MMOU, broad investigative measures not unlike those provided for under the treaties outlined above, including but not limited to - information sharing (including by obtaining ISP and telephone records), evidence gathering (including by compelling physical attendance for testimony), and freezing assets.

iii) Scope of Proceedings

UNTOC, COC and the EU-US MLA Agreement provide for cooperation primarily in criminal matters. The Tax Convention, on the other hand, provides an interesting example for data protection cooperation, as it provides primarily for cooperation in respect of administrative (or non-criminal) matters. Also the EU-US MLA Agreement allows for cooperation with administrative authorities.

With respect to the nature of proceedings in respect of which participants could cooperate, the MOUs either:

i. do not specify or limit the nature of such proceedings, or

ii. for the IOSCO E-MOU, specifies that participants could cooperate in respect of a broad range of proceedings, including civil, administrative and criminal proceedings.

iv) Treatment of Personal Data

In reviewing the treaties, we saw no consistent approach to the treatment of personal data. UNTOC, which inherently involves the sharing of personal data, does not specifically address the issue, although it does recognize the importance of data protection in its preamble. While the US-Canada Agreement provides for confidentiality of exchanged information, which could include personal data, it does not provide specifically for the treatment of personal data.

On the other hand, the Tax Convention provides that the requested party can require, as a condition of providing the requested information, that the requesting party comply with specified personal data safeguards as required under its domestic law. The EU-US MLA Agreement addresses use purposes, use limitations and data protection issues, thereby explicitly excluding the generic restriction of cooperation based on possible non-"adequacy" of the data protection regime of the states concerned[27]. In the case of the UN-based international human rights law ("IHRL") regime, only one treaty explicitly

[27] Against the backdrop of all earlier attempts to try and build "privacy bridges" between Europe and the rest of the world, the data protection solution offered in the EU-US MLA Agreement may represent a simple solution of particular note.

addresses personal information - OPCAT simply maintains that none will be published without the express consent of the person concerned.

While, unlike the ICDPPC Arrangement, none of the MOUs reviewed specifically addressed the treatment of personal data, none created a legal obligation to share information, such that participants presumably can (or could) stipulate certain data protection requirements as a condition of sharing information.

v) Applicable Law

The Experts raised the question of how "applicable law" (or "governing law") is addressed in the context of enforcement cooperation instruments. The instruments reviewed did not specifically address this issue. We note, however, that matters of interpretation or dispute resolution under an international agreement would generally be determined according to international law (vs. the domestic laws of one of the State participants).

We did note, however, that for legally binding treaties and agreements, domestic law is generally specified as relevant for determining the appropriate conduct of an authority taking particular action (e.g., an authority will not be required to do anything that would be contrary to its own laws). Similarly, the EU-US MLA Agreement does provide for the State law that will apply for certain operational aspects of the agreement.

vi) Implementation

Treaties and MLA agreements will generally be signed by participating States. The negotiation of treaties, generally being directly between state governments, can therefore be a time-consuming endeavour, often requiring years to finalize. State Parties are then generally required to take all necessary measures in accordance with domestic law to ensure ratification and, as far as non-self-executing provisions are concerned, implementation. Moreover, any State Party to the *Vienna Convention on the Law of Treaties* would be subject to thereto.

By contrast, many authorities can enter into non-binding MOUs or arrangements, more expeditiously, without the involvement of their state governments.

Conclusions

After the review outlined above, the Experts observed that cooperation on specific enforcement matters occurs across various sectors via informal arrangements, bi-lateral and multi-lateral agreements and international treaties.

The Experts identified that there were both benefits and challenges associated with the various types of frameworks outlined in this annex. While we have not

endeavoured to suggest conclusions with respect to the potential appropriateness of any of these frameworks for the purposes of privacy and data protection enforcement cooperation, we would highlight several high-level observations in relation to arrangements vs. agreements and treaties.

Arrangements: The Experts recognize that cooperation amongst DPAs is currently taking place pursuant to existing MOUs, like the ICDPPC Arrangement and APEC-CPEA. Further, the actively utilized IOSCO Arrangement, although from a different regulatory field, is an example of how an MOU can provide for a breadth of cooperation and assistance in respect of administrative matters amongst over one hundred participant authorities. The view was also expressed that arrangements or MOUs may be more easily implemented and amended (vis-à-vis legally binding instruments), while allowing for informal and efficient cooperation between authorities.

MLA Agreements/Treaties: On the other hand, it was also identified that some authorities will be, legally or practically, unable or limited in their ability (e.g., in the breadth of cooperative measures or in the sharing of evidence containing personal data) to cooperate pursuant to an MOU. The Experts reviewed several legally-binding instruments, including a bi-lateral agreement and several international treaties, that provided for a breadth of cooperation on administrative and/or criminal matters.

We see this work as an important preliminary step, filling an information gap and, hopefully providing a valuable resource for future strategic planning purposes.

Recommendation

Mapping out the current landscape has illustrated that enabling investigative enforcement cooperation at a global level is a complex matter, whereby there may be no "one-size fits all" solution. There is more work to be done in this area, but such work is outside the scope of this working group.

The Experts therefore propose the creation of a new working group, via resolution at the International Conference in Hong Kong in September 2017, to build upon the work completed by the Experts in this Workstream, by evaluating potential additional framework options, with a view to determining their feasibility and potential to broaden the geographic and functional scope of cooperation on privacy and data protection enforcement matters.

Such an evaluation could include, at the discretion of the working group, a brief survey to determine the frameworks pursuant to which ICDPPC member authorities could cooperate, as well as the perceived pros and cons of such frameworks. The options to be further considered and evaluated could include, without limitation (and in addition to the recommendations arising out of Workstream 1 and 2.1):

i. developing a model MLA treaty, inspired by existing examples, like those examined by the Experts, and others, with a view to ultimately encouraging national governments to implement such an instrument;

ii. developing a model agreement or set of model clauses, based on the various instruments the Experts reviewed, including the Arrangement, to serve as the foundation for bi-lateral or multi-lateral MLA agreements between States (on behalf of relevant enforcement authorities); and/or

iii. further promotion and education to encourage increased participation in the existing ICDPPC Arrangement.

Note: Option (iii), implementable in the short term, recognizes that implementation of the key Principles outlined in Workstream 1, as well as amendments to the Arrangement as proposed under Workstream 2.1, could also result in more authorities being able to cooperate pursuant to the Arrangement.

11. Terms of Reference – Group of Experts

GROUP OF EXPERTS ON LEGAL AND PRACTICAL SOLUTIONS FOR COOPERATION

Background

At the ICDPPC 2016 in Marrakech, Morocco, the International Conference of Data Protection and Privacy Commissioner (ICDPPC) adopted a new resolution on International Enforcement Cooperation, one in a series of past conference resolutions which makes progress on this important work stream in the ICDPPC's strategic work plan. The Resolution mandates the establishment of a new Group of Experts on the theme of international enforcement cooperation.

The following paragraph from the resolution outlines the work of the new Group of Experts:

'1) To mandate a new Working Group of Experts comprised of interested International Conference members and ideally, representative of the Conference membership from across the different global regions to develop a proposal for key principles in legislation that facilitates greater enforcement cooperation between members. The principles could be adapted by individual members to their national, regional and local needs. The principles would be accompanied by an explanatory memorandum that can be presented to national governments by individual members and where appropriate, observers. In addition, the Working Group is encouraged to suggest other measures that it feels may improve effective cross-border cooperation in the short or long term. The Working Group is encouraged to work in cooperation with other networks of privacy enforcement authorities active in cross-border enforcement cooperation, and to consult with networks of enforcement bodies from other sectors where appropriate, and is directed to report back to the 39th Conference on the product of its work.'

Title of the established entity

The Group of Experts on Legal and Practical Solutions for Cooperation shall be known as "the Group of Experts", and hereafter referred to in these Terms as 'the Group'.

This document sets out the Terms of Reference for all members of the Group. Each Expert agrees to abide by these Terms in their contribution to the Group's activities.

Mission

The Group is a working group of Experts from data protection and privacy enforcement authorities. Designated Experts have volunteered their time and expertise to carry out the mandate provided by the ICDPPC Resolution as outlined in the section 'background'.

The Experts are used to applying and enforcing data protection and privacy regulation and will use this focused and time-limited project space to build on past efforts to ultimately facilitate greater enforcement cooperation between members of the ICDPPC.

Length of mandate

The expected duration of activities undertaken by the Group will be December 2016 – September 2017. If any additional time is to be requested, the extension of the Mandate given to the Group by the ICDPPC would be at the discretion of the 2017 edition of the ICDPPC in Hong Kong.

The Group should therefore make all best efforts to try to come up with a distinct product for presentation at the 39th ICDPPC in Hong Kong in 2017.

Chairperson(s)

The Group shall agree on two Co-chairs to steer the activities of the Group. The Co-Chair's term shall be for the length of Mandate that the ICDPPC granted to the Group i.e. until September 2017.

The Co-chairs shall mutually agree on a reasonable arrangement to share the work of chairing the group. This arrangement should facilitate the timely and effective delivery of the products of the Group to the ICDPPC.

The Chairs shall be nominated and agreed at the first meeting of the Group.

It is possible for an Expert to be appointed to lead a specific area of the Group's work, working in collaboration with the Co-chairs and with the same goal of ensuring an effective output.

Composition – the Experts

Any ICDPPC member should be able to participate. The aim will be to ensure regional diversity in the composition of the Group. Each participant comes to this equally. It is also voluntary for conference members to participate.

Each Expert shall have sufficient expertise and knowledge to enable them to discuss the merits and disadvantages of their own national laws as well as compare them to the laws in other jurisdictions, and ideally, of international enforcement cooperation in practice. Prospective Experts shall also confirm at application to become a member of the Group that they possess a level of decision making authority, or ready access to such authority, in order to promote momentum and satisfactory progress of the work.

Experts from jurisdictions that do not have specific intentions to update their national law can still be part of the Group and contribute to a wider global initiative to encourage governments to improve cooperation in a like-minded way according to the direction provided by the Group's work.

Those Experts interested to become a member of the Group should apply to the Administration Team of the Group of Experts with:

- their expression of interest
- contact details
- confirmation that they meet the criteria outlined in these Terms of Reference
- confirmation that they agree to abide by the Terms of Reference.

Termination of membership

Any Expert wishing to terminate their membership to the Group should indicate their wish to the Chair(s) giving 14 days' written notice.

Organisation of tasks

The Group shall endeavor to meet face-to-face and virtually e.g. by teleconference on at least three occasions.

The dates for the face-to-face meetings (in the form of a calendar roadmap for the work) shall be agreed at, or shortly after, the first meeting with agreement of the Chair(s).

The Group can decide, by agreement with the Co-Chairs to establish sub-groups to deal with individual work streams which can meet in person, or virtually, by agreement.

Tasks

The Group of Experts will focus primarily on the development of recommended legislative principles, and two associated documents:

- One set of legislative principles.
- One explanatory memorandum explaining the rationale for the legislative principles.
- A short piece of practical guidance for ICDPPC members on how to use the documents with their legislators/governments at national level.

Such work could also include, should time and resources be available: development of a plan to raise awareness of the need to update national legal frameworks, making the Group's work available to shortlisted entities to be decided later, such as the UN.

The Group of Experts will also work, secondarily, on the development and suggestion of other pragmatic measures that it considers may improve cross-border cooperation. Specifically, this could include but not be limited to an alternative wording of certain paragraphs of the Global Cross Border Enforcement Cooperation Arrangement, which might allow for increased participation therein.

Administration Team of the Group of Experts

The Information Commissioner's Office of the United Kingdom will act as Administration Team to the Group for the duration of its activity unless decided otherwise by the Chair(s).

The Administration Team shall:

- act as a contact point for the Experts.
- Provide assistance and advice to the Chair(s) and Experts as required for development of agendas, useful materials etc. for the Group.
- Prepare any external communications required by the Chair on behalf of the Group
- Minute-taking for meetings
- Organize teleconferences and in-person meetings

The Information Commissioner's Office shall be responsible for running the Administration Team.

Costs

Each Member bears their own costs for participation in the Group's activities.

12. Reference Documents used by the Group of Experts

- Council of Europe Convention 108 (1981)
- Council of Europe Convention 108 – Additional Protocol to the Convention 108 (2001)
- Council of Europe Convention 108 – Explanatory Memorandum
- OECD Privacy Framework (2013)
- OECD report on the cross-border enforcement of privacy laws (2006)
- OECD Recommendation on cross-border co-operation in the enforcement of laws protecting privacy, (2007)
- OECD Digital Economy Paper No. 178 - Report on the implementation of the OECD Recommendation on cross border cooperation in the enforcement of laws protecting privacy (2011)
- OECD Digital Economy Paper No. 187 – Regulation of trans border data flows under data protection and privacy laws (2011)
- UN Model Law on MLA (2007)
- UN Model Treaty (1990)
- Joint Investigation Teams in the EU. From Theory to Practice. Conny Rijken and Gert Vermeulen (2006)
- Critical notes on the Global Cross Border Enforcement Cooperation (May 2015)
- OECD – Council of Europe Treaty Convention MLA on Tax Matters (1988)
- UN Convention against Transnational Organised Crime (UNOCC) (2000)
- Treaty No.185 Convention on Cybercrime (CoC), Council of Europe (2001)
- International Covenant on Civil and Political Rights (ICCPR) (1966)
- Ibero-American Personal Data Protection Standards (2017)
- US-Canada Cooperation Agreement (1995)
- Agreement on mutual legal assistance between the European Union and the United States of America (2003)

- UN Convention Against Transnational Organized Crime And Protocols (2004)

- ICDPPC Global Cross-Border Enforcement Cooperation Arrangement (2014)

- Adopted Resolutions from the ICDPPC at its 29th, 31st, 33rd, 34th, 35th, 36th and 38th Conferences relating to improving cross-border enforcement cooperation

- Qualitative information provided by each of the Experts relating to their Authority's own practice in response to a questionnaire from the Co-chairs (January/February 2017).
